Evaluating the WP29's recent guidance on data breaches

November 2017

As the implementation date for the General Data Protection Regulation ('GDPR') looms ever closer, the Article 29 Working Party ('WP29') on 3 October 2017 published a guidance document entitled 'Guidelines on Personal data breach notification under Regulation 2016/679' (the 'Guidance') in order to provide clarity on the boundaries and expectations of handling data breach notification under the GDPR. Richard Jeens and Mohan Rao, of Slaughter and May, analyse the WP29's new Guidance.

A version of this article first appeared in the November 2017 edition of Cyber Security Practitioner.

Introduction

The GDPR will come into force on 25 May 2018 and will bring about the most significant shift in the data protection and privacy landscape in probably 20 years. At the heart of the GDPR are enhanced rights for individuals, stricter rules for those that control and process those individuals' personal data and stiffer sanctions for non-compliance with those new rules. The threat of significant fines – of up to 2% of annual worldwide turnover – has grabbed headlines, but the broadening of individuals' rights and the threat of litigation to enforce those rights has also been an important incentive for organisations developing their response to the GDPR.

Arguably this combination of enhanced obligations, potential sanctions and concern for individuals' rights is most acute in the context of a personal data breach. The recently adopted Guidance prepared by the WP29 is therefore welcome. That is particularly so given the introduction in the GDPR of a 72 hour breach notification regime and the extension of obligations to 'data processors' as well as 'data controllers.' Some Member States, such as the Netherlands and Germany, will already be familiar with regimes where notification is obligatory, and many organisations in other countries, particularly in the financial services sector, will in practice be well-versed on the need to notify regulators of significant issues such as a data breach. (Indeed, the Guidelines are clearly modelled on those already used in the Netherlands.) However, for many the Guidance will represent a helpful framework to navigate not only the crisis that is a data breach but also what can (and should) be done in advance to mitigate the associated risks and potential consequences.

This article aims to summarise the key aspects of the Guidance, including what is covered, the approaches to be taken to notifying the relevant supervisory authority and affected individuals, and how this fits with existing best practice and our experience.

Types of breach

The Guidance is clear from the outset that 'breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data.' That is reinforced by the repetition of the approach taken in the WP29's previous

Opinion[1] that breaches can be categorised according to three principles: confidentiality breach (unauthorised access to personal data), availability breach (loss of access or destruction of personal data) and integrity breach (unauthorised alteration of personal data), with, of course, the scope for any individual breach to combine all of these elements. That means the rules on data breaches can apply in a very wide range of circumstances; the 'loss of access' scenario is not currently addressed in detail in the Information Commissioner's Office's ('ICO') guidance[2], for instance, albeit the rising trend in 'ransomware' which prevents access to data has shifted best practice here.

The key first step in determining a controller or processor's obligations therefore is establishing what sort of breach might have occurred. The approach taken by the Guidance is to apply Article 32 (Security of processing) of the GDPR and the assumption that controllers should know what personal data they have – to comply with their secure processing obligations – and what happens to it – to comply with their data breach obligations. This assumption about the availability of information on the data held by a controller is absolutely understandable given the objectives of the GDPR, but can be extremely challenging in the hours immediately following a potential data breach. Nonetheless, the more that is known about the data involved, the easier it will be to work through the obligations in the GDPR and the Guidance, most of which are driven by an assessment of the risk of harm to individuals' rights and freedoms. That assessment is applied differently in the Guidance on Article 33 (Notification of a personal data breach to the supervisory authority) and Article 34 (Communication of a personal data breach to the data subject) of the GDPR, so we address each in turn below.

Notification of a personal data breach to the supervisory authority – Article 33

In the event of a breach, Article 33(1) provides that a controller must notify the relevant supervisory authority 'without undue delay' and, where feasible, within 72 hours of becoming aware of the breach. Only the lead authority has to be notified, albeit the Guidance accepts that controllers may wish to proactively report the incident in other jurisdictions, such as those with affected data subjects. In either case, the key test is when the controller becomes 'aware' of the data breach – something put in sharp focus by the steady stream of news stories about large organisations who have unknowingly suffered significant hacks or data breaches over a period of time.

The Guidance helpfully acknowledges that, while in some cases it may be relatively clear that a breach has occurred, in others it may take time to establish whether personal data has been compromised and, if so, to what extent. While the 72 hour limit may seem daunting, the 'short period' of investigation will be critical in determining what has to be notified and when. For instance, while the Guidance suggests that a ransom demand from a cybercriminal would 'no doubt' amount to being aware of a data breach, experience suggests that the controller will want to investigate a threat actor's claims before assuming the worst.

This initial window is critical in terms of the controller's risk assessment and immediate response, for instance changing customer identification procedures. It can also help establish the tone of the first notification and public messaging, to ensure accurate information is provided and mitigate the scope for criticism for allowing the data breach to happen at all. That said, any investigation should begin as soon as possible and the Guidance is clear that controllers

[1] WP29, Opinion 03/2014 on Personal Data Breach Notification, http://ec.europa.eu/justice/data-protection/ article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[2] See, for example, the ICO's Guidance on data security breach management, https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf

cannot delay becoming 'aware' of a breach simply by not taking steps to verify suspicions.

In keeping with existing best practice, the Guidance also supports a phased notification approach, so that the relevant supervisory authority can be kept up to date as the facts become clearer. The Guidance notes that a delayed notification may be permissible, e.g. when a controller becomes aware of a breach, then in short order discovers additional linked breaches. In this scenario, it makes sense for the controller to hold off and make one 'meaningful' notification, rather than make notification of each breach as it becomes aware of it. Likewise, while emphasising that notification remains the controllers' legal obligation, the Guidance helpfully recommends 'an immediate notification by the processor to the controller' of a data breach, with further information to be provided as it becomes available.

