GDPR Blog Chapter 8: What happens when it all goes wrong – the Melodrama Part 2 – *updated for Data Protection Act 2018*

Welcome to Chapter 8. As every diligent reader of Bar Talk will now know, there is a new European-authored General Data Protection Regulation (GDPR). This will be in force in late May this year. It will be accompanied by a new Data Protection Act in the UK. The latter is still under Parliamentary scrutiny, so we have concentrated on briefing you on the "knowns" in GDPR rather than the "unknowns" in the new Data Protection Act. A summary of the latter will follow when it emerges from the Parliamentary process and becomes Law -***which of course it now has as DPA 2018 and this blog is designed to update you on its provisions. Remember, if there is no update, the GDPR Articles reign supreme.***

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].

We urge you to read these. They are a relatively light-hearted look at the world of Data Protection. They are very important given the tighter emphasis on this area in the GDPR ***and now the DPA 2018.***

Chapter 8: What happens when it all goes wrong - The Melodrama Part 2

The Melodrama Part 1 looked at what actions you had to take and who you had to inform in the event of a "personal data breach", that is where you left your computer and all its data about individuals on the bus. Or some malcontent trapped you into clicking on an apparently bona fide link in an email which destroyed all the data you held on your computer. We gave other examples as well.

Part 2 looks at where it hurts most – ***in your pocket***. There are two parts. The first concerns the Data Subject's civil rights. The second addresses administrative fines that the ICO can levy.

Civil Rights (Art.82)

Art.82 sets out the right to compensation from the Data Controller **and the Data Processor.** Under the Act, (that is, the existing Data Protection Act ***1998***) only the Data Controller was liable. There was also some confusion as to whether a Data Subject had to suffer pecuniary damage before claiming for distress. The Court of Appeal settled this in 2015 in *Google Inc v (1) Judith Vidal-Hall (2) Robert Hann (3) Marc Bradshaw(Claimants) and the ICO (Intervener)* [2015] EWCA Civ 311 allowing distress claims based on distress only without proof of pecuniary damage.

The GDPR now refers to "material or non-material damage". Does that expression leave us in the dark again? Borrowing from the clause 166(1) Data Protection Bill (version as of 4 March 2018) (sorry, we said we would not refer to this and we have done it twice now, but some guidance of what is likely to happen in the future is useful), "non-material damage" in Art. 82 includes distress. ***We can now confirm that DPA 2018 s.168(1) covers this point in the same terms.***

In summary therefore:

- Any Data Controller is liable for "damage" caused by processing which infringes GDPR
- Any Data Processor is liable for "damage" caused by processing only where (A) it has not complied with its Data Processor obligations in the GDPR (B) it has not followed the Data Controller's lawful instructions, either by not following or acting outside of these instructions
- If more than one Data Controller and/or Data Processor is involved in the relevant processing each is liable for the entire damage (but can claim back from the others that part of the compensation corresponding to the others' share of responsibility for the damage)
- Neither Data Controller nor processor is liable **if they prove** that they are not **in any way** responsible for the event giving rise to the damage.

Administrative Fines (Arts.83-84)

The Act permitted the ICO to levy fines of up to £500,000 in respect of a failure to comply with the Principles. **The position is rather more serious when the GDPR comes into force.** In summary, fines are now **up to**:

- **Euros 10m** (or 2% worldwide revenue if this is higher) – yes, you did read that correctly*; millions* - in respect of breaches of Arts.8 (child's consent to receipt of services); 11 (identification of data subjects); 25-39 (obligations of controllers and processors), 42 and 43 (certification to demonstrate compliance with GDPR).

- **Euros 20m** (or 4% of worldwide revenue if this is higher) for breaches of Arts. 5, 6, 7 and 9 (basic principles for processing including conditions for consent); 12-22 (data subject's rights); 44-49 (transfers of data to third countries); GDPR Chapter IX (as far as the Bar is concerned, rules made in the UK giving the ICO powers in relation to professional secrecy obligations; see Art.90); 58 (non-compliance with ICO orders).

It is worth remembering that:

- If you and your chambers stick to the rules outlined in previous Chapters *[see here and here]* then the question of fines should not arise. **But this does require a change of mindset. Instead of keeping everything, get rid of what you really do not need as soon as it is feasible to do so. If you need to keep papers on computer, use strong passwords and encryption and try to anonymise data (if you use Word, the Find and Replace function is a good starting point). Going forward, structure your documents so that is it easy to anonymise them in the future.**

- The ICO would prefer to ensure compliance rather than penalising errors, so the best thing to do is ask for guidance if you are in any doubt.

- In particular, if you have done something of which you are less than proud - your computer is heading to Edinburgh on the train but you are not - tell your IT manager and chambers **immediately** (…..but try the train company first!)

- Not all penalties are automatic. This is not an on-the-spot fine situation (though fixed penalties will exist of up to £4,350 if you haven't paid your registration fee). The ICO will consider the case.

