GDPR: data breach

The morning from hell…and what to do next.

What should be done?

The immediate aftermath of a data breach is a worrying time for all concerned. Various steps need to be taken quickly to ensure that the response is appropriate and the harm to the organisation is minimised. This will involve a carefully co-ordinated response across a variety of disciplines - all of which will be underpinned by legal advice.

A key legal consideration will be whether to inform the Information Commissioner's Office ("ICO") (the regulator tasked with handling data protection matters in the UK) of the breach.

The first question will be whether you actually need to make a notification to the ICO. You will then need to decide when and how such notification should be made. In certain circumstances individuals affected by the data breach may also need to be informed.

Our lawyers can help you formulate your response and deal with all of this. You should get us involved from the very beginning. If a notification to the ICO is to be made then this should be done quickly (the General Data Protection Regulation imposes tight timescales). Below are some pointers as to what you need to consider in the immediate aftermath of a breach.

What will the ICO want to know?

1 What has happened?

2 How did the data breach happen?

3 When did the data breach occur and when did the organisation / company find out about the data breach?

4 How did the data breach first come to your attention?

5 What is the nature of the data i.e. what type (or categories) of personal data has been compromised and what volume of personal data is involved?

6 What are the likely consequences of the data breach and the likelihood of such consequences occurring?

7 What are the proposed measures by the organisation / company to mitigate the consequences of the data breach?

8 Have the data subjects been notified? If so, when and provide a copy of such notification. If not, what is the rationale for not doing so?

9 What (if any) processes are in place to assess the possibility of such an incident occurring?

What might the ICO do following the report?

- Shadow your investigation
- Order you to communicate the personal data breach to individuals affected (if you have not already done so)
- Liaison/ feedback
- Eventually decide on enforcement action to be taken
- No further action

Get in touch

If you would like to discuss the above in more detail, or learn more about our services, we would be delighted to hear from you.

John Benjamin
Partner
T +44 (0)20 7280 8950
E john.benjamin@dwf.law