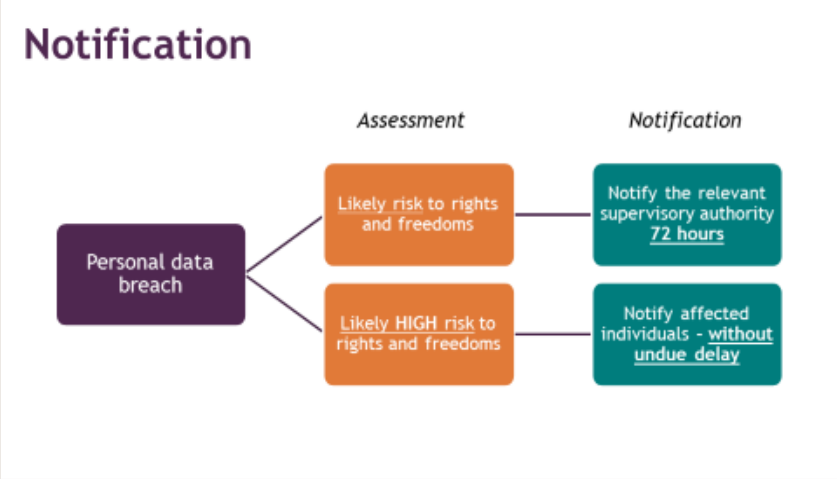
SLAUGHTER AND MAY

Practical aspects of handling data breaches now and post-GDPR

January 2018

A version of this article first appeared in Privacy Laws & Business UK Report, Issue 95 (January 2018).

No one working in the data privacy space will have failed to notice that the number, scale and consequences of data breaches have all increased in recent months. Unsurprisingly this has led to many more 'so what are we doing about it' questions from senior executives. The recent Morrisons' decision[1] and arrival in May 2018 of the GDPR, with its mandatory notification regime and significantly increased monetary sanctions, hardly calm the nerves. However, in our experience, there are a number of technical and practical lessons organisations can take from recent data breaches. Following these should ensure that organisations are as prepared as possible to deal with an unforeseen data breach.



Notification obligations

One of the first questions the legal team is asked when a data breach emerges is who the organisation has to notify and when. That, like so many aspects of dealing with a data breach, will depend on the nature of the breach – for instance, the sensitivity of the data potentially missing or compromised, the nature of the organisation in question, which jurisdictions it operates in and where the potentially affected data subjects are from. However, there is, and will continue to be post-GDPR, a fundamental distinction between notifying regulators and notifying potentially affected data subjects (or other stakeholders).

There is currently no blanket obligation in the UK for an organisation to notify the ICO of a data breach. The ICO recommends that organisations report serious data breaches to it, especially if these involve potential detriment to data subjects.[2] The situation is different under the GDPR as it introduces a mandatory breach notification regime "unless the personal data

[1] *Claimants v Wm Morrisons Supermarket PLC* [2017] EWHC 3113 *Various*
[2] https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf

breach is unlikely to result in a risk to the rights and freedom of natural persons". Moreover, the GDPR's definition of 'data breach' is broad and covers numerous scenarios, ranging from targeted hacker intrusions to temporary loss of access to data. However, drawing on our own recent experience and lessons from the Dutch regime, where a similar duty to report data breaches was introduced in January 2016, in practice regulators are likely to distinguish between temporary access breaches and more substantial confidentiality breaches.

Likewise, there is currently no obligation to notify individuals of breaches affecting their personal data, though the ICO recommends that organisations do so in the event of serious data incidents. Under Article 34 of the GDPR, organisations will be under a duty to inform data subjects 'without undue delay' where the data breach constitutes a high risk to their rights and freedoms. That is clearly a higher threshold for notification than that for notifying regulators in Article 33 – but it is the need for a risk assessment as part of the decision to notify that is key.

The recently adopted guidance prepared by the Article 29 Working Group suggests that, in assessing the level of risk involved, organisations should consider factors such as the nature of the breach, the nature of the compromised data, the number of individuals affected and any special characteristics that may make them more vulnerable.[3] This focus on potential harm to data subjects is consistent with current practices aimed at protecting customers, which in our experience aligns with the approach of other regulators, such as the FCA in the UK or its equivalents globally. In practice, this is one of the key judgment calls for organisations and their advisers to make, both at the outset and as the data breach is investigated.

