GDPR in Context: Data Breaches

Background

The General Data Protection Regulation (the "**GDPR**") will come into effect on 25 May 2018. The GDPR will be directly effective in each EU member state, with the aim that the same rules will be applied uniformly within the EU. This marks a shift in the approach to data protection at a European level, which until 25 May 2018 will rely on national implementing legislation in each EU member state.[1]

The period between now and 25 May 2018 is therefore the de facto transition period, during which organisations will need to assess their current approach to data protection, to undertake a gap analysis between that current approach and the requirements under the GDPR, and to implement any changes and improvements which are required to achieve demonstrable compliance with those GDPR requirements.

Overview

At present, outside the electronic communications industry, there is no legally binding obligation under Irish law to notify data breaches to either the Data Protection Commissioner or to any impacted individuals. The Data Protection Commissioner has, however, published a Code of Practice for Data Security Breaches (the "**Code**"), in the expectation that the Code will be followed.

One of the material changes impacting controllers under the GDPR relates to the mandatory notification of data breaches to the relevant supervisory authority, unless the breach is unlikely to result in risk to the rights of individuals, and to affected individuals, where the breach is likely to result in a high risk. These new obligations are integral to the principles of accountability and transparency that run through the GDPR.

Breaches

What constitutes a data breach is broadly defined in the GDPR, and the concept of breach covers more than an unauthorised use or disclosure of personal data. Obvious breach events, such as unauthorised access or disclosure eg, in the event of an IT system hack, or an inadvertent 'fat finger' employee disclosure, are already regularly reported under the Code.

However, under GDPR, any breach of security giving rise to accidental or unlawful destruction, loss or alteration of data (which would likely capture data being irreparably corrupted or accidentally wiped, for example), will need to be assessed to determine whether the mandatory breach notification obligations are triggered. In that regard, the GDPR adopts a risk based approach to notification, so that relatively benign breaches need not be notified to competent supervisory authorities or affected individuals.

---

[1]There will be national implementing legislation with regard to certain elements, in particular the sanctions regime. However, the general principles which govern the processing of personal data by both controllers and processors will apply automatically from 25 May 2018.

Data Breaches

Notifying the competent supervisory authority

The obligation on controllers to notify the competent supervisory authority arises in the case of any personal data breach, unless the breach is unlikely to result in "*a risk*" to the rights and freedoms of individuals.

The GDPR elaborates to a degree as to what might constitute a risk, noting in the recitals that where a breach is not addressed in an appropriate and timely manner, the risks can include a broad range of physical, material and immaterial damage, such as loss of control over personal data, financial loss, identity theft and damage to reputation.

Based on this broad understanding of risk, the notification obligation, with regard to the competent supervisory authority, will likely arise in a substantial number of breach events. However, even where no notifications arise, controllers should document the facts relating to the breach, its effects and any remedial action taken, in a manner that will enable the competent supervisory authority to verify compliance by the controller with its obligations to notify the competent supervisory authority in appropriate circumstances.

Notifying data subjects

As with notification to competent supervisory authorities, a risk based approach has been adopted when it comes to notifying data subjects. Controllers will need to inform data subjects affected by a breach if it is likely to result in a "*high risk*" to their rights and freedoms. This is a notably higher threshold than 'mere' risk in the context of notification to competent supervisory authorities.

Identifying high risk

The GDPR does not lay down a specific threshold as to when a breach causes a "*high risk*"to individuals and their rights. In practical terms, it can mean different things in different circumstances. The methodology of making the assessment, though, is something that can be generally applied.

A controller should begin with a qualitative and quantitative analysis of the nature and volume of the data concerned and the number of affected individuals. Sensitive personal data or information that could be used for identity theft are likely at the higher end of the risk scale, whereas contact details or similar may be at the lower end. Generally the higher the volume of data affected, the higher the level of risk, although this does relate closely to the qualitative analysis.

Having identified the nature and volume of data affected by the security breach, other factors to consider include whether the breach would cause any adverse effects for the individuals concerned and, if so, how likely it is that they will materialise. Relevant here would be whether the impacted data could be used by someone to their benefit or to the detriment of the affected individuals, and how serious or substantial those effects might be.

It should be kept in mind that if a controller determines that a breach does not pose a high risk, the GDPR reserves the right of the competent supervisory authority to override that decision. It is important for the controller, therefore, to be in a position to demonstrate the controller's reasoning in reaching that determination through documentation, as required under GDPR, of the facts relating to the breach, its effects and any remedial action taken.

When to notify

Notifications to competent supervisory authorities need to be made without undue delay, and if not made within 72 hours of the controller becoming aware of the issue, the controller will need to explain the delay. Furthermore, where it is not possible to provide all relevant information at once, it may be provided in phases without undue further delay. This means that controllers will have to consider notifying breaches before they have been able to carry out a full risk assessment, failing which they will need to explain the delay to their competent supervisory authority.

Notifications to data subjects also need to be made without undue delay, but without the 72 hour proviso. However, there are some circumstances in which no notification to individuals will be required, such as where the data has been encrypted, or steps have been taken to ensure that the high risk is no longer likely to materialise.

Data Breaches

The role of processors

While the notification requirements arise from the point at which the controller becomes aware of the breach, the fact that the breach may have arisen at a processor will not provide the controller with much of an excuse for delay. Under the GDPR, processors are subject to a direct obligation to notify controllers of a data breach without undue delay after becoming aware of it, and the GDPR also mandates that processing agreements include provisions obliging a processor to assist its controllers in meeting, inter alia, the breach notification obligations under GDPR. Processors should also note that the GDPR specifies that where a processor infringes the GDPR by determining the purposes and means of processing, it will be treated as a data controller in respect of that processing, and processors should therefore ensure that they engage appropriately with their controllers in the event that they become aware of a breach.

What to notify

A description of the breach will need to be provided with a notification to the competent supervisory authority. The notification needs to include the categories and approximate numbers of impacted individuals, the types and volume of data affected, a description of the likely consequences of the breach and any steps taken to deal with the breach.

Similar details need to be included in notifications to data subjects, with the additional condition that any such notice needs to be expressed in clear and plain language.

Next steps - planning for data security breach notifications

In simple terms, controllers should aim to have a robust breach management and response plan in place by May 2018. Broadly speaking, the plan should deal with breach detection, investigation, reporting and communications.

Even though there is scope for certain breaches not to be notified to the competent supervisory authorities, a plan should be designed for the default position that disclosure will be required. Matters that should be addressed in the plan include:

- the events or circumstances that will constitute a personal data breach in the context of the controller's processing activities and how they may be detected;
- identification of the person who will manage the breach internally and who must be informed of it;
- identification of a suitable resource to quickly ramp up and perform technical forensics (this may be an external technical advisor);
- identification of the steps can be taken to mitigate the breach, such as replicating any affected data and isolating the cause of the breach;
- a communications plan for internal and external communications; and
- the details of the controller's cyber risk insurance policy and the procedure for addressing any notification requirements.

Contacts

Anne-Marie Bohan
PARTNER
D +353 1 232 2212
E anne-marie.bohan@matheson.com

Deirdre Kilroy
PARTNER
D +353 1 232 2231
E deirdre.kilroy@matheson.com

Chris Bollard
PARTNER
D +353 1 232 2273
E chris.bollard@matheson.com

Carina Lawlor
PARTNER
D +353 1 232 2260
E carina.lawlor@matheson.com

Christine Woods
ASSOCIATE
D +353 1 232 2147
E christine.woods@matheson.com

12.101.7