WILLIAM FRY

// PRIVACY SOURCE

Personal Data Breach Notification under the GDPR

The Article 29 Working Party (now called the European Data Protection Board ("EDPB")) has published guidelines on the requirement under the GDPR for breaches of personal data to be notified to the competent supervisory authority and, in certain circumstances, to be notified to the individuals whose personal data have been affected. Organisations would do well to heed the guidelines. A controller who fails to notify could be subject to an administrative fine of up to €10m or up to 2% of worldwide turnover.

Personal Data Breach

Controllers are obliged to notify in the event of a personal data breach, a concept defined in Article 4(12) as:

> *"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."*

Article 33 – Notification to the Supervisory Authority

The obligation to notify the supervisory authority is set out in Article 33, which states that:

> *"In the case of a personal data breach, the controller shall, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."*

The EDPB guidance expands on when a controller should be considered 'aware' for the purpose of Article 33*: "when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised."* As it may take time for a controller to establish whether a breach has occurred, the controller will not be regarded as being aware during the period of investigation, but there is an emphasis on promptness: in beginning the investigation as soon as possible, in determining whether a breach has occurred and, if so, in taking remedial action and notifying the supervisory authority within 72 hours of becoming aware. Failing to act in a timely manner could be considered a failure to notify.

The guidelines outline the internal processes controllers should have in place for detecting and addressing breaches. The process should cover the following:

- Controller organisations should appoint a person(s) with the responsibility of investigating all security-related incidents. All information concerning such incidents should be directed to such persons.
- The responsible person(s) should investigate any security-related incident and establish whether it constitutes a breach of personal data.
- If it does, the responsible persons should assess the risk the breach poses to the individuals concerned.
- If the risk is sufficiently high, then the supervisory authority and if necessary, the individual(s) concerned should be informed of the personal data breach.
- Simultaneously the controller should act to contain and recover the breach.

The Notification

Under Article 33(3) the notification should:

a. *"Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;*
b. *Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;*
c. *Describe the likely consequences of the personal data breach;*
d. *Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."*

The GDPR does not define 'categories' of data subject, but the EDPB interprets it as meaning *"the various types of individuals whose personal data has been affected by a breach*", such as *"children and other vulnerable groups, people with disabilities, employees or customers."*

Where a notification is made more than 72 hours after the controller becoming aware of a personal data breach, it must be accompanied by reasons for the delay. The EDPB states that *"this should not be seen as something that regularly takes place."*

Where a controller detects multiple similar breaches after beginning investigation and before notification, it may take some time to establish the extent and number of the breaches. Rather than notify each breach individually, the controller may instead organise a meaningful notification that represents all the breaches. This is a 'bundled' notification, allowable when the breaches concern the same type of personal data, breached in the same way over a relatively short period of time. It is designed to prevent the notification requirement being overly burdensome in such a situation.

Conditions where Notification is Not Required

Under Article 33 breaches that are *"unlikely to result in a risk to the rights and freedoms of natural persons"* do not require notification to the supervisory authority. For example, if the personal data has been rendered unintelligible to unauthorised parties via state-of-the-art encryption, and the controller holds a copy or backup, the supervisory authority need not be notified because the breach is unlikely to pose a risk to individuals' rights and freedoms.

Controllers should be very careful in relying on encryption to such an extent: they should understand the level of protection it provides and whether it is appropriate to the risks presented, as well as the specifics of how it works. Moreover, the means of encryption may become obsolete over time, so that what is adequate now may not be in a few years.

Processor Obligations

Processors also bear obligations as regards breach notification. If a processor becomes aware of a breach of personal data it is processing on behalf of a controller then it must notify the controller *"without undue delay"* under Article 33(2). The controller will be considered aware as soon as the processor becomes aware. The EDPB advises that this means processors should notify controllers as soon as they discover a breach, providing further information in phases as it becomes available. This is essential so that the controller can meet its requirement to notify the supervisory authority within 72 hours. If the processor provides services to multiple controllers, who are all affected by the same incident, then it must inform all of those controllers.

Article 34 – Notification of the Data Subject

In certain situations the controller will have to notify the individuals affected by the breach as well as the supervisory authority. Article 34 states:

> *"When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."*

Whereas supervisory authorities must be notified *"unless the personal data breach is unlikely to result in a **risk** to the rights and freedoms of natural persons*", the natural persons concerned must only be informed where *"the personal data breach is likely to result in a **high risk** to [their] rights and freedoms."* Thus, there is a higher threshold for notifying data subjects. The EDPB states that the main objective of such notification is to provide the individuals with specific information about steps they should take to protect themselves and that therefore it should be communicated *"as soon as possible."*

Information to be Provided to the Individual

The notification must provide, in clear and plain language, at least:

- a description of the nature of the breach;
- the name and contact details of the data protection officer or other contact point;
- a description of the likely consequences of the breach; and
- 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.

This is only the minimum of information to be provided. In appropriate circumstances the controller should also give individuals specific advice on how to protect themselves from the adverse consequences of a breach, for example, advising data subjects to reset their passwords.

Contacting Individuals

The notification should be communicated directly to the affected data subject unless doing so would involve a "*disproportionate effort*", in which case individuals can be notified by means of a public communication or a similar measure whereby the individuals are informed equally effectively.

The EDPB emphasises that notifications should be communicated in clear, dedicated messages, not sent with other information such as regular updates or newsletters. The EDPB recommends that *"controllers should choose a means that maximizes the chance of properly communicating information to all affected individuals."*

Conditions where Notification is Not Required

Individuals do not need to be notified if any of the following conditions Article 34(3) are met:

- if the controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it, such as encryption; or
- if immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise.

