GDPR personal data breach reporting tips for local government

Data protection law is changing, with new rules around reporting of personal data breaches.

The General Data Protection Regulation (GDPR) makes it compulsory for organisations to report a personal data breach to the ICO within 72 hours of becoming aware of it, if it's likely to result in a risk to people's rights and freedoms.

Our work shows local government is not as prepared for the breach reporting changes as it could be. The ICO can help and has the following top tips for councils preparing for the reporting of personal data breaches.

1 Know what a personal data breach is

- Can your staff identify potential personal data breaches?
- Does your senior leadership team value the importance of staff being able to do this?

2 Make sure staff know what they need to do

- Have you prepared a response plan for addressing any personal data breaches that occur?
- Is responsibility for managing breaches allocated to a dedicated person or team?
- Do staff know how to escalate a potential breach to this person or team?

3 Have a framework for reporting breaches

- Is there a process to assess the likely risk to individuals as a result of a breach and notify them if necessary?
- Is there a process to notify the ICO?
- Is there a register to capture and measure the severity of all breaches and near misses?
- Do you use the information for continuous improvement?

4 Training should be business-as-usual

- Do you have minimum pass marks and tests for data protection/GDPR training and any follow-on specialist information security training?
- Is training refreshed annually?

These tips follow a piece of work done by the ICO's Assurance team. More information on how to prepare for the breach reporting requirements is contained in the Guide to GDPR.

January 2018