Data Breach Response Procedure

SOP · UK · Updated 2026-07-23 · Square brackets are placeholders to replace with your own details.

A data breach response procedure is the written sequence your team follows when personal data is lost, stolen, sent to the wrong person, or accessed without authorisation. It sets out who to tell first, how to contain the damage, how to assess the risk to the people affected, and how to decide within 72 hours whether the ICO must be notified.

The 72-hour window for notifiable breaches is short, and it does not pause for weekends. Organisations that handle breaches well are the ones that decided the roles, the reporting channel, and the assessment steps in advance — you cannot design a response during a live incident.

This template gives you the full procedure: what counts as a breach, immediate containment steps, the risk assessment, the ICO notification decision, telling affected individuals, and the breach log that evidences it all.

Purpose and scope

This procedure sets out how [Your company] responds to actual or suspected personal data breaches. It applies to all staff, all systems, and all personal data we hold — about customers, staff, or anyone else — in any format.

What counts as a personal data breach

- An email, letter, or attachment containing personal data sent to the wrong recipient.
- A lost or stolen laptop, phone, memory stick, or paper file.
- A phishing compromise, ransomware infection, or other unauthorised access to systems holding personal data.
- Staff accessing records they have no work reason to see.
- Accidental deletion or alteration of personal data with no backup.
- If in doubt, report it — the assessment below decides whether it matters, not the person who spotted it.

Roles and responsibilities

- Breach lead ([name/role], deputy [name/role]): runs the response, owns the breach log, and makes the ICO notification decision with [senior role].
- IT support ([name/provider]): contains technical incidents and preserves evidence.
- All staff: report suspected breaches immediately by [phone number/channel]. Honest mistakes reported promptly are never treated as misconduct; concealment is.

Immediate actions: report and contain

1.

Report the suspected breach to the breach lead at once by [phone/channel] — including evenings and weekends. Do not wait for the next working day.

2. Record the time you became aware. The 72-hour clock for any ICO report runs from this point.
3. Contain the breach: recall the email, remote-wipe the device, disable compromised accounts and change passwords, isolate affected systems, or retrieve the papers — whichever applies.
4. Preserve evidence. Do not delete emails, logs, or files connected to the incident.
5. Ask any unintended recipient to delete the data and confirm in writing that they have.

Assess the risk

1. Establish the facts: what data, about whom, how many people, what caused it, and whether the data is still exposed.
2. Assess the likelihood and severity of harm to the individuals affected — fraud, financial loss, distress, discrimination, or physical risk.
3. Weight the assessment up where special category data, financial details, or children's data are involved.
4. Record the assessment and conclusion in the breach log, however minor the incident.

Decide whether to notify the ICO

The breach lead and [senior role] decide, based on the assessment, whether the breach is likely to result in a risk to individuals. If it is, report it to the ICO within 72 hours of becoming aware, using the ICO's online reporting route. You do not need every fact before reporting — the ICO accepts information in phases, so never let an incomplete picture run the clock down.

If the decision is not to report, record the reasons in the breach log. That record is what shows the decision was considered, not missed.

Telling the people affected

If the breach is likely to result in a high risk to the individuals affected, tell them without undue delay, in plain language: what happened, what data was involved, what we are doing, what they can do to protect themselves, and who to contact at [Your company]. Coordinate with [insurer/IT provider/other organisations involved] before communicating, but do not let coordination become delay.

Records, lessons, and review

Every breach and near miss goes in the breach log kept at [system/location]: dates and times, facts, assessment, decisions, notifications, and actions. Within [period, e.g. two weeks] of closing an incident, the breach lead runs a short lessons-learned review and feeds any fixes into training, systems, or this procedure.

This procedure is reviewed [frequency, e.g. annually] and after every reportable incident. Owner: [name/role]. Next review due: [date].

How to use this template

1. Name the breach lead and deputy, and put their out-of-hours contact details where staff will actually find them at 6pm on a Friday.
2. Brief every team that the rule is "report at once, blame later" — the procedure fails if staff sit on mistakes.
3. Check your contracts with IT and software providers require them to tell you promptly about breaches on their side.
4. Check your insurance policy for its own breach notification conditions and add them to the contact list.
5. Run a tabletop exercise on a realistic scenario — a stolen laptop or a misdirected payroll email — within a month of adopting the procedure.
6. Set up the breach log before you need it, even as a simple spreadsheet.

Official guidance

- ICO — Report a breach
- ICO — UK GDPR guidance and resources