New York State Bar Association

Tokyo Conference

Panel 15

The Consequences of a Data Breach under GDPR

Data breaches are complex business events with possible far-reaching financial, reputational and technical consequences

What's this all about?

Making sure that personal data is kept secure is one of the cornerstones of the EU General Data Protection Regulation (GDPR). For more on GDPR see here for a glossary http://www.corderycompliance.com/eu-data-protection-glossary/ and here for some FAQs http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/.

Significantly GDPR introduced two data security breach reporting requirements – reports to a regulator and notifying those affected. GDPR allows a regulator to impose significant sanctions for data breaches – failure to report and late reporting of a data breach to a regulator can also be penalised.

Under GDPR there is also a general right to compensation for damage caused where GDPR has been infringed – this includes where there has been a data breach. Claims for compensation can translate into litigation before the courts, including for a group of people bringing a claim together – these are more popularly called class actions. The reputational damage of a data breach can be significant, notably in the eyes of customers. For publicly listed entities breaches can also mean that their share price suffers.

Managing data breaches is therefore a real compliance imperative. This note highlights some of the possible consequences of a data breach affecting data touching the EU.

Keeping data secure

Those handling personal data (so-called "data controllers" and "data processors") need to introduce appropriate technical and organisational measures (sometimes called "TOMs") to secure personal data. Assessing how to do this will need to take into account the technology that is available, implementation cost, the type of data and how it is being processed. Some of these TOMs could include: systems and processes to make sure the data stays confidential; systems and

processes to make sure that the data can be restored if there is an incident; and, a process for regularly testing and assessing the measures you have put in place.

How you remediate a failure to keep data secure will be all-important in the eyes of a regulator – this may make a big difference in terms of the next steps that a regulator may take investigating the breach and any sanction that the regulator may eventually impose (if any). If there is a data breach the regulator is likely to ask itself if there was any technology which could have prevented the breach. If so, you will have to come up with very strong reasons why this technology was not implemented – saying you did not know about it or did not budget for it even though you could have done so is unlikely to be a defence. You may therefore have to introduce new technology, and quickly – at least one regulator has decided in a case that a financial penalty will apply beyond a certain point for every day that technical measures are not implemented.

Breaches – all shapes and sizes

There is a wide definition of data breach under GDPR – it includes destroying personal data, losing it, altering it or improperly disclosing it. Data in transit or data at rest are also covered. Identifying what actually constitutes a data breach is key – a breach is not limited to lost data, so data beyond reach (for example because of a ransomware attack or a lost encryption key) could also be a breach.

Everyday typical data breaches include losing a laptop or iPhone, sending personal data to the wrong person via email or post, data left in an insecure location such as moving out of an office, leaving information behind on a train, plane or taxi, and personal data wrongly disclosed due to a phishing attack.

Breaches are known to occur in every type of organisation, and regularly. Failure to either identify a breach or to not identify one quickly can result in problems later such as having to explain to a regulator why a breach is reported late. In a worst-case scenario a late report to a regulator risks the imposition of a financial penalty. It's also likely that other measures such as further training will be required.

Reporting – "fessing up"

Under GDPR many data breaches have to be reported to the relevant regulator "without undue delay" and in most cases not later than 72 hours after becoming aware of the breach. Some

organisations will use software tools, like Cordery's Breach Navigator (https://www.corderycompliance.com/solutions/breach-navigator/) to help them take these decisions quickly. In some cases, depending on the scope of the breach, reports may have to be made to several regulators – the logistics of doing this will ratchet up the pressure of reporting within the 72-hour time-limit. Whilst there are some exemptions to the obligation to report these are likely to be limited in practice. Whether you use a tool like Breach Navigator or not to deal with a breach it is important to have some way of recording breaches that you do not report in case a regulator asks to see that log. GDPR also sets out the minimum information that has to be reported – these include the measures taken or proposed to address a breach. Resources have to be marshalled and used in a very short time-span to meet the 72-hour deadline – missing the deadline could result in a financial penalty over and above any penalty for the breach itself, so in extreme cases an organisation could be fined up to 6% of its global annual revenue for having a data breach and failing to report it in a timely manner. For a publicly listed entity the consequences are likely to be even more severe as share price generally drops on the news that a security breach has happened – especially if it has not been managed well within the business.

Data processors have to notify data controllers "without undue delay" after becoming aware of a data breach – tardiness on the part of a processor may impact on the controller reporting to the regulator. One possible consequence of a processor's breach is that a controller will wish to audit the processor, which will result in financial and human resource expense.

Also under GDPR, where a breach is likely to result in *"a high risk to the rights and freedoms of individuals"* the individuals affected have to be told about the breach *"without undue delay"*. Again some exceptions apply. EU regulatory guidance recommends that individuals should be told *"as soon as possible"*. In practice quick notification to those affected is likely to become the norm. Notifying individuals also requires thought and effort – there is no one-size-fits-all solution, for example if there is a risk of identity theft, SMS, email and website notice might all be appropriate if employees are involved.

Sanctions – the big stick

As has been widely publicised, under GDPR a regulator has the power to impose significant fines for GDPR infringements, the highest level being either a maximum of €20 million or 4% of the global annual revenue of an organisation, whichever is the greater – failing to ensure the security of personal data falls within this level. The fines for failure to report a breach to a regulator or

individuals are set at €10m or 2% of global annual turnover. EU regulatory guidance states that if there has been a data breach a regulator can issue fines for the lack of adequate security measures and also for failure to report and notify. GDPR data breach fine cases have been coming through – for more see here: http://www.corderycompliance.com/uk-dpa-to-fine-ba-for-data-breach/ & http://www.corderycompliance.com/ico-intention-to-fine-marriot-99-million-for-data-breach/.

Under GDPR a regulator also has the general power to order an organisation to temporarily or definitively cease processing personal data. However drastic this may sound there is no reason to suppose that this would not be applied to a data breach such as where an organisation has repeatedly committed very significant data breaches. Being ordered to stop processing or transferring data could have greater consequences than any financial penalty – it could effectively close some organisations down.

Compensation – pay up

Under GDPR any person who has suffered *"material or non-material damage"* due to an infringement of GDPR has a right to compensation from the organisation concerned for damage suffered, including where there has been a data breach. Organisations may need to set up compensation schemes to deal with possible claims, including processes to deal with unworthy claims.

Increasingly, class-action litigation (technically called group action or group litigation in the UK) in connection with data protection issues is on the rise. Under class-action litigation individuals with similar grievances can come together against an alleged wrongdoer and in effect act through strength in numbers (sharing advice and documentation etc.) and reduce costs. Various issues may arise, including whether a data controller or processor is exempt from liability, whether there is shared liability, the geographical location for bringing proceedings, any limitations on bringing proceedings such as time-bars and possible insurance coverage. For more on some recent cases see here http://www.corderycompliance.com/vidal-hall-data-protection-class-action-appeal-settled/ and here http://www.corderycompliance.com/client-alert-morrisons-data-breach-litigation-succeeds/. An emerging trend is to see law firms advertising their intention to bring a class-action claim immediately following news of a data breach – in the British Airways case mentioned above class action lawyers reportedly sent a notice of claim within 3 days of the breach becoming public.

Reputation – poor at privacy

Last but by no means least, the reputational damage of a data breach can be significant, notably in

the eyes of both existing and potential customers, along with investors, partners, suppliers and employees. A secondary consequence may be that in the context of a sale the value of an organisation may become diminished.

Jonathan Armstrong
Cordery
Lexis House
30 Farringdon Street
London EC4A 4HH

Office: +44 (0) 20 7075 1784
jonathan.armstrong@corderycompliance.com