- Factors taken into account will be (A) the nature, gravity and duration of the failure, (B) the intentional or negligent character of the failure, (C) mitigating actions taken by you to minimise damage, (D) how culpable you were taking into account the nature of technical and organisational measures employed, (E) previous failure, (F) the degree of cooperation given to the ICO to remedy the failure and mitigate adverse effects, (G) the categories of personal data affected, (H) how the ICO came to know of the failure (i.e. did you notify it), (I) the extent to which you complied with any previous enforcement notices (J) your adherence to approved ICO Codes of Conduct or Certification

mechanisms, (K) other aggravating or mitigating factors, (L) whether the proposed penalty is "effective, proportionate and dissuasive".

- There is a right of appeal against any ICO decision.

- The UK has the power to lay down and implement rules on other penalties applicable to infringements of the GDPR but which are not subject to administrative fines. Again, penalties have to be "effective, proportionate and dissuasive".

Other ICO Powers (Art 58)

Having got the serious stuff out of the way, we will now deal with the other powers the ICO has in its armoury. The ICO has **investigative** powers and **corrective** powers. These apply to you in your capacities as Data Processors and Data Controllers. ***Please see Part 6 of the DPA 2018 if you wish to read up what happens in detail. This is one of these provisions that the GDPR allowed the UK to expand as to how it should operate in practice, and allowed the UK to add additional powers if it wished to implement these.***

The **investigative** powers allow the ICO to:

- Order you ***(if necessary through the Courts)*** to provide information it requires for the performance of its tasks ***(DPA 2018 s.142 and 145)***
- Carry out investigations by way of data protection audits ***(DPA 2018 s.146)***
- Review certifications (don't worry about these for the moment)
- Notify you of an alleged infringement of the GDPR
- Obtain access to all personal data and information necessary for the performance of its tasks ***(DPA 2018 s.146)***
- Obtain access to your premises, including computer equipment, subject to compliance with UK procedural Law ***(DPA 2018 s.146)***.

These powers include obtaining information by means of "information notices" in order to assess whether an offence under the DPA 2018 has been committed or you are in breach of one of the principal parts of the GDPR, especially the processing elements in Arts.12-22. Section 142 sets out what is required, when you have to provide it and your rights of appeal under s.162. Section 149(2) delineates those parts of the GDPR/DPA 2018 in respect of which you may not have complied and which gives rise to these powers.

However, the ICO has no power to obtain information which is covered by legal professional privilege and which is connected with legal advice in respect of data

protection legislation or proceedings (actual or contemplated) under the data protection legislation (s.143(3) and (4)). In the unlikely event that you may expose yourself to criminal prosecution, you are also exempt from providing incriminating information UNLESS this relates to the DPA 2018 (s.143(6)-(7)).

We have also highlighted s.146. This concerns "assessment notices". It sets out provisions allowing the ICO, after service of written notice on you, to assess whether or not you are complying with data protection legislation.

The ICO is permitted access to your premises (Chambers or home office or both), specified documents, and may require you to assist the Commissioner to view documents (i.e. access to your computer), and to provide copies of documents and explanations of their contents. The ICO is also permitted to observe processing of personal data that takes place on your premises. The DPA 2018 even allows the ICO to interview people in Chambers who process your data (subject to their agreement).

"Assessment notices" must provide information about what happens if you fail to comply with such a notice, and as with "information notices" you have a right of appeal (s.162).

However, an "assessment notice" does not have effect if compliance would result in a disclosure of a communication which is subject to legal professional privilege and which is connected with legal advice in respect of data protection legislation or proceedings (actual or contemplated) under s.147 (s.147(2) and (3)).

Please note, it is a criminal offence to dispose of, conceal, block, falsify documents, equipment or material which the ICO would be entitled to see under the aforementioned provisions….not that we would suggest for one minute that you would engage in such conduct – see s.148 if you disagree! There is a defence that any such action would have occurred anyway even if a notice had not been served on you by the ICO.

The **corrective** powers include the following (Art.58(2)):

- Issuing you with a warning that intended processing are likely to infringe the GDPR
- Issuing you with reprimands where you have infringed the GDPR
- Ordering you to comply with a data subject's requests to exercise their rights under the GDPR
- Ordering you to comply with the GDPR in ways specified by the ICO and within specified timescales

- Ordering you to communicate a personal data breach to the Data Subject (Data Controllers only)
- Issuing temporary or permanent limitations on processing including a ban on processing
- Ordering deletion or rectification of personal data, or restrictions on processing and requiring you to inform recipients of personal data of such actions
- Imposing administrative fines (as above)
- Ordering you to stop sending data to recipients in foreign countries or to an international organisation (more about this in a later Chapter)

The Data Protection Bill contains some restrictions on these powers in relation to privileged documents in respect of data protection matters. We will deal with these when the Bill becomes Law. ***(See above).***

Under the DPA 2018, the ICO's corrective powers are set out in sections 149-159. We will merely summarise these in order to highlight the UK's implementation drafting.

