What to do if you have a data breach in the post GDPR world?

By Deborah Margolis - 31 October 2018

You may be forgiven for thinking that now that 25th May has passed that the GDPR panic is over. However, GDPR represents the new way of doing things, with increased scrutiny and new rules for breach notification.

Practically, data breaches are inevitable in businesses, with human error, IT glitches and external hacks being the main culprits for this. The UK's supervisory authority, the ICO witnessed a huge surge in notifications post-GDPR, not necessary because there were more breaches, but because businesses were over reporting: crucially not all breaches need to be notified.

What is a "data breach"?

A data breach is a breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclose of, or access to, personal data transmitted, stored or otherwise processed. This may include a hack where emails or systems are accessed or where personal data are mis-sent to the wrong person.

When do we need to notify the ICO?

The data controller needs to notify the ICO without undue delay and where feasible, not later than 72 hours of becoming aware of it, unless the data breach is unlikely to result in a risk to the rights and freedoms of individuals. This requires a judgment call by the data controller as to whether the breach is likely to result in a risk to the individuals concerned – and if it does not – then notification will not be required.

Businesses can notify the ICO either with a form which is on the ICO's website or by telephone.

When do we need to notify the individuals concerned?

© **2024 GQ|Littler**

There is a higher threshold for notifications to individuals and controllers only need to notify when the breach is likely to result in a high risk (as opposed to a "risk" for notification to the ICO) to the rights and freedoms of individuals. If you do decide that you need to notify the individuals then this should be done without undue delay.

There are some reasons why it might not be helpful to notify individuals of breaches:

- breach fatigue – i.e. that individuals will receive so many notifications about low level breaches so that in the event that they are notified about a serious breach they will not react to it.
- It is also worth considering whether the notification of a breach may actually cause more distress/harm than the actual breach itself.

What practical steps should businesses take?

Given the strict timelines for notification, businesses will need to act quickly and should be prepared for the event that they ever experience a data breach. We would therefore suggest taking the following steps:

- Have a plan ready in case of a breach setting out what steps will be taken and who will take responsibility for investigating the incident. It is also advisable to have template notification letters ready and to have a breach notification letter in place.
- Conduct regular data protection training, not just for HR but also for all of those within the business that process personal data. Whether training has taken place is a question that the ICO ask on their breach notification form.
- Know your contracts – make sure aware of any special notification provisions that you have put in place with clients or customers.
- Remember that businesses need to keep a record of all breaches, not just those that have been notified.

For more information on the topic, keep your eyes peeled for our webinar on the subject of GDPR in six months.

© **2024 GQ|Littler** - Page 2/2