# Guide to assessing personal data breaches

This guide is to help you assess personal data breaches. It applies to both initial and follow-up information.

Under the General Data Protection Regulation (GDPR), data controllers are required to notify the ICO about certain personal data breaches. The initial notification should, where feasible, be made within 72 hours of the data controller becoming aware of the breach.

Personal data breach reports should be initially assessed within the first seven days of the report being received. Any large scale or high-profile incidents should be identified quickly so that cases can be referred, or the relevant department notified e.g., civil, cyber, or press. To ensure any incidents are appropriately flagged you will need to keep up to date with the **Daily Update** email and the **Hot Topics** list when picking up cases. The PDB team has a target for closing or referring 80% of breach reports within 30 days of them being received at the ICO.

This guide will help you to assess the information provided by data controllers about personal data breaches. The questions appear in a different order on the telephone and online forms – this guide follows the order of the online form.

## Reviewing a breach report: Factors to consider

When reviewing a breach report you will need to consider whether the data controller has provided sufficient information to allow the ICO to:

- close the case at the initial stage, with advice and guidance where necessary;
- whether the case needs to be referred for further investigation, for example if it is likely to be high profile or result in regulatory action;
- or if we need the controller to provide more information to allow us to make a decision.

In making this decision you will need to consider a number of factors, including the nature of the breach and the potential harm caused. It is also important to think about what level of action by the ICO is reasonable and proportionate, given the circumstances of the case.

Consideration should be given to:

- **The nature, gravity, and duration of the breach**

  What has gone wrong? What is/was the potential impact of this?

Breaches caused by obvious security failings, that are serious or have occurred over a long period of time are more likely to be suitable for a fine than breaches that would have been difficult to foresee, do not have serious consequences and were quickly identified and remedial action taken.

Consideration should be given to referring breaches that have caused very significant negative consequences for data subjects, especially if the controller has failed to take action to prevent such consequences.

- **The nature and purpose of the processing concerned**

  What has the controller been doing, and why?

  Organisations should ensure that greater security is in place for high-risk processing, for example, if processing special category data. You should also give consideration to whether the controller should have been processing the data in any event, for example, was the controller storing payment card information, including CVV numbers, in contravention of the relevant payment card standards?

- **Whether the breach was caused by a systemic failure, or a human error**

  Why did it happen?

  Did the controller know they should have better security in place but fail to implement proper measures, or did they fail to consider the risks that could arise in respect of the personal information they were processing? If yes, we may consider the case suitable for referral, if however, the controller had put the necessary security measures in place and had policies and procedures, but staff had failed to follow these correctly, we may regard this as a human failure, rather than a systemic one.

- **Any action taken by the data controller to mitigate the damage suffered by data subjects**

  What steps has the controller taken to contain the breach and reduce the risks for individuals? Are there any steps that they should have taken, but haven't? Could this be dealt with through advice, or is the failure so significant that the matter requires further investigation? For example, if the controller has published sensitive personal information on their website, but has failed to

remove it, despite having been informed on numerous occasions that it was there

- **Any previous breaches by the controller?**

  Has the controller experienced similar incidents before? We should note whether the ICO has previously provided advice to the controller which, if that advice had been followed, could have prevented the breach from recurring.

- **Any other aggravating or mitigating factors**.

  You must objectively assess the circumstances of the breach, the controller's response and whether enough has been done to demonstrate that individuals' rights are being taken seriously. You should also be aware of any strategic priorities or 'hot topics' that the ICO would like to look at in detail regardless of whether the usual criteria are met.

---

## Personal data breach notification forms

Below goes through the different sections of the current online reporting form and what you will need to look out for and consider when making an assessment.

Personal Data Breach Reporting Form - report-a-personal-data-breach-form.doc (live.com)

### Report type

Check this section to see whether the initial report is complete, or they have indicated they will provide us with further information. This could help to determine whether the DC will be able to provide any additional information if we went out for any further questions. This could also provide you with information on whether a report has already been received about the incident and the controller is sending through additional information.

### Reason for report – after consulting the guidance

This section could be an opportunity to educate a controller. If a controller has indicated that they do not consider the incident meets the threshold to report but they want to make us aware. You should make an assessment on the incident and provide advice to the controller regarding their assessment. If you agree with their assessment of it not meeting the

threshold, consider providing the controller with guidance about the requirements and directing them to log the incident internally.