Ultimately, the message is clear: controllers who believe there has been a data breach (within the broad GDPR definition) must notify the relevant supervisory body promptly. There is time for some initial investigation but what can be achieved in that window will depend on the strength of the existing data mapping and monitoring systems, and it will only be in very rare circumstances when no notification is required (e.g. a loss of secure data which is separately backed up).

Communication of a personal data breach to the data subject – Article 34

By contrast, the Guidance on Article 34 makes it clear that the threshold for having to communicate a breach to an affected individual is higher than that for notifying a supervisory authority. At the heart of this is an assessment that there is a 'high risk to the rights and freedoms of natural persons.' This flows through to when data subjects must be notified, what must be communicated and how the message must be delivered. The 'when' is really addressed in Part IV of the Guidance on assessing risk. The key is the combination of the severity of the potential impact on the relevant individuals and the likelihood of that impact arising. The factors specifically addressed in the Guidance are familiar to privacy practitioners and include the nature of the breach (e.g. an external confidentiality breach is worse than a short term availability breach), the nature of the data (e.g. health or financial records or multiple pieces of personal data may be more sensitive), the number of individuals involved and the ease of identifying them, and any special characteristics of the individuals or controller (e.g. a school is likely to have more sensitive data than a newspaper). There are helpful illustrations in Annex 2 of the Guidance but each scenario is likely to be fact-specific.

The Guidance rightly presents this as an assessment based on the actual incident rather than the hypothetical scenarios more common to a data protection impact assessment. However, experience suggests that any risk assessment will very much be a rolling one based on imperfect or evolving facts. The 'what' in any communication must therefore be accurate, both in describing the data breach and assessing the potential consequences. That is consistent with the objective of notifying individuals being to provide them with specific information on what steps they should take to protect themselves. It does not mean that the controller must accept liability for possible harm which is not the result of the data breach itself, albeit it may be advisable for a notification to include suggested steps to mitigate this possible harm.

Finally, the form of any notification must also match the potential risk. Direct contact is the preferred option – and may be the only acceptable route in particularly severe examples such as health critical data – but the Guidance accepts that this may be disproportionate and, in keeping with Article 34(3)(c), accepts that a public communication that is equally effective can be used. Consistent with current best practice, the Guidance gives the useful examples of utilising emails/ SMS for direct messages, or letters/ prominent adverts in print media plus visible banners on the controller's own website for public communication – i.e. using several methods of

communication where one alone may not be effective. It seems clear that, for example, simply emailing notice of the breach to the last known email address on file for an individual may not be sufficient.

However, the concept of 'notification fatigue' is mentioned and the high threshold for disclosure to individuals is meant to avoid individuals being overwhelmed with notifications of 'technical' data breaches where there is little risk of adverse consequences occurring in relation to their data.

Documenting a breach

Consistent with the assumption of proper monitoring of what data is held and the security arrangements for that data, Article 33(5) requires a controller to document any personal data breaches. In a significant step up in expectation, at least from a UK perspective, detailed record keeping will be a standalone requirement under the GDPR.

This can help a controller demonstrate compliance to its supervisory authority, both in terms of substantive behaviour but also having the right procedural framework in place. For instance, the Guidance highlights that it can help to document the reasoning for decisions taken in response to each data breach, even when the decision taken is that notification is not necessary. More practically, the Guidance pushes data controllers to have a documented notification mechanism in place, which sets out the steps to follow once a breach is detected and how to manage it, and recommends that controllers be able to evidence appropriate training for employees on these procedures.

Having clear systems and procedures in place is undoubtedly helpful in the event of a data breach – and consistent with best practice at the moment. However, organisations will also need to be mindful of the risk of litigation or enforcement action following a data breach. That will put a greater emphasis on accuracy of reporting lines, the role of internal and external legal counsel and the care needed when creating or circulating documents (all in a time pressured situation). Overall, though, the Guidance is clear that it may no longer be enough to have a system which works in practice, but necessary to have one which is seen to be effective as well.

Conclusions

The Guidance is a welcome addition to the toolkit needed to handle what is and will continue to be one of the more challenging aspects of data protection and privacy. Notwithstanding the ambition for greater harmonisation across Member States, there remains uncertainty as to how the GDPR will be applied by different supervisory authorities (and of course the extent to which the final Data Protection Bill delivers an 'adequate' privacy regime in the UK). In that regard, hopefully lessons learnt from the Dutch and other notification regimes will be reflected in how the Guidelines are applied, as some of the practical experience there has not yet been picked up in the Guidelines themselves.

Nonetheless, key takeaways from the Guidance include:

- Technical preparation, especially having a clear understanding of what data you control, the security systems in place for that data and adequate monitoring to establish promptly whether there has been a breach;
- Practical preparedness, including having a clear framework for dealing with all types of data breaches;
- Responsiveness and adaptability, to be able to investigate quickly when you have suffered a data breach, to understand what sort of breach it is and to tailor your response to the risks accordingly;
- Communication protocols, both so that the relevant supervisory authorities can be informed promptly, accurately and consistently but also so that potentially affected data subjects can be notified (if needed) on a timely and effective basis, bearing in mind the potential for this to

require large scale communication arrangements; and

- Record keeping and remediation, to record the decision making process accurately at each stage and take steps to address possible issues as they are identified, remaining in each case mindful of the scope for potential investigation, enforcement or litigation.

Most of these points reflect current best practice. However, with the added threat of large fines and potential litigation, the Guidance should act as another part of the roadmap for controllers ahead of the GDPR application date in May 2018.

Richard Jeens
Partner
T +44 (0)20 7090 5281
E richard.jeens@slaughterandmay.com

Mohan Rao
Associate
T +44 (0)20 7090 3827
E mohan.rao@slaughterandmay.com