Data Breach Management and The New EU Data Protection Regulation

The new EU General Data Protection Regulation contains an obligation on Data Controllers to notify supervisory authorities of personal data breaches. In some cases this extends to the Data Subjects as well.

Article 4 of the Regulation defines 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"*

Currently in the UK, under the Data Protection Act 1998 (DPA), there is no legal obligation to report such breaches to anyone. However the Information Commissioner's Office (ICO) guidance recommends that serious breaches should be brought to its attention. Last year telecoms company Talk Talk was the subject of a cyber attack in which almost 157,000 customers' personal details were hacked. The company was criticised for its slow response especially the time it took to inform the ICO and customers.

Article 31 of the Regulation states that as the Data Controller becomes aware that a personal data breach has occurred it should without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority (in the UK the ICO). There is no need to do this where the controller is able to demonstrate that the breach is unlikely to result in a risk for the rights and freedoms of individuals. For example a very minor data breach involving innocuous information about a few individuals. Where the 72-hour deadline cannot be achieved, an explanation of the reasons for the delay should accompany the notification.

Notification Contents

The notification must contain the following minimum information:

- a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects and data records concerned;
- the name and contact details of the controller's Data Protection Officer (now a statutory position) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects.

Where it is not possible to provide the above information at the same time, the information may be provided in phases without undue further delay.

The new Regulation will require all personal data breaches, no matter how insignificant, to be documented by Data Controllers. This should include the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with Article 31. Some, if not all of it, will also be accessible via Freedom of Information requests, as many local authorities have already found.

Individuals' Rights

Article 32 of the new Regulation states that Data Subjects should be notified without undue delay if the personal data breach is likely to result in a high risk to their rights and freedoms (e.g. fraud or identity theft), in order to allow them to take the necessary precautions. The notification will be similar to the one to the supervisory authority (discussed above) and should describe, in clear and plain language, the nature of the personal data breach as well as recommendations for the individuals concerned to mitigate potential adverse effects.

Notifications to individuals should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the need to mitigate an immediate risk of damage would call for a prompt notification whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.

There is no need to communicate a personal data breach to individuals if:

(a) the Data Controller has implemented appropriate technical and organisational protection measures, and that those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption; or
(b) the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of Data Subjects is no longer likely to materialise; or
(c) it would involve disproportionate effort. In such case, there will instead have to be a public communication (e.g. press release) or similar measure whereby the Data Subjects are informed in an equally effective manner.

Even where a Data Controller has chosen not to information Data Subjects, the supervisory authority can instruct it to do so. No doubt there will be more detailed rules setting out what kinds of breaches require notification and to whom.

Compensation

Article 77 states that:

> *"Any person who has suffered material or immaterial damage as a result of an infringement of the Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."*

This, together with the new breach notification provisions (discussed above), will no doubt see an increase in Data Subjects taking legal action against Data Controllers for data breaches. There may even be more class actions like the one against the London Borough of Islington in 2013 when 14 individuals settled for £43,000 in compensation after their personal data was disclosed without their authority. This action followed an ICO investigation, which resulted in the council being fined £70,000 under the DPA.

Currently the ICO can issue fines (Monetary Penalty Notice's) of up to £500,000 for serious breaches of the DPA. When the Regulation comes into force, this will be increased to 4% of global annual turnover for the preceding year (for businesses) or 20 million Euros.

The EU General Data Protection Regulation will have a big impact on all sectors. Whilst it is unlikely to come into force until the middle of 2018, all Data Controllers should be examining their approach to personal data breaches now and be putting into place processes to comply with the new rules.

Act Now Training can help. Please see our one-day EU DP Regulation workshops and our 1 hour webinars. We can also conduct DP audits and assessments.