



Data Breach Response Basics

A practical introduction to recognising, reporting and handling personal data breaches. One-page summary.

The 10 things to remember

- 1 A breach is any security incident affecting personal data, including accidents; hacking is not required.
- 2 Breaches affect confidentiality, integrity, or availability; ransomware is a breach even if nothing is copied.
- 3 If you cannot show that disclosure or access did not happen, treat the incident as a breach.
- 4 Report immediately, even if it was you; speed beats embarrassment every time.
- 5 Contain fast: recall, remote wipe, disable accounts, isolate machines, but never act drastically alone.
- 6 Never delete evidence or cover up; a cover-up turns a process failure into individual misconduct.
- 7 Write a factual timeline note while it is fresh: what happened, when, what data, what you did.
- 8 The ICO must normally be notified within 72 hours of awareness; the clock runs through weekends.
- 9 A high risk to individuals means telling them too, promptly and in plain language.
- 10 Every breach goes in the internal register, even those that never needed reporting to anyone.