Advice Note on Data breaches and self-reporting

This note focuses on the key legal elements of responding to a breach of personal data security, principally the obligation to notify data protection authorities or data subjects.

The General Data Protection Regulation (**GDPR**) introduces an obligation on all organisations acting as data controllers to report data breaches and losses involving personal data to their relevant supervisory authority e.g. the Information Commissioner's Office (**ICO**) if the breach or loss is likely to result in a risk to individuals' rights and freedoms.

For more detailed guidance please see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/.

1. What is a 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.

Personal data breaches can therefore include:

- access of a database by an unauthorised third party;
- sending personal data to the wrong recipient;
- devices such as USB sticks, laptops or mobiles containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability (even if it is just temporary) of personal data, for example, where there has been a back-up failure.

2. When do you have to report a breach?

All personal data breaches must be recorded if you are a data controller of the relevant personal data, including the facts relating to the personal data breach, the effects of the breach and any remedial action taken in response *(Article 33(5), GDPR)* as data protection authorities may demand the right to inspect these records. However, only certain personal data breaches must be proactively notified to the relevant supervisory body and individuals concerned.

2.1 Supervisory Authority

Notification to the ICO is only triggered where a breach is likely to result in a risk to individuals' rights and freedoms. *(NB: in the case of a breach affecting individuals in different EU countries, the ICO may not be the lead supervisory authority. 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 i.e. you need to know which EEA country any data processors operate in).*

When assessing the risk to individuals, organisations will need to consider the specific circumstances of the breach, including the likelihood, severity and potential impact of the risk. The Article 29 Working Party (**WP29**) (which was set up to provide the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States) recommends considering the following factors when assessing risk:

- Type of breach.
- Nature, sensitivity and volume of personal data.
- How easy it is to identify individuals.

- How severe the consequences are for individuals.
- Special characteristics of the individual (for example, children or other vulnerable individuals may be at greater risk).
- Number of individuals affected.
- Specific characteristics of the data controller (for example a sports organisation processing large amounts of special categories of personal data will pose a greater threat than the mailing list of a club).

Example

The ICO recommends that where there has been theft of a database e.g. for your membership contracts where you hold any payment or bank details for those members, the data of which may be used to commit identity fraud, your members would need to be notified, given the impact this is likely to have on those individuals who could suffer financial loss or other consequences. On the other hand, it suggests that you would not normally need to notify the ICO, for example, about the loss or alteration of a staff telephone list.

2.2 **Individuals**

The requirement to communicate a breach to individuals is triggered where a breach is likely to result in a high risk to their rights and freedoms. The same factors listed above at paragraph 2.1 should be applied in assessing whether notification to individuals is required. WP29 suggests a presumption of high risk to individuals where the personal data involved is special categories of data. In practice, where notification to individuals is required, notification to the relevant supervisory authority will always be required.

Whether individuals should be notified will depend on the circumstances of the breach. For example, a loss of data which can be confirmed as encrypted and where the key has not been compromised, may represent a very low risk, and would not require notification to individuals (or indeed the supervisory authorities). However, even where data is encrypted, if there are no comprehensive backups of the data, then this could have negative consequences for individuals which could require notification (***WP29 Guidelines***).

NB: the ICO has the power to compel you to inform affected individuals if it considers there is a high risk.

Example

If your organisation suffers a breach that results in an accidental disclosure of some of its players'/participants' medical 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.

3. **What information needs to be contained in the notification?**

3.1 **Supervisory authority**

The following information needs to be provided:

3.1.1 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.

3.1.2 The name and contact details of the data protection officer (if applicable) or other contact point where more information can be obtained.

3.1.3 A description of the likely consequences of the personal data breach.

3.1.4 A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, actions taken to mitigate any possible adverse effects.

3.2 Individuals

The following information needs to be provided:

3.2.1 The name and contact details of the data protection officer (if applicable) or other contact point where more information can be obtained.

3.2.2 A description of the likely consequences of the personal data breach.

3.2.3 A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, actions taken to mitigate any possible adverse effects.

In practice, the ICO or other supervisory authority may assist a controller in identifying what information should be communicated to individuals. Dedicated messages to individuals about data breaches should not form part of any press release or other media statement unless there are no other means of contacting the individuals.

4. When does the data breach need to be notified?

4.1 Supervisory Authority

A data controller must notify a data breach to a supervisory authority promptly, and where feasible, not later than 72 hours after having become aware of the breach. According to WP29, a controller is deemed to become aware of a data breach when the controller has "*a reasonable degree of certainty*" that the incident affects personal data.

