UK GDPR – breach notifications

The GDPR, or General Data Protection Regulation, is a piece of European legislation which replaced the Data Protection Act (DPA) 1998 on 25 May 2018. A new UK Data Protection Act 2018 also came into force on the same day. The purpose of the UK Data Protection Act (DPA) 2018 is to apply the GDPR in the UK, and is now commonly referred to as 'UK GDPR'.

The Information Commissioner's Office (ICO) defines a 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."

This means that a breach is more than just losing data. The main `causes of breaches are loss or theft of paperwork; data sent to the wrong person by email; and data posted or faxed to the incorrect person. Breaches also include deliberate attacks on computer systems; unauthorised access of data by staff; and insecure disposal of paperwork.

Basic considerations

As a data controller or processor you are not only responsible for things that happen in your own workplace but also for the personal data that might be passed on to third parties for processing on your behalf. For example, these could be companies that deal with shredding, payroll, storage, recruitment or that carry out mail merges on your behalf. You must have a suitable written UK GDPR-compliant contract with such third parties.

You have to notify the ICO of a breach where it is likely to present a 'risk to the rights and freedoms of individuals'. It is a myth that all personal data breaches have to be reported – this is not the case. If you decide that there is no risk to the rights and freedoms of the individuals concerned then you don't need to report it. The circumstances of each incident should be considered on a case-by-case basis. Breaches should be notified within 72 hours of their discovery. The UK GDPR does not tell you when to self-report. You need to decide. You should document your decision. The ICO is an advocate of voluntary self-reporting.

If there is a likelihood of a high risk to people's rights and freedoms then those people affected need to be notified of the breach directly and without 'undue delay'. A high risk would be if the breach resulted in discrimination, financial loss, loss of confidentiality or any other significant economic or social disadvantage or if it damaged their reputation.

A breach notification must contain:

- Nature of the breach
- Categories and approximate numbers of individuals concerned
- Categories and approximate numbers of personal data records concerned
- Name and contact details of the data protection officer (DPO)
- Description of the likely consequences of the personal data breach
- Description of measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

What happens when a breach occurs?

Your method of responding to a breach rather than the breach notification itself should be at the forefront of your mind whenever one occurs. Immediately on becoming aware of a breach, it is important to not only seek to contain the incident but to also risk-assess any potential consequences.

There are four important elements to any breach management plan:

1. containment and recovery of the breach
2. assessment of the risks associated with the breach
3. notification of the breach
4. evaluation and response proposals.

What you need to do to prepare

- Make sure that everyone in the organisation understands what constitutes a data breach
- Introduce an organisational breach procedure (or update an old one) on reporting personal data breaches. This would include: who to contact in the organisation should staff or clinicians became aware of a breach; where the breach notification log is kept, how to complete it, how to submit it and the process of doing so
- Maintain a log of all personal data breaches (both reported and non-reported) and consider 'lessons learned' from past personal data breaches.

Common pitfalls

- Organisations do not have a breach management plan in place so when a breach occurs no one knows what to do
- Failure to report a significant data security breach within the required timescales
- Failure to notify individuals whose rights and freedoms have been affected by a data security breach.

Key points

- Act quickly to contain a breach and risk-assess potential consequences
- Ensure the organisation has an up-to-date plan in place for managing breaches and that staff are familiar with it
- Not every breach must be reported to the ICO, only those that pose a risk to people's rights and freedoms.

Further guidance

- ICO *Reporting information breaches*: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
- ICO *Self-assessment for data breaches*: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/
- The ICO have a dedicated advice line for UK GDPR enquiries if there is any doubt about whether to notify or not – 0303 123 1113, Option 4.

MDDUS GDPR checklist and guidance sheets: https://www.mddus.com/training-and-cpd/training-for-members/gp-risk-toolbox/gdpr