How to guide – breach report form

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

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

This helps us identify which member of staff may already be familiar with your specific incident. Please provide full name.

Report type

Please detail at this point whether this is the first instance of notifying the ICO of the breach and if it is whether you are submitting a completed report or whether you will be sending in additional information. Similarly, if you are providing additional information relating to an existing report whether this is a complete report or whether there will be additional information to follow. Once the breach report is recorded on our system you will receive an acknowledgement email detailing the reference number for the case. If you are providing a follow up report please include this reference as it enables us to link your additional information to the existing case we hold for you.

Please ensure that if you provide limited information in your initial report, you provide a follow up report in a timely fashion.

Reason for report – after consulting the guidance

After assessing the appropriate guidance, including completing the self-assessment tool on our website, please provide the reason for the report.

○ I consider the incident meets the threshold to report

You have assessed the breach and consider there to be a risk of detriment to data subjects and therefore are notifying the ICO appropriately.

○ I do not consider the incident meets the threshold to report, however I want you to be aware

Please note that only breaches that meet the threshold to report should be reported to the ICO. There is no obligation to make the ICO aware of incidents where the likelihood of risk is low. In these instances however, you are still expected to document the breach internally. This should include the facts, effects, containment and remedial measures implemented in light of the breach.

○ I am unclear whether the incident meets the threshold to report

If this is the first time reporting a breach to the ICO or you require additional support regarding a specific incident please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday) where you can discuss the breach with a member of staff and if appropriate submit the report over the telephone.

Size of Organisation

Please advise whether you are an organisation with fewer than 250 staff or 250 staff or more.

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

When considering this question, take into account not only contacting the ICO to report a breach but also if you have sought advice from us about a breach.

About the breach

Please answer these questions as thoroughly as possible to ensure that ICO staff assessing the breach are provided with enough information to gain a full understanding of the incident in question. Please refrain from using internal acronyms or jargon to ensure the content is clear to individuals who may not be familiar with the systems etc that may be used within your organisation. Please note that any examples provided in this guide are not exhaustive and should be considered as a guide.

Please describe what happened

Please provide a summary of the incident. This initial overview should enable the ICO to gain a general understanding of the nature of the breach.

Please describe how the incident occurred

What is the root cause of the breach? For example could it be due to human error, a system malfunction or maybe a failure to comply with existing policies and procedures already in place.

How did the organisation discover the breach?

For example did an incorrect recipient/member of the public make your organisation aware? Did the staff member realise the error that may have been made? How was it brought to your attention?

What preventative measures did you have in place?

For example this could be clear policies and procedures, a checklist or potentially a system configuration or some description to help prevent breaches of this nature.

Was the breach caused by a cyber incident?

For example was the breach caused by Ransomware or a Phishing attack.

When did the breach happen?

Depending on the nature of the breach, it may be difficult to pin point an exact time and date of occurrence. A rough estimate can be provided in this instance.

When did you discover the breach?

Please note that this is when the organisation was made reasonably aware which could differ from when the reporter was made aware.

Categories of personal data included in the breach

Consider the nature of the personal data that has been impacted and document in this section. Please note that addresses of data subjects are considered to be ‘basic personal identifiers’ while coordinates are classed as ‘location data’. Please give additional details to help the ICO assess the data in context. For example, health data can range from quite sensitive data to extremely sensitive data.

Number of personal data records concerned?

A singular record could be a missing form/list, a notebook or an electronic device. An email on the other hand may have been issued to 20 individuals, this would be therefore classed as 20 records. When assessing the number of data records, consider the nature of the incident and how many records that may be accessible to third parties. In some cases this could be a duplication of the same record (e.g email).

How many data subjects could be affected?

This relates to data subjects whose personal data has been impacted as a result of the breach, it does not include for example incorrect recipients of another individual's data.

(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

At the time of reporting, you may not know how many data subjects have been affected by a breach. You should therefore indicate the maximum number that may be affected. If all your customers may be affected, you should state how many customers you have.

Categories of data subjects affected?

Please tick all that apply. If a category is not listed, please provide additional details in the section directly below 'other'.

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

Please describe the impact on data subjects as a result of the breach at the time of the report being submitted and/or any impact on the data subjects that may occur at a later date . Please state if there has been any actual harm to data subjects.

For example could there be a potential risk of identity theft?

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

Please detail your overall assessment of the risk in relation to your breach notification.

Had the staff member involved in this breach received data protection training in the last 2 years?

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

Please provide a brief description, we do not require you to send us a copy of your training materials. For example – your training could include online e-learning or face to face classroom training.

If there has been a delay in reporting this breach, please explain why

Why was the report not submitted within the 72 hour time frame? Please provide your rationale behind this delay.

Taking action

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

This could include successful attempts to recover the information or confirmation you may have received from incorrect recipients that the data has been deleted/destroyed and will not be transmitted further. Alternatively, if an electronic device has been lost/stolen, confirmation that the contents have been wiped to prevent further access by unauthorised individuals.

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

This section focuses on what you are doing to learn from the incident and stop something similar from happening again. You should have a timescale for each action you intend to take.

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

This section is for any details you have not already included.

Have you told data subjects about the breach?

Please use the most appropriate action for your situation based on information provided to inform the ICO whether you have notified data subjects affected.

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

For example the Police, other regulators or supervisory authorities. Please consider any other organisations who may need to be notified.

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

Please confirm the Code/Scheme name

You should tell us if you are a member of a UK GDPR Code of Conduct or Certification scheme. All the Codes and Schemes are listed on the ICO's website.

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

For example, does the Code or Scheme require you to have particular measures in place to protect personal data of the kind involved in this breach?

Have you informed the relevant Monitoring Body or Certification Body?

We may ask you to inform the relevant Monitoring Body or Certification Body, if you have not already done so.

Suspicious websites

Please also consider that 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

About you

Organisation name

Please detail your company name where it states 'Organisation (data controller) name'. This does not relate to the specific individual who has completed the report. Instead the contact details of the reporter must be provided in the 'Person making this report' section.

Registration number

Please provide your ICO Registration number. If exempt please put N/A in this section.

If not registered, please give exempt reason

Please detail the reason/s you may be exempt from paying the registration fee. If you are unsure about your status, try our online self-assessment tool.

Business sector

Please explain the industry your organisation falls under.

Registered organisation address

Please provide your trading address.

Person making this report

Please note that any future correspondence issued relating to your case (if completed online) will be sent to the email address of the original reporter. This may include requests for further information if we feel it may be appropriate. Please ensure the member of staff within your organisation who is reporting the breach is suitably appropriate to deal with this request (and is able to liaise with other business areas/individuals where necessary).