Personal data breaches

At a glance

- The DPA introduces a duty on all data controllers to report personal data breaches to the Ombudsman and the individual(s) whose data was breached. You must do this within 5 days.
- You need to provide the Ombudsman and the individual(s) with certain information, including measures you have taken, and measures you recommend the individual to take.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate your communications with the Ombudsman and the individuals.

Checklist

Preparing for a personal data breach

- We know how to recognize a personal data breach.
- We understand that a personal data breach is not 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 risks to individuals as a result of a breach.
- We know the Ombudsman is the relevant supervisory authority for our processing activities.
- We have a process to notify the Ombudsman and the affected individuals of a breach within 5 days, even if we do not have all the details yet.
- We know what information we must give the Ombudsman and the individuals about a breach.
- We know what information about a breach we must provide to the Ombudsman and affected individuals, including advice to help them protect themselves from its effects.

In brief

- What is a personal data breach?
- What breaches do you need to notify the Ombudsman and affected individuals about?

- What role do processors have?
- How much time do you have to report a breach?
- What information must a breach notification to the Ombudsman and the affected individuals contain?
- What if we don't have all the required information available yet?
- How do you notify a breach to the Ombudsman?
- Are there any breaches I do not need tell the affected individuals about?
- Does the DPA require you to take any other steps in response to a breach?
- What happens if you fail to notify?

What is a personal data breach?

The DPA defines a "personal data breach" as follows:

"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 transmitted, stored or otherwise processed.

Breaches can be the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

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 lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed due to a malfunction of the storage medium.

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 Ombudsman and the individuals that may be affected if there are likely risks that to the rights and freedoms of the individuals

affected.

What breaches do you need to notify the Ombudsman and affected individuals about?

The Ombudsman expects all data breaches to be reported to the Ombudsman and the individual(s) whose data was breached.

A personal data breach may not by itself lead to enforcement action by the Ombudsman. The circumstances of the breach will determine whether an investigation will be launched. A breach notification form can be found on the website of the Ombudsman.

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.

So, on becoming aware of a breach, you should try to 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.

What role do processors have?

If your organisation uses a data processor, and this data processor suffers a reportable breach, then you – as the data controller - must inform the Ombudsman, and the individual(s) concerned, without undue delay and always within the five-day reporting time limit.

Example

Your organisation (the data controller) contracts an IT services firm (the data 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 Ombudsman and the individual(s) concerned.

If you use a data processor, the requirements on breach reporting should be detailed in the contract between you and your data processor, as required under the seventh data protection principle and paragraph 3 of part 2 of Schedule 1.

How much time do you have to report a breach?

You must report a personal data breach to the Ombudsman and the individual(s) concerned without undue delay, but not later than 5 days after you should, with the exercise of due diligence, have been aware of the breach.

In the context of data breaches, due diligence means that you must manage your systems on an ongoing basis and monitor them for any accidental or deliberate destruction, loss, alteration, unauthorised disclosure of or, access to, the personal data you process.

What information must a breach notification to the Ombudsman and the affected individuals contain?

When reporting a breach, the DPA says you must provide a description of:

- the nature of the personal data breach;
- the consequences of the breach;
- the measures proposed or taken by yourself to address the breach; and
- the measures you recommend the individual(s) to take to mitigate the possible adverse effects of the breach.

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

Data controller are expected to prioritize the investigation, give it adequate resources, and expedite it urgently. Nonetheless, it may not always be possible to investigate a breach fully within 5 days to understand exactly what has happened and what needs to be done to mitigate it.

If so, you should provide the additional information as soon as possible without undue further delay.

If you cannot provide full details within 5 days, it is a good idea to explain the delay to the Ombudsman 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 Ombudsman and individuals within 5 days 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 Ombudsman and the individuals more information about the breach without delay.

How do you notify a breach to the Ombudsman?

To notify the Office of the Ombudsman of a personal data breach, please contact us.

Are there any breaches I do not need tell the affected individuals about?

The DPA requires that all personal data breaches are reported to both the Ombudsman and the affected individuals within 5 days.

Example

A hospital suffers a breach that results in an 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. This breach must be reported to the Ombudsman and the individuals concerned.

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 risk to the rights and freedoms of those individuals. This breach does not need to be reported to the Ombudsman and the individuals concerned.

Does the DPA require you to take any other steps in response to a breach?

It is best practice to record all breaches.

As with any security incident, you should investigate whether the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes,

further training or other corrective steps.

What happens if you fail to notify?

Not notifying a breach in time may cause additional damages to the individual's whose data has been breached. This will damage your reputation and undermine the trust individuals have in your business or organisation.

Failing to notify a breach when required to do so is an offence under the DPA and can result in a conviction and a fine of one hundred thousand dollars.

Failing to notify may also be subject to a monetary penalty imposed by the Ombudsman under section 55 of the DPA.

Relevant provisions

Data Protection Act (2021 Revision)

Section 16: Personal data breaches

Further guidance

Article 29 Working Party: Guidelines on personal data breach notification