These powers are divided into three sections:

1. ***Enforcement notices***
2. ***Powers of entry and inspection***
3. ***Penalties***

1. ***Enforcement notices***

The ICO can require you to take the steps set out in an "enforcement notice" issued by it, or conversely require you not to take the steps it specifies, in respect of any failure to comply with data protection legislation. The steps have, according to DPA 2018 s.149(6), have to be "appropriate" to remedy the failure. Any requirement not to take specified steps includes a power to ban the processing of all or a particular subset of personal data (s.150(3)).

So far as the Bar is concerned, these failures essentially arise from non-compliance with:

- ***the principles of processing which we have discussed extensively in earlier chapters [here] -GDPR Chapter II Arts. 5-11***
- ***a data subject's rights in GDPR Arts.12-22***
- ***the requirement to notify a personal data breach to the ICO (Art.33)***
- ***the principles for the transfer of personal data to third countries (GDPR Arts. 44-49)***
- ***regulations under DPA 2018 s.137 (payment of charges)***

The ICO has to make clear what the failing is and the reasons it has for reaching that conclusion (DPA 2018 s.150(1)). It is bound to consider (under DPA 2018 s.150(2)) whether your failure to comply with the legislation has caused or is likely to cause damage or distress to any person.

"Enforcement notices" are also required to set out what happens if you do not comply with the notice and rights of appeal available to you. (DPA 2018 s.150(5)).

Rectification and Erasure of Personal Data and Enforcement Notices (DPA 2018 s.151).

In Chapter 5, we told you about the data subject's rights to have his or her inaccurate data corrected by you on request (whether you are a controller or processor).

The ICO can also weigh in on this matter. It can issue an enforcement notice in two circumstances:

- *to ensure that you comply with the data processing principle that data should be accurate*
- *to lend support to a data subject's rights to have his or her data rectified (or, completed, in the event that the data is incomplete)- GDPR Art.16 or erased (for one of the reasons in GDPR Art.17) or to have the processing of his or her data restricted (for one of the reasons in GDPR Art. 18)*

See DPA 2018 ss.151-153 for other related provisions.

2. *Powers of Entry and Inspection (s.154 and Schedule 15)*

Schedule 15 is a procedural Schedule allowing the ICO powers of entry to premises, and search and seizure under warrant in the event of one of the failures under DPA 2018 s.149(2) that we described above.

Other than to draw your attention to paragraph 11 (there is no power to seize anything that is the subject of legal professional privilege), there is no purpose to be served by detailing rights which will be exercised by the ICO.

3. *Penalties (s.155 and Schedule 16)*

We gave a brief outline of the GDPR aspects above, majoring on the sheer amount that you can now be fined. Here we will simply expand on this outline.

Firstly, the penalty provisions are to be found in GDPR Art.83. Section155(2) of DPA 2018 refers to these powers.

Secondly, the ICO cannot simply decide to issue a penalty notice. You have to have either:

- ***Infringed s. 149(2) – see above or s.137 (non-payment of ICO charges); or***
- ***Failed to comply with the requirements of an "information notice", an "assessment notice" or an "enforcement notice".***

Thirdly, the ICO cannot levy any penalty it fancies. It has to ensure that (so far as GDPR matters are concerned), penalties are "effective, proportionate and dissuasive" (Art.83(1)). Further, the penalties can be imposed in addition to the "corrective powers" we set out above.

Fourthly, neither of the two foregoing paragraphs apply in the case of failure to pay charges (the combined effect of DPA 2018 s.155(4), s.149(5) and s.137).

Fifthly, you need to look at DPA 2018 Schedule 16 for the administrative detail e.g. payments, variations etc.

Sixthly, there is power for the Government to add to the failures outlined above and provide for a maximum penalty. This will be achieved by separate regulation.

Lastly,

- ***DPA 2018 s.157 and GDPR Art.83 determine the maximum amount of penalty that can be levied for failure to comply with GDPR provisions.***

- ***DPA 2018 s.157(4) sets out the maximum penalties for failure to comply with "information notices" "assessment notices" and "enforcement notices" – it is the higher amount we have set out above!***

- ***The ICO can set maximum penalties for failure by you to comply with the provisions relating to charges payable to the ICO (DPA 2018 s.158).***

The ICO also has a series of administrative and advisory powers. If you wish to read these, they are at Art. 58(3). These include powers to issue certifications, previously mentioned but not immediately relevant.

Guidance

We would just mention that the DPA 2018 requires the ICO to produce and publish "guidance" about how the ICO intends to exercise its functions with regards particularly to the aforementioned notices, but also to the ICO's other functions

(DPA 2018 s.160). This section sets out a number of factors which the ICO is required to take into account. This guidance can be found on the ICO's website at https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/.

Bar Council IT Panel