If the controller has indicated, they are unclear on whether it meets the threshold to report. Guidance should be provided to the controller about the threshold for reporting to the ICO and on how to risk assess breaches with relevant signposting to our website. For example, to the self-assessment tool or risk assessing guidance.

**Size of organisation**

Considering the size of an organisation could be useful when providing guidance to an organisation following a breach. For smaller organisations they can be signposted to the SME hub on the website for simplified guidance which might be easier to understand. Larger organisations will often have a better understanding of the legislation and could be signposted to the main guidance.

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

If this is the first time, they have contacted us this could mean the organisation may need some further guidance within any closure letters we send. This may not always be the case, but it is something to look out for.

## About the breach

**Please describe what happened?**
**Please describe how the incident occurred**

These two questions at the start of the form should outline what has happened and will usually give you the context of the situation surrounding the breach and the root cause of the incident.

- To what extent can the data controller be considered responsible for what has happened (rather than the incident being wholly attributable to individual error on the part of a staff member)?
- Could the incident have easily been avoided?
- Did the controller have sufficient measures in place that should have prevented the incident?
- Do we have enough information to understand what went wrong on this occasion?

For the ICO to take regulatory action, there must have been a serious breach. In relation to breaches of the security principle, we must be able

to show that there has been a failure to have appropriate organisational and technical measures in place to protect the personal data they handle.

If the incident relates to a s.170-173 DPA ’18 offence this should be notified to the Criminal Investigation Team for consultation, prior to a final decision being made (see CrIT referral process in guidance on s.170)

**How did the organisation discover the breach?**

How the data controller became aware of the incident may influence the assessment of the likelihood of detriment to the data subject.

For example, if the recipient of an incorrectly addressed email contacted the data controller to inform them that information had been received in error, the recipient has acted responsibly, and it may be reasonable to infer that the risk to the data subjects is reduced

**What preventative measures did you have in place?**

What should have happened? Had the data controller considered the potential risks to the data they handle and implemented processed and procedures to protect that information? Had staff received training in data protection and information governance?

A serious failure on the part of the data controller to have sufficient measures in place, or to recognise the potential implications in respect of the data they hold may lead to regulatory action being taken against that controller, whereas, if the failures were relatively minor, or processes had been put in place but had failed on this occasion, we may be able to deal with this by issuing advice.

**Was the breach caused by a cyber incident?**

A cyber incident is a third-party attack on a controller or processor’s computer systems, such as a ransomware or phishing attack. Breaches caused by inputter error or internal system malfunction are not classed as cyber incidents.

Most cyber breaches are referred to the Cyber Investigations team, who have the technological expertise to assess the security measures that the DC had in place, however the PDB team will deal with low level phishing attacks, where the data controller had measures in place that should have prevented the attack, such as staff cyber security training and system firewalls, and action has been taken to contain the breach and prevent similar attacks in the future, such as passwords being changed, forwarding rules removed and multi factor authentication being introduced.

Nb: If a phishing attack has occurred following a different type of cyber-attack, such as a brute force attack which has led to scam emails being sent from the system, this should be referred to the Cyber Investigations team, as the first incident was the brute force attack. If in doubt, contact the cyber sector specialist or a PDB team manager.

**When did the breach happen?**
**When did you discover the breach?**

What was the time scale between the incident occurring and the data controller becoming aware of it? Should they have noticed sooner? Have they reported the incident without undue delay and, if feasible, within 72 hours of becoming aware?

Has the delay in discovering or responding to the breach increased the potential detriment for the data subjects?

For example: An Estate Agent accidentally published a copy of a sellers passport and driving licence when publishing the property listing on Right Move. They have a process in place for checking all their listings within 24 hours of publication. The error was spotted through this check and the documents were removed quickly. In the meantime, the listing had only been viewed 3 times. Acting quickly has reduced the potential for detriment. If they had delayed taking action, more people may have viewed the data, putting the data subject at greater risk.

**Categories of personal data included in the breach**

Has any special category or criminal conviction data been disclosed? This could potentially increase the level of detriment for the data subject. Data controllers must have technical and organisational measures in place to protect all the personal data they hold, but the ICO expects such measures to be particularly robust if the data is likely to be of a more sensitive nature.

