GDPR Personal data breaches policy

1.0 Background

1.1 The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

1.2 The council should ensure it has robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not it needs to notify the relevant supervisory authority and the affected individuals.

1.3 Council must also keep a record of any personal data breaches, regardless of whether it is required to notify.

1.4 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

1.5 The ICO[1] makes it clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

2.0 What breaches do we need to notify the ICO about?

2.1 When a personal data breach has occurred, the council will need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then the council must notify the ICO; if it's unlikely then it doesn't have to report it. However, if it decides that it doesn't need to report the breach, it needs to be able to justify this decision, so you should be documented.

2.2 This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. The council will need to assess this case by case, looking at all relevant factors.

3.0 How much time do we have to report a breach?

3.1 A notifiable breach must be reported to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

Author: John Hesketh
Adopted:
Review:

[1] Information Commissioners Office