Guidance

Data breach a guidance note for staff

The Council has a zero tolerance approach to personal data breach reporting. This means that any potential breach should be reported to the Data Protection Officer as soon as you become aware of it. This guidance note is to help staff understand and act in accordance with this expectation.

What is a personal data breach?

A personal data breach means 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. Put another way, it amounts to a security incident that has affected the confidentiality, integrity or availability of personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Examples of personal data breaches can include:

- data being lost, destroyed or corrrupted;
- computing devices containing personal data being lost or stolen;
- data being sent to an incorrect recipient;
- data being accessed by or passed on to an unauthorised third party (this can include by other services of the Council where not permitted);
- alteration of personal data without permission;
- deliberate or accidental action (or inaction) by a controller or processor;
- loss of availability of personal data including, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

What happens when a breach is reported?

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.

When a personal data breach has occurred, we should try to contain it as well as considering the likelihood and severity of the potential or actual impact on an individual's rights and freedoms. If the impact of the breach is more severe, the risk to those rights and freedom's is higher; if the likelihood of the consequences is greater, then again the risk is higher. We will assess risk on a case by case basis, looking at all relevant factors.

If it's likely that there will be 'a risk' to the rights and freedoms then we must notify the Information Commissioner's Office (ICO). If it is likely that there will be 'a high risk', then we must also inform the individuals concerned. All decisions on whether to notify the ICO or individuals will be made by the Data Protection Officer.

One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach. The ICO has the power to compel us to inform affected individuals if they consider there is a high risk.

How quickly must I report a breach and what information is required?

You must report any actual or suspected breach to the Data Protection Officer immediately you become aware of it. The breach notification form (LINK) takes you through a process whereby we ask you to provide us with all the information we will need in order to establish what action now needs to be taken and what we will need to provide to the ICO in the event that we are required to report it.

The reason why it is essential that you inform the Data Protection Officer immediately is because in those cases where we must report, the report must be made without undue delay - in other words, notification must take place as soon as possible. Additionally, in the case of a report to the ICO, the report should not be not later than 72 hours after the Council became aware of the breach where feasible. It is important to understand that the clock starts ticking from the point of discovery.

What if we don't have all the required information available yet?

The legislation recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it.

However, the ICO expects controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. You must still notify us of the breach when you become aware of it, and submit further information as soon as possible. If you cannot supply all of the requested information immediately please tell the Data Protection Officer why, and when this detail will be available.

What if the breach has happened as a result of actions by a contractor?

All contracts with third party personal data processors (contractors) should clearly specify how they report potential breaches to us. Reporting needs to be done in a timely manner to enable us to meet our breach reporting obligations under the legislation.

You should still report any breach you are notified about to the Data Protection Officer as soon as you become aware of it.

Are there any other steps to take in response to a breach?

We will keep a full record all breaches, the effects and remedial action taken, regardless of whether or not they need to be reported to the ICO and / or the individual. This will enable us to comply with the accountability principle within the legislation.

We will investigate the breach and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

We may also need to consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

What happens if we fail to notify?

Failing to notify a breach when required to do so can result in a significant fine of up to 10 million euros.

Failing to deal properly and quickly with a breach can also have damaging consequences both for the individual(s) involved and also in terms of the Council's reputation.

Last updated:
3/11/23 5:31