

Personal data breaches

At a glance

- The UK GDPR introduces a duty on all organisations to report certain personal data breaches to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority or the affected individuals, or both.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Checklists

Preparing for a personal data breach

- We know how to recognise a personal data breach.
- We understand that a personal data breach isn't only about loss or theft of personal data.
- We have prepared a response plan for addressing any personal data breaches that occur.
- We have allocated responsibility for managing breaches to a dedicated person or team.
- Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach

- We have in place a process to assess the likely risk to individuals as a result of a breach.
- We have a process to inform affected individuals about a breach when their rights and freedoms are at high risk.
- We know we must inform affected individuals without undue delay.
- We know who is the relevant supervisory authority for our processing activities.

- We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.
- We know what information we must give the ICO about a breach.
- We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.
- We document all breaches, even if they don't all need to be reported.

In brief

- [What is a personal data breach?](#)
- [Risk-assessing data breaches](#)
- [When do we need to tell individuals about a breach?](#)
- [What information must we provide to individuals when telling them about a breach?](#)
- [What breaches do we need to notify the ICO about?](#)
- [What role do processors have?](#)
- [How much time do we have to report a breach?](#)
- [What information must a breach notification to the ICO contain?](#)
- [What if we don't have all the required information available yet?](#)
- [How do we notify a breach to the ICO?](#)
- [Does the UK GDPR require us to take any other steps in response to a breach?](#)
- [What else should we take into account?](#)
- [What happens if we fail to notify the ICO of all notifiable breaches?](#)

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;

- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Risk-assessing data breaches

Recital 87 of the UK GDPR says that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

Remember, the focus of risk regarding breach reporting is on the potential negative consequences for individuals. Recital 85 of the UK GDPR explains that:



“A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.”

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

Example

The theft of a customer database, whose data may be used to commit identity fraud, would need to be notified, given its likely impact on those individuals who could suffer financial loss or other consequences. But you would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of a staff telephone list.

So, on becoming aware of a breach, you should contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

For more details about assessing risk, please see section IV of the Article 29 Working Party guidelines on personal data breach notification.

When do we need to tell individuals about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the UK GDPR says you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means the requirement to inform individuals is higher than for notifying the ICO. Again, you will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effect of a breach.

Example

- A hospital suffers a breach that results in accidental disclosure of patient records. There is likely to be a significant impact on the affected individuals because of the sensitivity of the data and their confidential medical details becoming known to others. This is likely to result in a high risk to their rights and freedoms, so they would need to be informed about the breach.
- A university experiences a breach when a member of staff accidentally deletes a record of alumni contact details. The details are later re-created from a backup. This is unlikely to result in a high risk to the rights and freedoms of those individuals. They don't need to be informed about the breach.
- A medical professional sends incorrect medical records to another professional. They inform the sender immediately and delete the information securely. This is unlikely to result in a risk to the rights and freedoms of the individual. They don't need to be informed about the breach.

If you decide not to notify individuals, you will still need to notify the ICO unless you can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. You should also remember that the ICO has the power to compel you to inform affected individuals if we consider there is a high risk. In any event, you should document your decision-making process in line with the requirements of the accountability principle.

What information must we provide to individuals when telling them about a breach?

You need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of any data protection officer you have, or other contact point where more information can be obtained;

- a description of the likely consequences of the personal data breach; and
- a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

If possible, you should give specific and clear advice to individuals on the steps they can take to protect themselves, and what you are willing to do to help them. Depending on the circumstances, this may include such things as:

- forcing a password reset;
- advising individuals to use strong, unique passwords; and
- telling them to look out for phishing emails or fraudulent activity on their accounts.

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, you need to establish the likelihood of the risk to people's rights and freedoms. If a risk is likely, you must notify the ICO; if a risk is unlikely, you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

What role do processors have?

If your organisation uses a data processor, and this processor suffers a breach, then under Article 33(2) it must inform you without undue delay as soon as it becomes aware.

Example

Your organisation (the controller) contracts an IT services firm (the processor) to archive and store customer records. The IT firm detects an attack on its network that results in personal data about its clients being unlawfully accessed. As this is a personal data breach, the IT firm promptly notifies you that the breach has taken place. You in turn notify the ICO, if reportable.

This requirement allows you to take steps to address the breach and meet your breach-reporting obligations under the UK GDPR.

If you use a processor, the requirements on breach reporting should be detailed in the contract between you and your processor, as required under Article 28. For more details about contracts, please see our draft [UK GDPR guidance on contracts and liabilities between controllers and processors](#).

How much time do we have to report a breach?

You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

Section II of the Article 29 Working Party Guidelines on personal data breach notification gives more details

of when a controller can be considered to have 'become aware' of a breach.

What information must a breach notification to the ICO contain?

When reporting a breach, the UK GDPR says you must provide:

- a description of the nature of the personal data breach including, where possible:
 - the categories and approximate number of individuals concerned; and
 - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

What if we don't have all the required information available yet?

The UK GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So its Article 33(4) allows you to provide the required information in phases, as long as this is done without undue further delay.

However, we expect controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. You must still notify us of the breach when you become aware of it, and submit further information as soon as possible. If you know you won't be able to provide full details within 72 hours, it is a good idea to explain the delay to us and tell us when you expect to submit more information.

Example

You detect an intrusion into your network and become aware that files containing personal data have been accessed, but you don't know how the attacker gained entry, to what extent that data was accessed, or whether the attacker also copied the data from your system.

