Expert comment

Rob Corbet is a Partner at Arthur Cox and Member of the Examination Board for the Practitioner Certificate in Data Protection — the views expressed are his own

Recent media reports quote the Data Protection Commission ('DPC') as confirming that it received 1,184 personal data breach notifications in the first two months after General Data Protection Regulation ('GDPR') commenced on 25th May 2018. This equates to around 50% of the total breach notices filed in the entire of 2017. While the increased volume is hardly surprising, the compliance burden on controllers and processors is presenting a real operational challenge.

So are all those notifications necessary?

What's a data breach?

For a start, many organisations are misunderstanding what constitutes a reportable data breach. While there are many areas where controllers can fall short of GDPR compliance, only a personal data breach as defined in Article 4(12) of the GDPR comes within the scope of an event which is potentially reportable to the DPC. Most instances of non-compliance can attract a sanction from the DPC under Article 83, or potential civil liability under Article 82, but for the most part, they don't require that the controller/processor proactively present the breach to the potential prosecution/plaintiff.

A personal data breach is only potentially reportable if it constitutes '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'. A key precondition therefore is a 'breach of security'. Having bad security may put you out of compliance with Article 32 of the GDPR, but it does not lead to a reportable event under Article 33 or 34 unless the lack of security has been successfully exploited.

Types of breach

The Article 29 Working Party Guidelines on Breach Notification (the 'Guidelines', copy at www.pdp.ie/docs/1077) which were revised in February 2018 detail the various types of breaches that are in scope, including 'confidentiality breaches', 'integrity breaches' and 'availability breaches'. In each case, they explain what is meant and provide examples.

Risk assessment

Not all personal data breaches are reportable. So, having established whether or not you've suffered a personal data breach, the next consideration is whether or not the breach presents a risk to the rights and freedoms of natural persons under Article 33(1). If this is 'unlikely', then no report to the DPC is required. If it is likely (or more specifically 'not unlikely'), then a report is required to be made by the controller within 72 hours where feasible. If there is likely to be a 'high risk' to the rights and freedoms of natural persons, then a secondary notification to the data subjects concerned is required without undue delay under Article 34(1).

DPC's reporting forms

Curiously, the DPC's online breach notification form for 'national' breaches asks controllers to categorise the seriousness of the breach as 'low', 'medium', 'high' or 'severe'. This is causing some confusion, as it is unclear why the form would invite the reporting of 'low' risk incidents given that they appear to be outside of the scope of reporting under Article 33 in the first place. It may be that the DPC is attempting to differentiate between the likelihood of a risk arising and the level of potential impact to individuals. However controllers are struggling with such additional distinctions when measured against the letter of the GDPR. Similarly, the consequences that arise from a 'high' versus a 'severe' categorisation (and the reasons for the distinction) also remain to be seen, but presumably it is an effort by the DPC to prioritise notices that the controllers themselves have identified as 'severe'.

It is notable also that the current version of the DPC's 'cross border' online breach notification form does not require categorisation of risk in this way. Instead, it requests clarity about the potential impact on affected individuals using the criteria of 'negligible', 'limited', 'significant' or 'maximal'. Again it is unclear why a 'negligible' impact incident would ever require to be included on any reporting form. To be fair to the DPC, there does not appear to be a consistent approach across the EU as to what data must be provided in a breach notice so perhaps the reporting forms might evolve as controllers and regulators alike adapt to the new reality.

Processors

In any event, no risk assessment comes into play in the case of processors. So, if a processor encounters a personal data breach, it must notify the controller without undue delay after becoming aware of the breach. In turn, the controller has to navigate its way through the above risk assessment process.

Awareness

The question then arises as to what constitutes awareness of a reportable breach. This is critical as it starts the clock ticking for the 72 hour reporting obligation which sits on the controller. The Guidelines suggest that awareness happens where there is 'a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised'. Prior to that, the Guidelines afford the controller 'a short period of investigation in order to establish whether or not a breach has in fact occurred'. However, if this reporting period exceeds 72 hours, the report must explain the reasons for the delay under Article 33(1).

Reality

Many examples in the Guidelines are predicated on their being 'clear evidence of a breach' or where 'there is no doubt that [the controller] has become aware'. The only examples where reporting is not required are where it would be arguable that no 'personal data breach' has occurred in the first place. The guidance and examples also consistently err on the side of reporting and, against a backdrop of serious sanctions, controllers are naturally worried about making the right calls. This inevitably leads to over-reporting.

In reality, controllers and processors are faced with any number of cases where reporting appears to be required, yet where little is gained beyond the clogging up of the system. For example, on one interpretation of the GDPR, Guidelines and the DPC forms, each of the following incidents would be reportable to the DPC within 72 hours:

- On the Friday afternoon of a bank holiday weekend, a processor notifies a controller that its systems are down otherwise than for planned maintenance, but the reasons and time for resolution are not yet known. The processor will issue an update as soon as it can.
- A bank receives an email from a customer saying that her spouse has been using her account password and she's worried because they've just had a row.
- A controller is a high profile target for cyberattacks and it can see hundreds of phishing and brute force attacks ongoing at any one time from multiple different sources. These attacks happen on a daily basis. While it is impossible to say that there is no risk of its IT perimeter being compromised, this controller will only introduce mandatory password changes where there is credible evidence of an account being compromised. (In contrast, a less sophisticated controller who has poor IT security standards will not have to report the attack unless and until 'awareness' finally occurs).
- A disgruntled former employee has just posted the name, home address and PPSN of the HR manager on a third party blog site.

Conclusion

The DPC is receiving thousands of data breach reports under GDPR and the figure across all EU data protection supervisory authorities must be likely to hit hundreds of thousands (or more) in the first year. Hopefully an analysis of these reports will enable the Guidelines and associated reporting channels to be further refined so that controllers and processors can operationalise GDPR reporting in a manner that is workable in practice, while still serving the interests of data subjects.

Rob is Chairing the 13th Annual Data Protection Practical Compliance Conference taking place in Dublin on 15th and 16th November 2018.

For further information, visit www.pdp.ie/conferences

Rob Corbet
Partner, Head of Technology & Innovation
Arthur Cox
rob.corbet@arthurcox.com