Data Breach Protocol – Further Guidance for Data Protection Officer

[***insert organisation name***] is a [***controller/processor***] of personal data. As the [***Data Protection Officer/Data Protection Lead***] for [***insert company name***] it is likely that you been assigned the responsibility of addressing unauthorised or unlawful processing of personal data, or accidental loss, destruction of or damage to personal data.

This note provides further examples and guidance on accountability and record keeping, and on the notification requirements where a potential data breach has occurred. This note should be read in conjunction with our Data Breach Protocol.

Notifying the ICO (or other relevant supervisory body)

- **Who is our relevant supervisory authority?** This depends on where our 'main establishment' is (i.e. where decisions about the purposes and means of processing are taken). For UK organisations this will often be the ICO.

- **Do I need to notify the ICO (or relevant supervisory authority)?**
  You only need to notify the ICO if there has been a data breach **and** that breach is 'likely to result in a risk to the rights and freedoms of individuals'.

  This means that, where there is a data breach, provided that the data cannot be accessed by unauthorised persons then the ICO would not need to be notified. For example, if a securely encrypted device containing personal data was lost, but the encryption key remained in the secure possession of the company along with a backup of the data, then the breach would be unlikely to result in a risk to the rights and freedoms of the data subjects, so the breach would not need to be notified to the ICO.

  If in doubt it is better to err on the side of caution and notify the ICO. There is no penalty for reporting an incident that ultimately transpires not be a breach.

  The flowchart contained in the Annex to this guidance note should assist in identifying whether a breach needs to be notified to the ICO and/or individuals affected.

- **What information do I need to provide to the ICO?**
  When notifying the ICO of a breach you must provide the following information:
  - a description of the nature of the breach including, where possible, the categories of data subjects affected (employees or customers, for example), the categories of personal data records affected (health records, financial details, educational records, for example), and the approximate number of data subjects and data records affected by the breach;
  - the likely consequences of the breach (identity theft, financial loss or fraud, for example);
  - the measures taken or which you propose to take to address the breach; and
  - your name and contact details.

  The above are minimum requirements but it is recommended that you provide as much information as possible when notifying the ICO of a breach. The data breach log should assist in providing the ICO with the necessary information

  Where there are multiple similar breaches you may be able to submit a 'bundled' notification, provided that the breaches relate to the same type of personal data, which has been breached in the same way over a relatively short period of time.

- **When do I need to notify the ICO?**
  A notifiable breach has to be reported to the ICO within 72 hours us becoming aware of the breach. Where you fail to notify the ICO within 72 hours, it should be accompanied by the reasons for the delay.

  The information can be provided in phases if it is not all ascertainable within 72 hours and where precise information is not yet available you can provide an approximation. An example would be where further information is required to establish all of the facts in the event of a complex cybersecurity breach. You must ensure you act in a timely manner and without undue further delay in providing additional information.

  When you provide any subsequent information to the ICO you must provide reasons for the delay, and it is recommended that when you first notify the ICO you should make them aware that further information is likely to follow.

- **When do I 'become aware' of the breach for the purposes of notifying the ICO?**
  You become aware at the point when you have a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

  In some cases this will be clear from the outset, for example if a laptop containing unsecured personal data was lost, the controller becomes 'aware' as soon as it realises that the laptop is missing.

  In other cases, however, it may take time to establish if personal data has been compromised. Where it is not immediately clear you should ensure that steps are taken as soon as possible to investigate whether a breach has occurred. You are permitted a short period of investigation to establish whether or not a breach has occurred and, during this time, you will not be regarded as being 'aware' of the breach.

  It is recommended that you have internal processes in place to be able to detect and address a breach. This may include technical measures such as data analysis and practical measures such as having a reporting procedure in place (which may include our data breach protocol) so that you can be notified as soon as possible of any breach.

<u>Notifying Individuals</u>

- **When do individuals have to be notified directly?**
  You must notify individuals directly where a breach is likely to result in a ***high*** risk to rights and freedoms of the individual. The ICO can also require you to notify individuals.

  You must contact the individuals directly unless doing so would involve a 'disproportionate effort', in which case a public communication is required.

  The notification should be 'dedicated' i.e. you cannot bury the news of the breach in a newsletter or other regular correspondence, and it may be that several methods of communication are appropriate, especially if the breach is severe.

  When contacting individuals you should be wary of using a contact channel that has itself been compromised by the data breach, as there may be a risk the notification could be intercepted.

- **When is a breach considered a 'high risk' to the rights and freedoms of the individual?**
  A breach is high risk where, if left unaddressed, it is likely to have a significant detrimental effect on the individual (resulting in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage, for example).

