Data breach – Handling personal data breaches

Darren Isaacs

Deborah Margolis

28th June 2021

You become aware of a personal data breach. This might be the loss, theft, destruction, or alteration of personal data or where there has been unauthorised access to it. It may have been deliberate, or just an accident. What should you do?

Breathe

First, don't panic.

Data Breach Policy

Do you have a data breach policy in place setting out what you should do in this situation? Either way, the following is some helpful guidance for you.

Team

Get together your data breach team. This should include your Data Protection Officer ("DPO") (if you have one), and (depending on your business/the potential size of the problem) your head of HR, head of IT, head of Legal and/or Compliance.

Preliminary investigation/assessment

Of course, you'll want to take immediate steps to recover the data and to determine if you need to notify either the Information Commissioner's Office ("ICO"), the independent authority which enforces data protection obligations in the UK, or the impacted individuals themselves, in line with the strict deadlines imposed by GDPR. In order to do that you should first quickly carry out a preliminary assessment of what has been lost, how it happened and why.

You will need this information to understand whether a data breach has truly occurred, how serious it is, and whether or not you need to notify the ICO or any individuals who are affected.

You do not always need to notify the ICO or the individuals of a personal data breach, but you do need to think about it, make a decision, and record your reasoning process.

Damage Limitation

Take steps to try to limit any ongoing damage, loss or unauthorised use of data. For example, if this data has been leaked by a disgruntled ex-employee, ensure they have no further access to your systems. In complex cases, consider if you need a third-party business to help you with this.

How serious is the data breach and do you need to manage internal or external messaging? If so, if you do not already have one, you may need a communications plan to manage internal communications as well as a PR plan. Note that typically the ICO and individuals should be notified prior to making public statements. Having said this, if breaches become public before you are able to notify them you may need to do so as soon as possible thereafter.

Who must I notify and when?

You need to notify the ICO **unless the breach is unlikely to result in a risk to the rights and freedoms of individuals**. This takes some consideration and analysis – it is best to discuss this with your privacy advisers, as there are a number of factors to take into account.

If you do need to notify the ICO, you must make the notification **without undue delay** and where feasible, within **72 hours** after becoming aware of the breach. You may also have to notify the data subject "without undue delay" (see below for where this will be required).

If the notification to the ICO is not made within 72 hours as required, along with the notification you must notify the ICO of the reasons for the delay.

If you decide you do not need to report the breach, as stated above you need to be able to justify that decision, so you should make sure you document it and should consider taking advice on your decision and you will need to keep a record in any event.

If you have considered these points, but are still unsure whether the breach is likely to result in a risk to the rights and freedoms of data subjects, you should take into account the following factors:

- The type of breach
- The potential harm to the rights and freedoms of data subjects
- The number of individuals involved and how easily they can be identified from the data
- The nature, sensitivity and volume of personal data
- Are there specific characteristics of the individual or the controller which increase the risk?

What must the ICO notification include?

You should include the following information in your notification to the ICO:

- A description of the nature of the personal data breach including, where possible, the categories and approximate number of individuals and personal data records concerned.
- The name and contact details of the DPO (if applicable) or another contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, steps that will be taken to mitigate any possible adverse effects.

If you do not have all of the information, you can provide further information when you have it, but must do so without undue delay.

Here is a link to the notification form.

Do I have to notify the individual of the data breach?

If the data breach is likely to result in a **high risk to the rights and freedoms of data subjects**, normally you must notify the affected data subject or subjects **without undue delay**.

You should use the same factors as the ones you use to decide whether there is a risk requiring you to notify the ICO of the data breach. For example, breach of diversity data is likely to result in a high risk to the individual.

Note that depending on the circumstances, there are some exceptions where you may not need to notify the data subject. This could potentially include where the information is unintelligible due to being encrypted, but these are intended to be very limited exceptions and you should take advice on whether they apply in your situation before relying on them. For example, even if the information is intelligible but you do not have a backup of the data this could negatively impact the individuals triggering notification.

What information needs to be given to individuals?

Where you need to send a breach notification to an individual it must be in plain, easy to understand language and must include the following:

- The name and contact details of the DPO (if you have one – it is not a requirement in the UK) or another contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to address the personal data breach, including, where appropriate, actions taken to mitigate any possible adverse effects.

What if the individual doesn't know their data was being processed?

Normally staff will be aware that you are processing their data, for example, through your privacy notice and data protection policies, as you have a duty to be transparent with data subjects about the processing that you carry out and the reasons for it.

Having said this, there may be situations where the individuals are not aware of the data you are processing. For example, while you are normally required to notify staff of CCTV that is in place there are limited circumstances where you may, subject to having carried out a data privacy impact statement ("DPIA"), be lawfully carrying out covert surveillance. If such information is inadvertently lost or disclosed, you should notify the individual as set out above.

Although not strictly required to do so, in order to get ahead of the issue and allay concerns which the individual is likely to have, it would normally be sensible to also notify them of the reasons for the monitoring and why you felt this was justified (which will be covered in the DPIA that you should have already carried out).

What are the legal risks if I do not comply with the ICO notification obligations?

It is important to comply with the notification requirements. This is because failing to notify a breach when required to do so can ultimately result in fines of up to £8.7 million, or 2% of annual global turnover.

The ICO could also require you to stake additional steps such as requiring the business to notify the data subject of the breach.

Take steps to prevent further breaches

You should consider what you can do to prevent a similar data breach happening in future.

This might typically include considering:

- The technical and security measures in place at the time of the breach and if they need to be updated to limit the risk of this happening again.
- Are staff trained on the security measures? Does that training need to be updated or repeated? When reporting a breach to the ICO, one of the questions is whether the staff member involved in the breach had received data protection training in the two years prior to the breach.
- How effective were the processes that you had in place to deal with data breaches? What processes can you put in place to handle the situation better if a similar incident were to happen in the future?

This guide is for information only and is not legal advice. It reflects the position as of 28 June 2021. For any questions, please get in touch with our data privacy experts Darren Isaacs or Deborah Margolis, or your normal GQ|Littler contact.