**Number of personal data records concerned**

Was the breach caused by the disclosure of one document containing many data subjects' details (such as a spreadsheet) or many documents containing information about one person (such as a response to a subject access request)?

**How many data subjects could be affected**

Are a large number of data subjects affected? To what extent?

Are a small number of data subjects (or even just one) affected to a great extent?

Data breaches affecting a large number of individuals will not necessarily result in regulatory action – it will depend on the nature of the personal data and the potential consequences for these individuals arising from the breach. However, other departments in the organisation may need to be aware of breaches that affect a significant number of individuals, such as the Intelligence Hub, PADPCS and the Press Office.

**(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**

This question has been added to the form for cyber incidents as in some cases the exact numbers affected are not yet know. This may not apply to your assessment of an incident unless you are looking at a phishing case.

**Categories of data subjects affected**

Are the data subjects children, or vulnerable adults? Has the controller taken appropriate measures to ensure the necessary levels of protection had been put in place? A breach that may not cause significant concern for some people may be extremely distressing for others, particularly if they are already vulnerable.

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

What are the adverse effects? What impact would they have on the data subjects if they occurred? Has the data controller given full consideration to what may happen? Is this assessment reasonable, or have potential concerns been missed or discounted?

This helps us to assess the response of the data controller; are they taking the breach seriously? A failure to respond to a breach, or acknowledge the potential implications, may indicate that the incident should be referred for further investigation.
Nb – we will only consider the potential consequences for data subjects. Consequences for organisations, such as reputational damage, are not covered under the legislation.

Consequences for data subjects includes things such as:

- Loss of control over personal data.
- Limitation of a data subject's rights.
- Discrimination.
- Identity theft and/or fraud.

- Financial loss.
- Unauthorised reversal of pseudonymisation.
- Damage to reputation.
- Loss of confidentiality of personal data.
- Any other significant economic or social disadvantage to the person concerned.

**Is the personal data breach likely to result in a <u>high</u> risk to data subjects?**

Article 34 GDPR states "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persona, the controller shall communicate the personal data breach to the data subjects without undue delay".

If the data controller has assessed the risk as high, but has not informed the data subjects, we should consider contacting the DC as soon as possible to raise this as a concern.

When assessing a personal data breach report you should consider the level of risk for the data subject. Has the controller considered all the relevant factors and made a reasonable risk assessment? When assessing whether this breach is likely to result in regulatory action, we'll need to give consideration to how *likely* it is that these consequences will arise.

High risk to data subjects arising from human error rather than organisational failing is less likely to lead to regulatory action, however consideration should be given whether further investigation is required. In order to close the report with no further action we should be satisfied that the organisation has taken steps to minimise the impact of any harm to the data subject and to learn from the incident.

**Please give details**

How likely consequences are to arise will depend on preventative, containment or recovery measures the controller has in place. For example, personal data may have been pseudonymised or encrypted, data may have been uploaded to the controller's website but not accessed, data may have been recovered from an unintended recipient and assurances given that it would not be shared (for example, when information is sent to the wrong NHS body in error, there is an expectation the information will be treated in confidence).

**(Cyber incidents only) Recovery time**

The only cyber incidents dealt with by the PDB team are low level phishing attacks, with limited consequences. If a controller indicates that

they have experienced a phishing attack but has not recovered it may be appropriate to refer the report to the Cyber Investigations Team, as more specific technical advice may be required.

All other types of third-party cyber-attacks should be referred to the Cyber Investigation Team as a matter of course.

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

This is helpful to understand whether the controller is aware of its responsibilities in ensuring that its staff are compliant with the legislation and are aware of their responsibilities. By providing training to staff frequently will ensure they are provided with up-to-date guidance on the legislation.

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

This helps us to assess the level of the controller's security measures. If they have indicated that the staff member involved hasn't had training or they don't know, we should be asking, "Why not?"

Controllers are obliged to have sufficient organisational measures in place to protect the personal data they hold. There is little to be gained by having processes and technical measures, if staff do not know what they are or how to use them. Failure to have adequate training in place may lead to concerns about the controller's overall compliance with the legislation, and it may be appropriate for the matter to be referred for further investigation.

If a controller indicates that the staff member had received data protection training, but that person had failed to follow the correct process, or had not considered the implications of their actions, it may be appropriate to offer advice about the need to review the efficacy of that training.

