

Report a personal data breach

This form is for organisations that have experienced a personal data breach and need to report it to the ICO. **Please do not include any of the personal data involved in the breach when completing this form.** For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

You should ensure the information provided is as accurate as possible and supply as much detail as possible.

About your report

Please answer the following questions, to help us handle your report efficiently and to better understand our customers.

If you have already spoken to a member of ICO staff about this breach, please give their name:

Report type

- ☐ Initial report – report complete
- ☐ Follow-up report – report complete
- ☐ Initial report – additional information to follow
- ☐ Follow-up report – additional information to follow

(Follow-up reports only) ICO case reference:

Reason for report – after consulting the guidance

- ☐ I consider the incident meets the threshold to report
- ☐ I do not consider the incident meets the threshold to report, however I want you to be aware
- ☐ I am unclear whether the incident meets the threshold to report

Size of organisation

- ☐ Fewer than 250 staff
- ☐ 250 staff or more

Is this the first time you have contacted us about a breach since the GDPR came into force?

- ☐ Yes
- ☐ No
- ☐ Unknown

About the breach

Please describe what happened

Please describe how the incident occurred

How did the organisation discover the breach?

What preventative measures did you have in place?

Was the breach caused by a cyber incident?

- ☐ Yes
- ☐ No
- ☐ Don't know

When did the breach happen?

Date: Time:

When did you discover the breach?

Date: Time:

Categories of personal data included in the breach (tick all that apply)

- ☐ Data revealing racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Sex life data
- ☐ Sexual orientation data
- ☐ Gender reassignment data
- ☐ Health data
- ☐ Basic personal identifiers, eg name, contact details
- ☐ Identification data, eg usernames, passwords
- ☐ Economic and financial data, eg credit card numbers, bank details
- ☐ Official documents, eg driving licences
- ☐ Location data, eg coordinates
- ☐ Genetic or biometric data
- ☐ Criminal convictions, offences
- ☐ Other (please give details below)

Please give additional details to help us understand the nature of the personal data included in the breach:

Number of personal data records concerned?

How many data subjects could be affected?

(Cyber incidents only) If the number of data subjects affected is not known, estimate the maximum possible number that could be affected/total customer base

Categories of data subjects affected (tick all that apply)

- ☐ Employees
- ☐ Users
- ☐ Subscribers
- ☐ Students
- ☐ Customers or prospective customers
- ☐ Patients
- ☐ Children
- ☐ Vulnerable adults
- ☐ Other (please give details below)

Describe any detriment to individuals that has arisen so far, or any detriment you anticipate may arise in the future

Is the personal data breach likely to result in a high risk to data subjects?

- ☐ Yes
- ☐ No
- ☐ Not yet known

Please give details

(Cyber incidents only) Recovery time

- ☐ We have successfully recovered from the incident with all personal data now at the same state it was shortly prior to the incident
- ☐ We have determined that we are able to restore all personal data to the same state it was shortly prior to the incident and are in the process of doing this
- ☐ We have determined that we are unable to restore the personal data to the same state it was at shortly prior to the incident, ie backups failed, no

current backup, backup encrypted etc

- ☐ We are not yet able to determine if personal data can be restored to the same state it was shortly prior to the incident

Had the staff member involved in this breach received data protection training in the last two years?

- ☐ Yes
- ☐ No
- ☐ Don't know

Please describe the data protection training you provide, including an outline of training content and frequency

(Initial reports only) If there has been a delay in reporting this breach, please explain why

Taking action

Have you taken action to contain the breach or limit its impact? Please describe these remedial actions

Please outline any steps you are taking to prevent a recurrence, and when you expect they will be completed

Describe any further action you have taken, or propose to take, as a result of the breach

Have you told data subjects about the breach?

- ☐ Yes – we have determined it is likely there is a high risk to data subjects so we have communicated this breach to data subjects
- ☐ Yes – we have determined that it is unlikely there is a high risk to data subjects, however decided to tell them anyway
- ☐ No – but we are planning to because we have determined it is likely there is a high risk to data subjects
- ☐ No – we determined the incident did not meet the threshold for communicating it to data subjects

Have you told, or are you planning to tell any other organisations about the breach?

- ☐ Yes
- ☐ No
- ☐ Don't know

If you answered yes, please specify

Are you a member of a UK GDPR Code of Conduct or Certification Scheme, as approved and published on the ICO website?

- ☐ Yes
- ☐ No

If yes:

Please confirm the Code/Scheme name

Are the Code or Scheme's requirements relevant to the breach that has occurred?

- ☐ Yes
- ☐ No

Have you informed the relevant Monitoring Body or Certification Body?

- ☐ Yes
- ☐ No

Suspicious websites

If the breach relates to a suspicious website, you can report the website to the National Cyber Security Centre (NCSC). By reporting, you can help stop cyber criminals and protect others online.

The ICO won't see the details of your report to NCSC, so you should make sure you tell us everything we need to know on this form.

[Report a suspicious website - NCSC.GOV.UK](https://www.ncsc.gov.uk/report-a-suspicious-website)

About you

Organisation (data controller) name

Registration number

If not registered, please give exemption reason

Business sector

Registered organisation address

Person making this report

In case we need to contact you about this report

Name:

Email:

Phone:

Sending this form

Initial report

If this is your initial report, please send your completed form to icocasework@ico.org.uk, with 'Personal data breach notification' in the subject field.

Follow up report

If this is a follow up report, please *reply to the email we sent you*, attaching this completed form to it. (Make sure you leave the subject line as it is – this will ensure your follow-up gets added to your case).

OR, send by post to:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

You should read our guidance to determine what steps you should take.

Based on the information you have provided, we will contact you within seven calendar days to provide information about our next steps. If this is your initial report, we'll give you a case reference number.

If your correspondence relates to an existing case, we'll add it to your case for your case officer to consider.

22 February 2022 – Version 4.0

If you need any help in completing this form, please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday).

For information about what we do with personal data see our [privacy notice](#).