Although the GDPR introduces important new rules and sanctions, the data breach provisions do not radically depart from current best practice. Organisations that have prepared for a data breach scenario and appreciate internally – both in the legal and wider communications teams – the different rules applicable to regulator and data subject communications should be well placed to handle current and future notification obligations. To that end, the sharp focus and concern about the rush to inform regulators within 72 hours of becoming aware of the breach may be something of a distraction. Rather, organisations can address this by making an initial notification to a regulator about simply the fact that a data breach has occurred, and then keeping the regulator informed as the internal investigation (and wider communications strategy) develops.

A further benefit of making an initial notification of this kind to a regulator (but not to data subjects) is that it mitigates the risk of failing to notify within the prescribed 72 hours, particularly where the regulator takes a different view of when the organisation became "aware" of a data breach. Indeed, whether or not there has in fact been a data breach will not necessarily be clear until further investigation has been done, but initial notification followed by correction/update can help resolve this tension and time pressure.

What to say

However, notifying a regulator and knowing what the notification obligations are only the first steps towards the successful management of a data breach. Knowing what to say is often much more challenging. For most organisations, the heart of any communication strategy is to mitigate the risk of harm to potentially affected data subjects, whether customers, employees or otherwise, and also to emerge from the data breach incident with the organisation's reputation as unscathed as

[3] A link to the WP29 Guidance on data breach notification is available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

possible. These objectives also need to take into account the substantive content requirements of updating relevant regulators (potentially across the globe) and complying with any market announcement obligations.

One key challenge that stands out from our experience is securing the benefits of presenting a coherent narrative in as timely a basis as possible. There are conflicting needs between not committing to a particular cause or set of consequences of the data breach and being clear about an organisation's proactive response. Further pressure in this regard may come from customer comments on social media seeking timely action and an increasing level of transparency from companies when loss of personal data occurs, which will be expressed publicly before an organisation's fact gathering is 'complete'.

Another key challenges is the need to investigate and adapt continually to the changing facts of the situation – particularly difficult given the inevitable 'unknowns' of a data breach situation. A breach may come about due to an internal or external actor; you may be notified by the hacker, by a concerned journalist or by social media; your data may be offered for sale or you may be asked for a ransom. It may not be clear which of these scenarios applies at the outset, so the initial investigation is key to framing the overall narrative.

It becomes even more important to navigate these challenges when considering that the internal and public response to a data breach can be as, if not more, important than the data breach itself. This is because the reputational damage and fallout from being seen to deal with a data breach inadequately is likely to carry longer term consequences for consumer and investor trust. Again, most recently with Equifax and Uber, it is instructive that it is the response of each to the data breach that has been more criticised than the fact of the breach itself.

How to say it

Keeping customers 'on board' is an important part of the external communications strategy during a data breach incident. The communications strategy is best viewed as a "whole package" (including disclosures, customer communications and regulatory notifications), rather than as a combination of distinct one-off announcements. Care should be taken to ensure that legal, IT and management all have a chance to provide input on communications before issued – particularly to ensure consistent information with a consistent level of detail is provided to different stakeholders.

Once the substantive customer communications have begun there can be real benefit in having a well-functioning helpline and accessible FAQs. These can express regret that the incident has occurred and acknowledge the inconvenience that can be caused to customers. However, looking ahead to the risk of claims, a business should resist internal pressure to deliver overly reassuring statements to stakeholders before it is in a position to substantiate them, and it is important to avoid references to distress or damage caused to customers.

There will of course be a distinction between information provided to regulators and that provided to customers. Regulators will inevitably focus on the detail of the breach (and the organisation's substantive response), which will be relevant to their investigation and potential enforcement action. Conversely, customers will want to know how they are affected personally, which may mean individual queries need to be dealt with on a more measured basis and each data subject's position needs to be investigated.

A further consideration in establishing the organisation's narrative is when, and whether, to get police involved. Some organisations express concern about going to the police with sensitive data loss information before it becomes public, as they fear information leaks that could lead them

to lose control over the timing on when to go public.

However, in our experience organisations have a lot to benefit from involving the police at an early stage. It can have a positive effect in demonstrating willingness to external stakeholders to tackle the breach in an open and frank manner. This can support the narrative that the corporate itself is also a victim in a data breach scenario – a narrative that is often lost in the public backlash to announcements of data breach. It is also helpful to demonstrate to relevant regulators that the organisation is taking the matter seriously as, in addition to the business' own investigation, a criminal investigation may take place.