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

Factors that may be reasonable when considering a delay include:

- The need to seek specialist advice to establish whether a breach had in fact occurred (e.g., a forensic investigator in the event of a cyber-security breach)
- The need to spend time containing the breach or mitigating the risk for data subjects (e.g., by personally contacting a large number of

individuals to advise them about the potential for identity theft and what steps they can take)
- The original risk assessment concluded that the breach fell below the threshold for reporting, but they have now discovered new information they could not have been expected to know at the time, and the new information has changed the risk assessment, making the breach reportable.

Factors that would not be reasonable when considering a delay include:

- Lack of availability of staff to investigate and report the breach, e.g., the DPO was away. (Organisations should have a breach management plan in place which includes what to do if breaches are identified out of hours or when specific staff members are unavailable)
- Deciding to investigate fully, rather than inform the ICO when it is reasonably clear that a breach has occurred.
- The lack of availability of the ICO's breach notification helpline (an online reporting form exists for those who need to report out of hours).

## 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**

Here the organisation should be outlining what steps they have taken in response to the incident, they should be addressing what they plan to do in future to prevent it happening again and the steps they have taken to limit the risk.

What steps is the controller taking to contain the breach, mitigate risk for data subjects and prevent future breaches?

Are the steps the data controller are taking satisfactory? Is there anything else we think the data controller *should* do? Can we address any failings in this regard through advice and guidance, or is the impact on individuals more serious, such that the use of regulatory action would be preferable?

The questions in this section of the report are clear and specific, so if the controller has failed to answer them, or provide adequate information, this may cause concern that the breach has not been acted on quickly. It may be appropriate to contact the controller at the earliest opportunity to raise this as an issue and provide advice about steps that should be taken to mitigate risk.

If the controller has taken action you will need to assess whether these steps seem appropriate, for example, if the controller has identified that identity fraud is possible, and has offered to pay for CIFAS registration, it shows they are acting to assist the data subject by mitigating risk

**Have you told data subjects about the breach?**

Article 58(2)(e) of the GDPR allows the ICO to order the data controller to communicate the personal data breach to the data subject.

If data subjects have not been notified, are we satisfied with the reasons given? Is it reasonable for data subjects not to be told? Are they likely to be exposed to harm if they are not told (for example, they will not be able to take steps to protect themselves if they're not aware)?

If the controller has assessed the risk to data subjects to be high, they should have informed those data subjects in accordance with Article 34 GDPR.

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

Whether or not a data controller has informed other agencies is unlikely to change the outcome of the case in terms of regulatory action, however it may influence what we do next in terms of the sort of advice we provide or whether we require the data controller to provide further information to us. For example, if a controller has lost data as a result of a burglary, has this been reported to the police? If not, why not?

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

You will need to check this section to determine whether the organisation is part of UK GDPR Code of Conduct or Certification Scheme. These cases will be handled differently and have a different process. If you pick up a case where the organisation is part of a scheme, please follow the process when dealing with these cases.

# About you

**Organisation (data controller) name**

Is the data controller known to us? Have they reported similar issues previously? It may be appropriate to check whether they have been given advice in the past, but have failed to act on this, resulting in a recurrence. If the breach is of a serious nature, this may be grounds for further investigation.

Has the data controller been the subject of regulatory action previously? If so, this may mean that the organisation is of greater concern to the ICO. However, this will also depend on the reason for action being taken and the nature of the new incident.

**Registration number**
**If not registered, please give exemption reasons**

Check that the registration is still in date. If the registration number has not been provided, check to see whether the controller is registered with the ICO. If not, and you believe they should be, provide advice about a controller's legal obligation to register and pay the data protection fee, and signpost to the registration self-assessment tool.

**Business sector**

For use when setting the case up on ICE. This could also be useful when sending the sector specific leaflets with the template letter.

---

## Decision to be taken by ICO officer

Taking into account all of the information provided you need to decide whether the case should be:

- Closed immediately (either with the IC templated letter or bespoke closure letter).
- Requires further information from the data controller for an assessment to be made; or
- Referred for investigation to Cyber, Civil or CRIT. Nb; all s.170-173 DPA 2018 cases should be sent to the Criminal Investigations Team for consultation before any final decision is made.

