**GDPR Blog Chapter 7 - What happens when it all goes wrong - The Melodrama Part 1 –** *updated for the Data Protection Act 2018*

*Welcome to Chapter 7.* Over the past few weeks, we have dissected the General Data Protection Regulation (GDPR) which will be in force in May this year, together with a new Data Protection Act ***(the DPA 2018)***.

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]*; 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]*.

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 7 What happens when it all goes wrong - The Melodrama Part 1*

So far, we have introduced the play and the members of the cast. We have, metaphorically speaking, seen them go about their day-to-day business and observed their roles and responsibilities. We have then provided guidance as to how individual barristers and chambers would be affected.

This Chapter introduces the "excitement" into the plot. Someone or something happens that should not have happened. Melodrama Part 1 looks at what you do. Melodrama Part 2, in the next Chapter, looks at what could happen to you.

Having wound you up into a statement of excitement, let us look at what this means in reality.

Firstly, how does the melodrama arise? Lots of ways. You are attacked by a hacker who manages to penetrate your system and scramble your data. You leave your computer in the taxi after that great night out. You open an attachment in an email from your bank – but it is not your bank at all. Someone has borrowed its identity and your data is now frozen and subject to a demand for payment to release it. Your pupil discloses personal data when he or she was not supposed to do so.

These are all "**data breaches".** The GDPR identifies a "personal data breach" as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration,*

*unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".*

So now what?

*General Duty (Art.31)*

Note first that whether you are a **Data Controller** or a **Data Processor** or **both**, you have a duty to cooperate with the ICO in the performance of its tasks, when requested – see the next Chapter for how this might take place.

*Data Security (Art.32)*

We have already emphasised that prevention is better than cure *[here]*. GDPR Article 32 emphasises that you should adopt security measures which are appropriate to the risk. It sets out suggestions; anonymising data; encrypting information so that no-one can understand it; backup and prompt restoration of data in the event of an incident; regular testing of measures taken to ensure data security.

This is all couched in the rather sensible language that when adopting security measures, you should take account of the current state of the technological art (if that is not a contradiction in terms), the costs of implementation and the nature, scope, context and purposes of the processing you are undertaking. In addition, you can take into account just how likely it is that people's rights and freedoms will actually be compromised. From there, you can assess the level of security required against the risks that might arise – accidental or unlawful destruction, loss of data, unauthorised access to data etc.

*Duty to the ICO (Art.33)*

If you suffer a personal data breach then, once you are aware of it:

- you have to notify the ICO without undue delay,
- where feasible, this has to be done **within 72 hours** of becoming aware
- if you exceed 72 hours, you have to give the ICO reasons for the delay
- if you are acting as a Data Processor, you have to tell your Data Controller

If you are the Data Controller you may be receiving the bad news from your Data Processor!

The 72 hour deadline is very short, especially if it is necessary to investigate what has happened. You **don't** have to comply with the above if the rights and freedoms of Data Subjects are unlikely to have been put at risk.

When you notify you have to provide certain information. This is:

- the nature of the personal data breach
- what categories of Data Subjects are affected
- (approximately) the number of Data Subjects affected
- the categories of personal data records
- the approximate number of data records
- the name and contact details of a contact person who can provide more information if required (probably your IT Manager if it happened in relation to Chambers' systems)
- the likely consequences of the personal data breach
- measures already taken or proposed to deal with the personal data breach, including mitigation measures.

If you can't provide all that information at the same time, you can do it in stages, so long as there is no undue delay.

In addition, the Data Controller (not apparently the Data Processor) has to document what has happened - facts, effects and remedial action. This allows the ICO to verify compliance with this Article.

*Duty to the Data Subjects (Art.34)*

Things do not stop with the ICO. You (in your role as Data Controller) also have to notify **all** affected Data Subjects where there is a **high risk** to their rights and freedoms.

You have to tell Data Subjects:

- what was the nature of the breach (in clear and plain language)
- the contents of the last three bullet points above.

You (as Data Controller) can, however, avoid this if:

- if you implemented appropriate technical and organisational measures which were applied to the relevant personal data, for example by encrypting the data
- you have taken measures subsequent to the breach which ensure that the breach will not reoccur

- disproportionate effort is involved – in which case, a public notification is required (e.g. in the case where millions of items of personal data are lost).

What amounts to a "**high risk"** depends on the data you are processing. We cannot give you a fixed view for every circumstance. However, loss or disclosure of personal health data about children in a criminal case might be a suitable illustration. At the other end of the scale, if you lose one person's publicly available contact details (with no other data), this would amount to minimal risk.

The astute among you will have noted that there may be a conflict. This involves the situation where, e.g. the Data Subject is or is associated with the opposing party in pending, anticipated or existing litigation and notification potentially amounts to disclosure of your client's confidential information or legally privileged information. If this arises, it should be referred to the ICO for a definitive ruling.

***The DPA 2018 qualifies Art.34 under the authority of Art.6(3) which permits adaptation of GDPR provisions. So, the DPA 2018 provides that in certain circumstances the Art.34(1) and (4) provisions do not apply.***

***So, in matters of (a) the prevention or detection of crime, (b) apprehending or prosecuting offenders, (c) the assessment or collection of tax, a data controller is not required to communicate to the data subject any data breach that occurs.***

**A concluding warning: this is all new. We hope you will appreciate now why we have always recommended preventive measures to ensure the security of the personal data you are holding. There is potentially a serious amount of effort involved in complying with these onerous provisions. Think prevention!**

**The 72 hour deadline is very short, especially if the breach is discovered on a Friday evening or a Saturday morning. It will often not be immediately obvious what data has been lost, and it may be necessary to spend time investigating the position. It would therefore be strongly advisable for chambers to have a documented incident response plan in its IT Policy to provide an immediate focussed response to any incident that does occur. See *[here]* for a draft of such a plan.**

**Bar Council IT Panel**