QUICK REFERENCE GUIDE

GDPR: Data breach notification

Introduction

Data controllers must report personal data breaches to the Information Commissioner's Office (ICO) no later than 72 hours after becoming aware of the breach (Article 33(1) of the GDPR) if the personal data breach is likely to result in a risk to the rights and freedoms of data subjects. Where that risk is a high one, the controller must also communicate the breach to the data subjects without undue delay (Article 34(1) GDPR).

The European Data Protection Board has endorsed its predecessor's Guidelines for compliance with GDPR on personal data breach notification. A copy of the Article 29 Working Party Guidelines are accessible here:
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Data processors are obliged to notify the relevant controller(s) without undue delay after becoming aware of a personal data breach. There is no need for a processor to assess the likelihood of risk before notification. There may also be contractual considerations over and above the GDPR, both in terms of timescale and content of reporting.

If a decision is made by a controller not to notify the ICO or the data subject, then the controller will need to be able to justify this decision so documenting the reasons for not doing so is essential. The controller must also document in a breach log any breaches, the facts relating to the breach, its effect and any remedial action taken.

SHOOSMITHS

03700 86 30 00
www.shoosmiths.co.uk

What is a personal data breach?

"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 4(12) of the GDPR).

This can include access by an unauthorised party, sending data to an incorrect recipient, computer devices containing personal data being lost or stolen, material system downtime or unauthorised or accidental alteration of personal data. This is commonly referred to as a loss of confidentiality, integrity or availability.

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to a data subject. Such damage could include: identity theft or fraud, financial loss, damage to reputation or loss of confidentiality.

What risk factors should be considered when deciding whether to notify?

The Guidelines recommend consideration of the severity of the potential impact on the rights and freedoms of a data subjects and the likelihood of these occurring. Relevant factors are:

- the type of breach
- the nature, sensitivity and volume of personal data
- ease of identification of individuals
- severity of consequences for individuals
- special characteristics of the individuals e.g. children
- the number of affected individuals
- special characteristics of the controller e.g. a medical organisation.

Examples of personal data breaches:

David is the HR manager in a fruit and veg factory. He mistakenly emails payroll details of 50 employees to a group email address containing 100 customers, rather than to the organisation's accounts team. The email contains the name, payroll number, NI number, salary, pension contributions and bank account details of each employee.

Q: Does this trigger the duty to notify the ICO?

A: Yes

Q: Is notification to the ICO sufficient or should the employer also inform affected employees?

A: As the breach in question affects a reasonably large number of people and relates to highly private information, it is likely to result in a high risk to the rights and freedoms of the relevant employees. As a result, the employer should notify the employees of the breach.

Jane is a solicitor in a large law firm. In sending an invoice to a client, she also accidently attaches a list of all the firm's partners, their areas of specialism, their email addresses and work phone numbers.

Q: Should the law firm report this incident to the ICO as a personal data breach?

A: As this information is likely to be publicly available i.e. on the firm's website, the individuals' LinkedIn pages etc., it is unlikely that there will be a risk to the partners concerned. A view could be taken not to notify the ICO.

What must the notification to the ICO contain?

Article 33(3) of the GDPR states that notice to the ICO must contain details of:

- 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
- the name and contact details of the data protection officer or other contact point where more information can be obtained
- likely consequences of the personal data breach
- 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.

What if not all the information is available?

If it is not possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it, a controller may provide the information in phases, but this must be done without undue further delay.

Controllers are expected to prioritise the investigation, give it adequate resources, and expedite it urgently. Notification to the ICO of the breach must still be made when the controller becomes aware of it. Any delay should be explained, and the expected timescales for submitting more information should be provided.

What risk factors should be considered when deciding whether to notify?

As well as possible physical, material or non-material damage to individuals and reputational damage to the controller, the ICO has corrective powers which include:

- issuing warnings and reprimands
- specifying how and when the controller or processer must comply with the GDPR
- ordering the controller to communicate a personal data breach to a data subject
- impose a temporary or definitive limitation on processing
- ordering the suspension of data flows to a recipient in a third country or international organisation.

In addition to, or instead of, the above powers, the ICO can impose a fine of up to EUR10 million or 2% of total worldwide annual turnover, whichever is higher (Article 83(4) of the GDPR). However, higher fines can be imposed for breaches of certain GDPR provisions (Article 83(5) of the GDPR), in particular Article 5 which contains the 'integrity and confidentiality' principle whereby organisations must ensure appropriate security of personal data and protect against data breaches. Administrative fines of up to EUR20 million or 4% of total worldwide annual turnover (whichever is higher) can be imposed for such breaches.

We can support you with addressing personal data breaches or notifying the ICO. For further information please contact Shoosmiths' employment and/or data protection teams.

Employment contacts:

Gwynneth Tan
T: +44370 086 8477
E: gwynneth.tan@shoosmiths.co.uk

Stuart Lawrenson
T: +44370 086 6733
E: stuart.lawrenson@shoosmiths.co.uk

Adele Hayfield
T: +44370 086 4226
E: adele.hayfield@shoosmiths.co.uk

Commercial contacts:

Nick Holland
T: +44370 086 8754
E: nick.holland@shoosmiths.co.uk

Anastasia Fowle
T: +44370 086 7052
E: anastasia.fowle@shoosmiths.co.uk