Responding to a cybersecurity incident

How and when to report a cybersecurity incident to the ICO.

ico.
Information Commissioner's Office

What should you do after a cybersecurity incident?

When you suffer a cyber-attack or a related cybersecurity incident, you might need to report it to the Information Commissioner's Office (ICO).

This leaflet explains when you should report it to us and what we will do in response.

When should you report the incident?

There are many kinds of cybersecurity incidents. If you have suffered a cyber-attack or related incident you will need to report it to us if there is a **personal data breach**.

This means a breach of security leading to "the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data."

Breaches can be accidental or deliberate, and a breach can be more than just losing personal data.

You must report a breach to us within 72 hours of becoming aware of it, unless you can demonstrate that it's unlikely to result in a risk to individuals' rights and freedoms.

What should you do if you suffer a personal data breach?

If you suffer a personal data breach you'll need to contact the ICO:

- You're legally obliged to report any personal data breaches within 72 hours of becoming aware of them, unless you can show that the breach is unlikely to pose a risk to individuals' rights and freedoms.
- You can report the breach online via our website at: www.ico.org.uk or via our helpline (Mon – Fri; 9am-5pm) on 0303 123 1113.
- You don't have to wait for 72 hours – the sooner you contact us the better.
- You can report in instalments and give us updates when you get more information.
- Give us as much detail as possible and be as accurate as you can.
- If there is a high risk to individuals' rights and freedoms you must tell them without delay.

What the ICO will do when you report a breach

If you report a breach by phone, we can give you immediate guidance about next steps:

- We might need some more information after you have reported. If we do, we'll contact you.
- If it's a more serious breach we may need to carry out an in-depth investigation.
- We may take regulatory action against you if we feel that you have not taken adequate steps to protect the data or manage the breach.

Other steps we may take include:

- We may use your reported data breach to identify data security incident trends.
- Where appropriate, we may share it with the with the National Cyber Security Centre (NCSC) and other law enforcement or cybercrime agencies, or other regulators such as the National Crime Agency (NCA) or the police or the Financial Conduct Authority (FCA).
- If it's relevant we may share the information with data protection regulators in other countries.

What other organisations should be notified of a serious cyber incident?

The NCSC offers unrivalled free and confidential real-time threat analysis, defence against national cyber attacks and technical advice on cyber security.

While reporting an incident to NCSC is not a requirement, they help victims of major cyber incidents to minimise any harm caused (including reputational damage). Visit www.ncsc.gov.uk/incident-management for more information.

Addressing the security of data processing

A key principle of the General Data Protection Regulation (GDPR) is that you process personal data securely by means of 'appropriate technical and organisational measures'.

Doing this requires you to consider risk analysis, organisational policies, and physical and technical measures.

The measures you take must ensure the confidentiality, integrity and availability of your systems and services and the personal data you process within them.

Can you ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services?

Confidentiality:

Have you pseudonymised or encrypted the personal data?

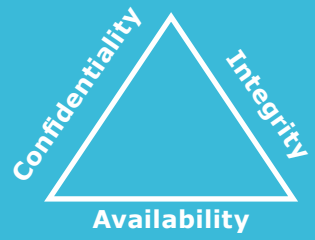
Integrity:

Do you have appropriate technical/security measures in place to:

- deal with the risk?
- regularly test in order to evaluate effectiveness?

Availability:

Can you restore the availability and access to personal data in a timely manner?



You can report a personal data breach online at www.ico.org.uk, or by calling our helpline (Mon – Fri; 9am-5pm) on **0303 123 1113**

ico.
Information Commissioner's Office