When notifying the ICO you can obtain advice on whether the affected individuals need to be informed, as well as on the best way to contact the affected individuals.

- **When do I need to notify the individuals?**
  The individuals must be notified 'without undue delay', which means as soon as possible, in order to allow them take steps as soon as possible to protect themselves from the potential consequences of the breach.

- **What information do I need to provide?**
  You must describe in clear and plain language the nature of the breach, and you must provide the same information that you provide to the ICO (see above).

  Where appropriate you should also provide specific advice to individuals to help them protect themselves from possible adverse consequences of the breach, such as resetting passwords.

Are there any circumstances where I don't have to notify individuals?

You do not need to notify individuals who:

- You have applied appropriate technical and organisational measures to protect personal data prior to the breach that renders personal data intelligible to any person who is not authorized to access it.

- Immediately following a breach you have taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise.

- It would involve disproportionate effect to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place.

Examples of data breaches that would require notification

Examples of data breaches that would require notification to the ICO would include:

- A CD with unencrypted data goes missing. Even though it is not certain whether anyone has gained access you would still have to notify the ICO.
- A third party informs you that it has received some personal data relating to one of your customers by mistake.
- Your organisation's computer network is hacked and data that you hold has been compromised.
- You are informed by a customer or third party that they have received an email impersonating your organisation, which nonetheless contains accurate personal information suggesting that your organisation's data security has been compromised.

Notifying the Data Controller

If your company processes data for or on behalf of another company, for example where a company outsources its IT support or marketing to third parties, you have obligations to notify that company (the 'data controller') in the event of a breach.

- **What are my obligations to a company whose data I process?**
  The data controller retains overall responsibility for the protection of personal data, but as a data processor you will often be contractually obliged to assist the controller in complying with its obligations under the GDPR.

This means that if you become aware of a breach of personal data that you are processing for another company, you must notify them 'without undue delay', but it is recommended that you notify them immediately and provide any further information as it become available.

- **Do I notify the ICO and/or the individuals concerned?**
  As a general rule, once you have notified the data controller of a potential breach it is the data controller, not the processor, who will decide whether or not to notify the ICO and/or the individuals concerned.

  An exception to this is where the controller has given you authorisation to do so and this is part of the contract between you and the data controller. Even where this is the case, however, the ultimate legal responsibility remains with the controller.

Consequences of Failing to Report a Breach

Failure to report a breach to either the ICO or the individual(s) concerned could lead to the company facing sanctions under the GDPR.

Where you fail to notify the ICO within 72 hours you must provide reasons for the delay.

If you fail to notify either the ICO and/or the data subjects as appropriate, then you may face a fine of up to €10,000,000 or up to 2% of the total worldwide annual turnover of the company (although it should be noted that any fine imposed by the ICO will be proportionate to the size and nature of the breach, and will take into account the action taken by the controller to mitigate the effects of the breach).

There may also be additional sanctions imposed for the lack of adequate security measures that led to the breach in the first place. These could include a temporary ban on the company processing personal data and withdrawing any certification awarded by an industry certification body.

Accountability and Record Keeping

Regardless of whether or not a breach needs to be notified to the supervisory authority, you must keep documentation of all breaches, and it is recommended that you also document your reasoning for the decisions that are taken in response to any breach. This would include the reasoning for not notifying a breach or any delay in providing notification.

We have provided you with a data breach log for this purpose, which sets out the required details of the breach and measures taken or to be taken in response that you need to record.

Where you notify individuals directly of any breach we recommend that you keep records of who was notified, what they were told and the method(s) of communication.

Finally, we recommend that you are able to show that your employees have been informed of the company's data breach protocol and what to do in the event of a data breach.

Evaluating the Response and Recovery to Prevent Future Breaches

It is possible that your existing procedures could lead to another data breach in future and therefore it is important that following nay breach you identify where improvements can be made.

Consider the following points:

- **Make sure you know what personal data is held and where and how it is stored.**

- **Establish where the biggest risks lie.**

- **Risks will arise when sharing with or disclosing to others.**
  Make sure this method of transmission is secure and you only disclose the minimum amount of data necessary.
- **Identify weak points in your existing security measures.**
  For example, the use of portable storage devices.

- **Monitor staff awareness of security issues and provide training where necessary.**

Further Guidance

Further guidance on data breach notification can be found in the following ICO guidance:

Data breach notification guidanc

and the Article 29 data protection notification policy guidance https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-breaches/

ANNEX

A. Flowchart showing notification requirements