For example, the 72 hour countdown will start as soon as you realise an unencrypted CD or other removal storage device with personal data has been stolen. Even though you may not understand how the breach has taken place, you will still have a *'reasonable degree of certainty*' that it has taken place. On the other hand, where you need to gather some evidence to establish *'with a reasonable degree of certainty*' that the suspected data breach has occurred, WP29 recognises that you may need a "short period of time" to perform an investigation before the clock starts. Although there is not a set deadline for this preliminary investigation and assessment, actions to investigate should be carried out as soon as you find out about a suspected breach. If you fail to carry out any preliminary investigation (e.g. by ignoring an alert or suspicion that a breach may have occurred) or you don't carry out an investigation promptly, you may be held accountable for a breach of your obligations under Article 32 GDPR ***(WP29 Guidelines).***

It is not clear from the WP29 guidance whether you should still notify if you have reasonable certainty that a breach has taken place, but little information on the risk associated with the breach. However, it is clear that where you are in doubt, you should still make an interim notification in such circumstances until more is known. There will be no penalty for making a notification which ultimately turns out *not* to be a breach, but please be aware that notifying the ICO or such other regulator about a security incident does run the risk of investigation into the adequacy of security measures, even if it turns out that no harm has been done on that particular occasion.

4.2 Individuals

There is no set deadline for notifications to individuals, but this must be done without undue delay and will ultimately depend on the circumstances. For example, where financial information has been lost, the need to mitigate an immediate risk of damage would call for immediate communication to those individuals affected to give them the opportunity to change their passwords, security details etc.

WP29 suggests that normally data subjects will be notified after the supervisory authority, and following advice from such authority, but recognises that this will not always be the case, and importantly, that notifying the authority will not serve as a justification for failure to communicate to data subjects. In other words, don't wait for advice from ICO if the individuals affected are plainly at risk in the meantime.

5. **What if you don't have all of the information available yet?**

If you don't have all the necessary information within 72 hours of when you become aware of the data breach, it is still possible to provide this information in phases, provided further information is provided to the ICO promptly. The presence of this option to notify in stages will make it difficult for any organisation to argue that it is not feasible to make any notification within 72 hours.

6. **What role do your data processors have to play?**

The data controller is solely responsible for making data breach notifications. However, when a data breach has occurred in relation to data processed by a data processor, the processor has an obligation to report the breach to the controller without undue delay after becoming aware of it *(Article 33(2), GDPR).* ***(Please see template data processing agreements, which address how the processor should notify a data breach to the controller).***

WP29 advises that you, as a data controller, will be deemed to become aware of a processor's breach when it communicates the breach to you. In practice, therefore, there is likely to be a permissible time lag between the processer's first awareness, and the time when you must notify the ICO, given that the processer may need to carry out some investigations to establish with reasonable certainty that the breach has occurred and which data controller(s) it effects and you as a data controller may need to perform your own investigation.

7. **What if you fail to report a breach?**

Failing to notify a breach when required to do so could result in administrative fines of up to EUR10 million or 2% of annual global turnover. However, if you fail to take appropriate security measures against data breaches in accordance your obligations under the Accountability principle (Article 5, GDPR) (***See Advice note on Accountability***) you may be subject to fines up to the higher threshold of fines i.e. EUR20 million or 4% of the annual global turnover. It is currently unclear which fine threshold applies for a violation of the information security obligations under the GDPR, but it is possible in some circumstances that failing to implement an appropriate data breach response plan could trigger this higher threshold of fine.

8. **What should you be doing now?**

A personal data breach is a situation when regulatory scrutiny will be applied to your security measures and compliance with Articles 5 and 32 GDPR. Could you have put technical and organisations measures in place which would have prevented the personal data breach? Therefore, good preparation for data breach handling will allow you as a data controller to manage your risk better. The following will give you a good idea of the things to consider now to help you get ready to react to any breach:

8.1 ***Know your data*** – map your data so you know what personal data you are processing, what is used for, what systems are used and where the data is stored. Failure to quickly identify data potentially affected by a breach through ignorance of what is on your systems, is likely to be seen as a big negative in any assessment by the ICO

8.2 ***Data breach management plan -*** put together a comprehensive data breach management plan i.e. who is responsible for the overall management of a breach response, detection, escalation, communications, investigation, and recovery/remediation

8.3 ***External advisors*** – consider whether there is scope for engaging a technical response/ forensic investigation provider to speed up the reaction to a data breach and access to the information needed for notification

8.4 ***Training***- training is essential to support your relevant policies and procedures to ensure that all employees can identify any security breaches and escalate them to appropriate individuals and teams responsible for data breach management

8.5 ***Testing-*** test your systems and procedures to identify and remedy any vulnerabilities

8.6 ***Insurance-*** consider your insurance coverage for potential personal data breaches, particularly in light of the potential fines under GDPR although in the UK it is generally not possible to insure against a fine, only the costs of dealing with an incident and the costs of any proceedings or appeal

8.7 ***Monitoring –*** establish a routine of regular system testing, updated and refresher training for current and new staff/volunteers and a regular review of any identified breaches to see whether they highlight the need for procedural changes