Euro-toques Ireland: Personal Data Breach Response Plan

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 transmitted, stored or otherwise processed.

Internal notification

Any employee who becomes aware of an actual or suspected personal data breach or that data has been placed at risk is to notify the company Data Protection Officer (DPO) without delay. This includes a notification received by an employee from any processor or director of Euro-toques Ireland of any such incident.

The communication to the DPO is to be made by telephone or in person. Email is not acceptable as reported incidents must be responded to promptly. The employee must ensure that the DPO receives the information. If the employee does not succeed in contacting the DPO, he/she is to contact the Office of the Commisssioner General, the financial directors of the organisation, in that order, without delay.

Communication is to be by the same means as described above.

Assessment of situation

An assessment into the circumstances of the reported breach will commence as soon as possible. The scale of an assessment will be influenced by the extent suggested by the situation. Normally, the assessment team will include the Head of Community and the Commissioner General and the DPO. Other employees/contractors may join the assessment team depending on the circumstances. For example: The IT company may join the investigating team if electronic data is implicated.

The DPO will advise the assessment team. The assessment team will determine:

- Whether a breach has occurred
- The nature of the personal data involved (including whether it includes special categories of personal data)

- The cause of the breach
- Establish whether there is anything that can be done to recover a loss or contain further loss. This may involve engaging the services of contractors/processors;
- The number of individuals who are affected
- The potential risk to affected individuals.
- The results of the aforementioned assessment will determine what notifications and further actions are required, if any.
- Complex, large-scale breaches will require thorough investigation. An Garda Síochána will be notified in cases involving criminal activity. Notifying a personal data breach to the Data Protection Commission (DPC) Controllers have a mandatory obligation to report data breaches to their supervisory authority (the DPC in Ireland) within 72 hours of becoming 'aware' of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. An example of an incident that does not require reporting might be where personal data is already publicly available.

When Eurotoques notifies a breach to the DPC, it should fill in the required Breach Notification Form on the DPC website.

In the event that Eurotoques Ireland informs data subjects of a data breach, the most appropriate method will depend on the circumstances. In general, data subjects must be contacted by some personally directed method rather than a general public notice. Notification may be by telephone call, SMS, email or letter.

When notifying data subjects of a breach, the controller should provide the following information, at least:

- A description of the nature of the breach;
- The name and contact details of the DPO or other contact point;
- A description of the likely consequences of the breach;
- A description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects. Where appropriate, specific advice should be given to data subjects to protect themselves from possible adverse consequences of the breach, such as resetting passwords where access credentials have been compromised.

Eurotoques will maintain a register of any breaches that occur.