**Cases that can be closed immediately**

Examples of breaches that we could usually be closed immediately are:

- Loss of encrypted devices, where another copy of the data exists, or where it doesn't but this is unlikely to result in serious consequences to the individual.
- Data disclosed to professional parties, where it has been confirmed that the data has been destroyed/deleted e.g., minor disclosures within the NHS.
- Loss/disclosure of data where it would be difficult to identify individuals e.g., ward handover sheets containing limited identifiers.
- Personal data sent to insecure email accounts but with no evidence of compromise (e.g., NHS staff reporting that the nhs.net account was not used)
- The level of detriment for data subjects can be regarded as low, and the data controller has security measures in place.
- The data controller has taken action to mitigate risk and prevention measures are being improved.

**Cases suitable for templated closure**

Cases that are suitable for the templated closure letter are likely to be incidents that are low level. You will also need to consider whether there is anything outstanding that we would need to recommend to the controller. If it looks like the DC are doing all the can and there is nothing further to recommend this could also be suitable for a templated closure.

NB – It may also be possible to add in another recommendation to the template if there is minor guidance outstanding.

**Cases suitable for immediate closure – bespoke letter**

Considering the information provided by the controller, does this appear to be something they are taking seriously and trying to put right. You should be looking at what should have prevented this, and whether they are taking the appropriate steps to address the incident, prevent a reoccurrence and limit the risk.

Cases that are suitable for closure but not with a template would be cases that require some further bespoke advice. Consider whether the controller would benefit from a bespoke letter outlining some guidance for breach prevention in future or steps they should be taking to limit risk. These cases could be a little more complex, from an organisation with limited data protection knowledge, or are low level but need further guidance.

**Cases where further information is required**

If there is insufficient information to make an assessment you should contact the data controller to request additional information. Try and be

robust with your decisions as to whether further information is needed. Think about whether the missing information is something we could add as a recommendation to the controller in a closure letter.

Where appropriate, this can be done by telephone and recorded on a telephone file note which should be added to the case. Always ensure necessary security checks are carried out before disclosing any information by telephone.

If you are unable to contact the reporter by telephone, or it is not appropriate to do so, you should send a request for further information by email. This must be directed to the reporter and sent to the email address from which the original report was received. List all the information your require and provide an end date by which the response should be provided. The PDB team usually ask for further information to be provided within 7 days, but consideration should be given to any indication provided by the data controller regarding the length of time their enquiries will take.

Once the follow up response has been received you should re-assess the information provided by the controller to determine which course of action to take.

If a data controller fails to respond to a request for further information, you should make another attempt to contact them and chase this. If a second attempt to obtain the information fails, refer the matter to your team manager for advice or possible escalation.

Nb – All the ICO closure letters clearly inform the data controller that the ICO may consider the matter further if we become aware of new information that impacts on our decision.

**Cases suitable for referral for investigation**

Cases that may be suitable for referral to Civil Investigations are those where:

- **Possible regulatory action** - Based on all of the information provided by the data controller, it appears that the criteria for regulatory action may be met. This includes an assessment that
    - the data controller has not taken sufficient action to put the matter right for data subjects; and/or
    - the data controller has not taken sufficient action to prevent a recurrence.
- **Possible high-profile case/strategic file** – The matter is so significant that, regardless of whether an Enforcement outcome is likely to be applied, the ICO should carry out a detailed

investigation into the incident (for example, does the case have the potential to become a high priority investigation?)

- **Complex case** – Taking into account the complexity of the case, it is unlikely that two sets of enquiries (e.g., the initial and follow-up forms) will yield sufficient information to enable a decision to close the case to be made.
- **At the request of the civil investigations team** – Civil Investigations have asked us to refer cases about a particular topic, or from a particular DC to them. E.g., the hot topics list might indicate they want to be assigned all cases by a particular DC.

All enforcement action is considered in line with the ICO's Regulatory Action Policy (RAP). For further information please see - [Regulatory Action Policy (ico.org.uk)]

| Version | Changes made | Date | Made By |
|---|---|---|---|
| 0.1 | First draft | 05 October 2022 | Grace Cullinane |
| 0.2 | Review – minor changes to content made | 06 January 2023 | Victoria Bradshaw |
| 0.3 | Link added for reporting form & Link to RAP added | 10.01.2022 | Grace Cullinane |
| | | | |
| | | | |