Controllers must be able to demonstrate to the supervisory authority that they can rely on any of these conditions. If a controller decides not to communicate a breach to an individual, a supervisory authority may nevertheless require it to do so if it considers that the breach is likely to result in a high risk to individuals. If the supervisory authority determines that the decision not to notify data subjects is not well founded, it may apply sanctions.

Assessing Risk

The controller's assessment of the level of risk to the rights and freedoms of individuals is the basis on which they decide whether to notify the supervisory authority or the individuals concerned. Accordingly, on learning of a breach, the controller should immediately seek to (i) contain the risk and (ii) assess the risk that could result from it. The EDPB provides guidance on how controllers are to assess risk. Controllers should evaluate the risk on the basis of an objective assessment, considering the specific circumstances of the breach, including its severity and potential impact. The EDPB advises evaluating every breach on the basis of the following criteria:

- **The type of breach** – Different types of breach present different levels of risk. For example, a breach in which personal data is disclosed to unauthorised parties holds greater risk than a breach where personal data is lost and no longer available.
- **The nature, sensitivity and volume of personal data –** The EDPB states that usually the more sensitive the data is, the higher the risk it presents, but that personal data that is already available about the individuals must also be considered. The EDPB surmises that "a combination of personal data is typically more sensitive than a single piece of personal data." They give the example of the accidental disclosure of an identity document, which might be innocuous enough on its own, but in conjunction with other personal data could be used for identity theft.
- **Ease of identification of individuals** – The ease with which a party with access to the compromised data can identify individuals is a vital consideration. Identification of data subjects may be directly or indirectly possible from the breached data. It may depend on the specific context of the breach and the public availability of other identifying details.
- **Severity of consequences for individuals** – This can depend on the nature of the personal data (such as data that might enable identity theft or cause psychological distress, embarrassment or damage to reputation) or on the individuals concerned (such as vulnerable individuals who might be at a greater risk of harm). If the data is wrongly disclosed to parties, what the controller knows about those parties is also important: sending personal data to the wrong department of one's organisation does not present the same risks as disclosing it to parties unknown, or malicious hackers. Duration is also a factor, in that the impact is greater if the consequences are long-term.
- **Special characteristics of the individual –** Some individuals, such as children, may be placed at greater risk by breaches.
- **The number of affected individuals –** Generally, the higher the number of individuals affected, the greater the impact a breach can have, although a breach can be serious even if it affects only one person.
- **Special characteristics of the data controller –** The nature, role and activities of the controller may affect the level of risk to individuals. For example, data processed by a hospital will usually be more sensitive than that of a newspaper mailing list.
- **General points** – The EDPB states that a controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. When in doubt, a controller should err on the side of caution and notify.

Accountability and Record Keeping

Accountability is one of the fundamental principles of the GDPR. This is reflected in the Article 33(5) obligation that:

> *"The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."*

Controllers are required to maintain an internal register of all breaches, even those they are not required to notify supervisory authorities and individuals of. The controller should record:

- the particulars of how the breach happened;
- the causes of the breach;
- the personal data affected by the breach;
- the effects and consequences of the breach; and
- the remedial action taken by the controller.

The EDPB also recommends that controllers document the reasoning behind decisions taken in response to a breach. This is especially important in relation to a decision not to notify a supervisory authority or individuals of a breach, in which case the controller should document clearly why it considers the breach unlikely to result in a risk to the rights and freedoms of individuals.

Controllers and processors should have a documented notification procedure in place setting out the process to follow once a breach has been detected, in particular specifying how to contain, manage and recover the incident, assess risk and notify the breach. The EDPB advises that controllers and processors should be able to demonstrate that they have educated their employees about such a procedure to show compliance with the GDPR.

Possible Consequences

If a controller fails to notify the supervisory authority or the data subjects of a breach despite the requirements of Articles 33 and/or 34 being fulfilled, then the supervisory authority will consider all the corrective measures available to it under Article 58(2), which includes the imposition of an administrative fine of up to €10 million or up to 2% of total worldwide annual turnover. If the failure to notify a breach is deemed to reveal an absence of security measures or inadequacy in the existing security measures under Article 32, then this will be regarded as a separate and additional infringement, also punishable by the full range of Article 58(2) measures, including a separate administrative fine.

Conclusion

It is essential that controllers begin putting in place processes for responding to personal data breaches. Controllers should recognise that time is of the essence in the event of a security incident and be clear on who is responsible for investigating and determining whether it constitutes a personal data breach. Controllers should recognise the higher threshold of risk which necessitates notification to individuals. It is advisable to become familiar with the criteria for evaluating risk as formulated by the EDPB, but one should remember that these are only indicative and that risk must always be judged objectively with regard to all of the circumstances. Furthermore, controllers should observe their obligation to document all personal data breaches and the reasoning underpinning their responses to same.

Contact Us

If you have any queries in relation to this, or would like to know more about our PrivacySource offering, please contact our Partner below, or your usual William Fry contact.

David Cullen
PARTNER
+353 1 639 5202
david.cullen@williamfry.com

Leo Moore
PARTNER
+353 1 639 5152
leo.moore@williamfry.com

John O'Connor
PARTNER
+353 1 639 51823
john.oconnor@williamfry.com

Contact our PrivacySource Team here

Follow us @WFIDEA