Preparedness

Given the unpredictable nature of a data breach situation, organisations should make every effort possible to arrange plans and processes that will guide a response but allow for adaptability. For instance, it will be easier to handle a data breach if there is an existing governance plan that has been tested, both for practical points such as how to locate alternatives when key individuals are not available and for legal points such as market announcement obligations in different jurisdictions. Any such plan should involve laying out the responsibilities and sign-offs needed for the communications, legal and IT team to interact in putting together and approving external and internal messages.

There are also many practical benefits to having 'dry run' exercises in the organisation to demonstrate how a date breach will be dealt with. Responding to a data breach is often a large coordination challenge between various teams within the business, particularly across multiple jurisdictions or time zones, and it can be helpful to rehearse processes in advance and update the plans with the information gained. In putting together a response plan, many organisations have drawn upon existing 'dawn raid' protocols or experience.

Litigation and Enforcement Risk

The damage to an organisation's reputation or business operations may currently be the most costly aspect of a data breach in the long run. Indeed, the share price of Talktalk has never recovered following its much publicised data breach issues over the last few years. However, the trend towards increased sanctions or claims following on from a data breach is accelerating.

In this regard, the markedly tougher sanctions for non-compliant organisations in the GDPR have caught organisations' attention. While the ICO currently has the power to issue fines of up to £500,000 where organisations are in serious breach of the Data Protection Act ("DPA"), these fines could, under the GDPR's breach notification regime, soar up to 2% of an organisation's total worldwide turnover (for non-compliance with the notification rules) or 4% for more substantive breaches. It remains to be seen how the ICO will use these new fining powers. We anticipate guidance to be published on this next year.

The potential scope of civil liability is also increasing. The recent Morrisons case shows how organisations can face civil claims for damages both in terms of primary liability under the relevant data protection rules (DPA and, shortly, the GDPR) and secondary liability for the acts of employees. Even where the organisation is not the 'data controller' in the acts leading to the data breach, it can have liability for the acts of an employee. Further, this is likely to lead to claims for loss arising from breaches of principle 7 of the DPA or Article 32 of the GDPR, on the basis of the potential gaps in an organisation's data security arrangements highlighted by a data breach.

The vicarious liability aspects of the Morrisons decision are, as the judge himself noted, the most difficult to accept, so this analysis may well change on appeal. Pending that, the importance of having robust technical and human resourcing systems for handling, storing, deleting and allowing access to data is clear.

While the quantum of the damages in the Morrisons case will be determined at a separate trial, cases in recent years have seen an increase in the compensation awarded by the Court. The Court of Appeal notably established in *Google v Vidal-Hall*[4] that distress suffered by a claimant (i.e. without any monetary loss) was a sufficient basis for recovery of damages and the measure of damages for data breach or privacy infringements has gone up. Though both are at the more extreme end, contrast the Mosley[5] case in 2008 where a comparatively small award of £60,000 was made, and the Gulati[6] case in 2015 where between £80,000 and £260,250 was awarded to each claimant.

Conclusion

Organisations should therefore take a holistic approach to preparing for and responding to a data breach. That means taking a joined-up approach to the overall messages and narrative provided to all stakeholders, while recognising the different legal thresholds applicable to the notification obligations (and possible other market announcement or regulatory regimes).

For regulators, that means keeping them informed on a timely and consistent basis. For instance, provide them with daily or weekly updates on progress on all aspects of the breach. This could include information on what the ongoing steps to retrieve/protect the data are, how customers are reacting and what remedial measures are being taken.

For customers or other potentially affected data subjects, there is a balance between expressing regret or empathy with their concerns and avoiding drawing any causal link between the incident and damage or distress suffered. Depending on the volume of affected customers, organisations can consider setting up a helpline or an internet site to keep customers across different jurisdictions informed.

Achieving this – and the resultant benefits in terms of reputation protection and mitigation of the risk of enforcement action and/or civil claims – relies on being joined-up internally. That includes ensuring there is clear leadership in preparing for and responding to a data breach incident, with appropriate input from legal, technical and communications teams and external advisors. Taking practical steps to prepare should give an organisation a solid foundation to build on when forced to handle a data breach.

---

[4] *Google v Vidal-Hall* [2015] EWCA Civ 311
[5] *Mosley v News Group Newspapers Limited* [2008] EWHC 687 (QB)
[6] *Gulati v MGM Ltd* [2015] EWHC 1482

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

Dated January 2018

550023131