Legal Update

GDPR and Data Breach Notifications: Updated Guidance

Some of the foremost practical challenges posed by the EU's privacy regime, the General Data Protection Regulation (the 'GDPR'), are the obligations pertaining to notifications for data breaches. This primarily arises due to the required timelines for notifications. Fortunately, new guidance has been issued relatively recently by the Data Protection Commissioner in Ireland and the European Data Protection Board to assist data controllers with reporting and managing data breaches (the "Guidance").

Under the GDPR a personal data breach is 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'.

In the event of a relevant data breach the data controller must report the breach to the supervisory authority without undue delay and no later than 72 hours after becoming aware of it. Controllers must provide a reason for any delays. The controller must also notify the data subject without undue delay of relevant data breaches. Data processors also have an obligation to notify the data controller of any breach they become aware of without undue delay. To enable supervisory authorities to verify compliance with the GDPR data breach requirements, controllers are obliged to document all data breaches that occur even where there is no reporting obligation as there is no risk to the fundamental rights and freedoms of the data subject.

The Data Protection Commissioner (the **''DPC''**) published its 2020 annual report in February 2021. The report indicates that the DPC received 6,783 data breach notifications in 2020. Interestingly 110 of these were deemed non breaches as they did not meet the definition of a data breach as defined in the GDPR. The report contains various case studies which may be of assistance to data controllers in deciding whether they are required to report a data breach to the supervisory authority and what measures they should have in place to prevent or mitigate the effects of a data breach. The case studies are also useful as they demonstrate how the DPC approaches various data breach notifications.

The European Data Protection Board (the **''EDPB''**) adopted Guidelines 01/2021 on Examples Regarding Data Breach Notifications on 14 January 2021. These guidelines reflect the common experiences of the EU supervisory authorities since the GDPR became applicable and its aim is to assist data controllers in deciding how to handle data breaches. The Data Protection Working Party published similar guidelines previously and the EDPB's guidelines are intended to complement this. Similar to the DPC'S 2020 report, these guidelines provide case-based guidance on common causes of data breaches.

Both guidelines demonstrate the importance of having effective processes in place to enable data controllers to efficiently respond to any data breach and to mitigate any possible risks to the personal data. The controller should ensure that when required, the supervisory authority is notified of the breach without undue delay and ensure that all data breaches are documented in compliance with the GDPR.

Recommended Action:

It is advisable to review data protection policies and procedures, and in particular the provisions pertaining to notifications for breaches, in light of the Guidance and update them if necessary.

Mark Browne
Partner
Head of Asset Management
and Funds
Email: markbrowne@clerkinlynch.com
Phone: +353 1 611 4400

Eileen Woods
Trainee Solicitor