You notify the ICO within 72 hours of becoming aware of the breach, explaining that you don't yet have all the relevant details, but that you expect to have the results of your investigation within a few days. Once your investigation uncovers details about the incident, you give the ICO more information about the breach without delay.

How do we notify a breach to the ICO?

To notify the ICO of a personal data breach, please see our [pages on reporting a breach](#). These pages include a [self-assessment tool](#) and some [personal data breach examples](#).

Remember, a breach affecting individuals in EEA countries will engage the EU GDPR. This means that as

part of your breach response plan, you should establish which European data protection agency would be your lead supervisory authority for the processing activities that have been subject to the breach. For more guidance on determining who your lead authority is, please see the Article 29 Working Party [guidance on identifying your lead authority](#).

Does the UK GDPR require us to take any other steps in response to a breach?

You should ensure that you record all breaches, regardless of whether or not they need to be reported to the ICO.

Article 33(5) requires you to document the facts regarding the breach, its effects and the remedial action taken. This is part of your overall obligation to comply with the accountability principle, and allows us to verify your organisation's compliance with its notification duties under the UK GDPR.

As with any security incident, you should investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented. Human error is the leading cause of reported data breaches. To reduce the risk of this, consider:

- mandatory data protection induction and refresher training;
- support and supervising until employees are proficient in their role.
- updating policies and procedures for employees should feel able to report incidents of near misses;
- working to a principle of "check twice, send once";
- implementing a culture of trust – employees should feel able to report incidents of near misses;
- investigating the root causes of breaches and near misses; and
- protecting your employees and the personal data you are responsible for. This could include:
 - Restricting access and auditing systems, or
 - Implementing technical and organisational measures, eg disabling autofill.

As mentioned previously, as part of your breach management process you should undertake a risk assessment and have an appropriate risk assessment matrix to help you manage breaches on a day-to-day basis. This will help you to assess the impact of breaches and meet your reporting and recording requirements. This will provide a basis for your breach policy and help you demonstrate your accountability as a data controller.

What else should we take into account?

The following aren't specific UK GDPR requirements regarding breaches, but you should take them into account when you've experienced a breach.

As a result of a breach an organisation may experience a higher volume of data protection requests or complaints, particularly in relation to access requests and erasure. You should have a contingency plan in place to deal with the possibility of this. It is important that you continue to deal with those requests and complaints, alongside any other work that has been generated as a result of the breach. You should also consider how you might manage the impact to individuals, including explaining how they may pursue compensation should the situation warrant it.

It is important to be aware that you may have additional notification obligations under other laws if you

experience a personal data breach. For example:

- If you are a communications service provider, you must notify the ICO of any personal data breach within 24 hours under the Privacy and Electronic Communications Regulations (PECR). You should use our PECR breach notification form, rather than the GDPR process. Please see our [pages on PECR](#) for more details.
- If you are a UK trust service provider, you must notify the ICO of a security breach that may include a personal data breach within 24 hours under the Electronic Identification and Trust Services (eIDAS) Regulation. You can use our [eIDAS breach notification form](#) or the GDPR breach-reporting process. However, if you report it to us under the UK GDPR, this still must be done within 24 hours. Please read our [Guide to eIDAS](#) for more information.
- If your organisation is an operator of essential services or a digital service provider, you will have incident-reporting obligations under the [NIS Directive](#). These are separate from personal data breach notification under the UK GDPR. If you suffer an incident that's also a personal data breach, you will still need to report it to the ICO separately, and you should use the GDPR process for doing so.

You may also need to consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

The European Data Protection Board, which has replaced the WP29, has endorsed the [WP29 Guidelines on Personal Data Breach Notification](#). Although the UK has left the EU, these guidelines continue to be relevant. You should also be aware of any recommendations issued under relevant codes of conduct or sector-specific requirements that your organisation may be subject to.

What happens if we fail to notify the ICO of all notifiable breaches?

Failing to notify the ICO of a breach when required to do so can result in a heavy fine of up to £8.7 million or 2 per cent of your global turnover. The fine can be combined with the ICO's other corrective powers under Article 58. It is important to make sure you have a robust breach-reporting process in place to ensure you detect, and notify breaches, on time and to provide the necessary details, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects. If you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

Further Reading

[External link](#) Relevant provisions in the UK GDPR - See Articles 33, 34, 58, 83 and Recitals 75, 85-88

External link

In more detail – ICO guidance


See the following sections of the Guide to the UK GDPR:

- [Security](#)
- [Accountability and governance](#)

GDPR 'in more detail' guidance:

- [UK GDPR guidance on contracts and liabilities between controllers and processors](#)

Existing DPA guidance:

- [Encryption](#)
- [A practical guide to IT security: ideal for the small business](#) 

Other related guidance:




- [Guide to PECR](#)
- [Notification of PECR security breaches](#)
- [Guide to eIDAS](#)

The [Accountability Framework](#) looks at the ICO's expectations in relation to personal data breach response and monitoring.


In more detail – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR. Although the UK has left the EU, these guidelines continue to be relevant.


WP29 published the following guidelines which have been endorsed by the EDPB:

- [Guidelines on personal data breach notification](#) 
- [Guidelines on lead supervisory authorities](#) 
- [Lead supervisory authority FAQ](#) 

In more detail – European Union Agency For Cybersecurity

The European Union Agency for Network and Information Security (ENISA) have published [recommendations for a methodology of the assessment of severity of personal data breaches](#) .

Further Reading

-  [Report a security breach](#)
For organisations