BRODIES LLP

PERSONAL DATA BREACH NOTIFICATION UNDER THE GDPR

Under the General Data Protection Regulation, certain personal data breaches must be notified to the relevant supervisory authority (in the UK, the Information Commissioner's Office (ICO)). Organisations may also need to tell affected individuals about a breach.

The Article 29 Working Party (WP29) has issued guidance on when and how breaches should be notified. This handy guide summarises that guidance and explains what constitutes a personal data breach and when it is notifiable.

What is a personal data breach?

A personal data breach is "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". The WP29 identifies three types of personal data breach.

Confidentiality breach	Availability breach	Integrity breach
Where there is an unauthorised or accidental disclosure of, or access to, personal data	Where there is an accidental or unauthorised loss of access to, or destruction of, personal data	An alogrithm makes a decision with no human input

The WP29 takes a broad view of what might constitute a breach. For example, loss of availability following a denial of service attack or power failure, which renders personal data unavailable on a temporary or permanent basis, could fall within the above definition.

When do I have to notify the ICO of a breach?

A breach is reportable under the GDPR unless it is "unlikely" to result in "risk" to the rights and freedoms of individuals.

Where a breach is reportable, controllers must notify the ICO without delay and, where feasible, no later than 72 hours after becoming aware of the breach.

The WP29 considers that a controller will be "aware" when it has "a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised."

The notification should explain:

- The nature of the breach;
- Contact details for the controller's Data Protection Officer ("DPO") or other point of contact;
- A description of the likely consequences; and
- A description of the measures that the controller has taken, or plans to take, to address and mitigate the breach.

Under the GDPR, processors must notify controllers of data breaches "without undue delay". The WP29 takes the view that a controller will become "aware" once the processor has informed it of the personal data breach.

Controllers should therefore have in place appropriate internal processes to detect and address breaches (such as upwards reporting to the appropriate level of management (or DPO if the controller has one)) as well as appropriate arrangements in place with processors.

When and how do I have to contact affected individuals?

Communication of a breach to affected individuals is required only where it is likely to result in a "high risk" to their rights and freedoms.

The communication should be made without undue delay and should include at least:

- The nature of the breach;
- Contact details;
- A description of the likely consequences; and
- The measures that the controller has taken, or plans to take, to address and mitigate the breach.

Where possible, the controller should also provide practical advice to individuals on how to protect themselves from the consequences. Controllers must contact individuals directly (e.g. by email or SMS), unless that would involve disproportionate effort. In that case, a public communication should be used. The message must be accessible in alternative formats and relevant languages. Controllers should take into account any guidance from the ICO and other bodies, such as law enforcement agencies.

How do you assess "risk" and "high risk"?

The WP29 recommends considering the following factors:

- The type of breach – unauthorised access may pose a greater risk than if the data is lost.
- The nature, sensitivity and volume of personal data (e.g. health records or financial data).
- Ease of identification of individuals – was the personal data encrypted?
- Severity of the consequences for individuals.
- Special characteristics of the individual – does it affect children or vulnerable individuals?
- The number of affected individuals.
- Special characteristics of the controller – a breach affecting a hospital will likely give rise to higher risks than the same breach affecting a marketing mailing list.

Do organisations need to keep a record of personal data breaches?

The GDPR requires organisations to maintain a register of all breaches, regardless of whether there is a requirement to notify the ICO of a breach. The register should record:

- The cause of the breach, what happened and what personal data was affected;
- The effects and consequences; and
- The remedial action taken.

If an organisation has a DPO then the DPO should be involved in the breach response from the outset. The DPO's tasks will include cooperating with the ICO and acting as a contact point for affected individuals.

Find out more

You can download the WP29's guidance from its website.

Key contacts

To discuss how the GDPR will impact on your organisation, or how Brodies can assist you with your preparations, please get in touch with a member of Brodies' data protection and information law team.

Grant Campbell
PARTNER
+44 (0)131 656 0115
grant.campbell@brodies.com

Martin Sloan
PARTNER
+44 (0)131 656 0132
martin.sloan@brodies.com

You can follow the latest developments on the GDPR, including the latest guidance from regulators, on our GDPR microsite:
brodies.com/GDPR