The Security Provisions of GDPR

This note is part of Cordery GDPR Navigator.

Technical terms are used in this document which are explained in the Cordery GDPR Navigator glossary. You can find out more about GDPR Navigator at www.bit.ly/gdprnav.

Introduction

The provisions relating to information security continue to be one of the most talked about elements of GDPR. Prior to GDPR coming into force there were already data breach reporting requirements in some countries in the EU (for example in Austria, Germany and the Netherlands) and there were also EU wide data breach reporting obligations for some sectors (e.g. telecoms). GDPR however for the first time introduced universal data breach reporting requirements across the EU.

Some technical terms are used in this note. If you are not sure what these terms mean you can use the glossary which is also part of Cordery GDPR Navigator.

Where are the new rules relating to data security?

Most of the rules relating to data security are contained in four articles of GDPR:

- Article 32: Security of processing
- Articles 33 & 34: Breach notification
- Article 35: Data Protection Impact Assessment (DPIA)

We will look at each of these in turn. You can find these articles quickly using the GDPR Articles Index which is included with Cordery GDPR Navigator. You can find out more details of Cordery GDPR Navigator at www.bit.ly/gdprnav. It is important to say that GDPR is a lengthy document (88 pages including its recitals) and it is not written in the most helpful language. We have simplified some of the terminology in this note. You might want to refer to the full text of GDPR which is more detailed.

In addition to the text of GDPR, on 3 October 2017, the Article 29 Working Party (WP29) published draft guidance on the security breach provisions of GDPR which has now been adopted. This guidance 'Guidelines on Personal data breach notification' is 30 pages long including its Annex. The European Data Protection Board (EDPB), the replacement body of WP29 under GDPR, adopted the WP29 guidance document on 25 May 2018. Whilst the guidance is only guidance and ultimately decisions on interpretation are likely to be taken by the courts, the guidance might be useful in understanding how regulators intend to approach aspects of GDPR.

Making sure that data is secure is one of the cornerstones of the new rules. To do this GDPR introduced two security breach reporting requirements - reports to the regulator and to those affected.

There is wide definition of data breach under GDPR – it will include destroying the data, losing it, altering it or improperly disclosing it. A data breach can include data in transit or data at rest. The WP29 guidance also stresses that whilst there is more to do for data controllers, data processors also have to understand their obligations under GDPR. The WP29 guidance says:

> *"GDPR now makes notification mandatory for all controllers unless a breach is unlikely to result in a risk to the rights and freedoms of individuals. Processors also have an important role to play and they must notify any breach to their controller."*

Article 32 – Security of Processing

Article 32 is the main provision which sets out what companies have to do to make data secure.
In many respects the data security provisions in Article 32 are similar to those in the 1995 Directive and pre-GDPR local law in each of the EU Member States. There is quite a complicated definition of the responsibilities to keep data secure in Article 32 but basically it says that those handling data (data controllers and data processors) need to introduce appropriate technical and organisational measures to secure the data. This assessment will need to take into account the technology that is available, implementation cost, the type of data and how it is being processed.

Article 32 then says that some of these technical and organisational measures 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;
- a process for regularly testing and assessing the measures you have put in place.

In addition organisations should consider their other obligations under GDPR – for example, is it necessary to hold the data in the first place? Does the business know that real data should not be used to test new systems? Is the data out of date? In most cases a DPIA will be useful.

As with similar provisions in the previous data protection law regime (for example Principle 7 of the UK Data Protection Act 1998 (DPA 1998)) the test under Article 32 is likely to be retrospective and objective. This means that if there is a breach the regulators are likely to ask themselves if there was any technology which could have prevented the breach. If so, the company will have to come up with very strong reasons why this technology was not implemented. Saying they did not know about it, or they did not budget for it even though they could have done is unlikely to be a defence. Good security is not just about technology however. We still see a lot of hard copy breaches and these breaches can be the most serious. Simple measures like reducing the hard copy files people carry with them and putting padlocks on bags can reduce risk.

Article 32 also emphasises the need for a process of regularly testing, assessing and evaluating security measures. Again this is similar to existing legislation and codes of conduct issued by data protection regulators – for example the Dutch data protection regulator has said that any data breach plan to be effective has to be tested at regular intervals and improved as necessary.

The Article 32 requirements include both technical and organisational measures – we already know that good information security depends on good people, good processes and good technology. GDPR emphasises that as a legal requirement. It is important to remember that a security breach will not be limited to cases where data has been lost. Ransomware attacks could also be considered as a data breach under GDPR, even if there is no evidence that the data has been accessed. Similarly, losing an encryption key could also be a data breach according to the WP29 guidance. WP29 suggests that it is helpful to categorise breaches in three groups which it defines as follows:

1. a confidentiality breach – where there is an unauthorised or accidental disclosure of or access to personal data;
2. an availability breach – where there is an accidental or unauthorised loss of access to or destruction of personal data – this might include ransomware for example. WP29 says: *"a breach will always be regarded as an availability breach where there has been a permanent loss of, or destruction of, personal data"*; and
3. an integrity breach – where there is an unauthorised or accidental alteration of personal data.

Naturally one incident could be a combination of one or more types of breach.

How might this work in practice?

Whilst obviously there have been no cases yet under GDPR, cases under the existing law show how this might work in practice. For example, in September 2015 the UK DPA (the Information Commissioner's Office or ICO) took action after an airline had a data security incident. This happened when a temporary employee emailed a scanned picture of an individual's passport to his personal email account. The temporary employee had not been trained but he had the same access privileges as permanent employees who had been background checked before being given access to the database. The ICO said that the airline should have put basic checking controls in place and the airline agreed as part of the regulatory settlement to introduce a new policy categorising data and setting out the different levels of security protection which would apply to each category.

In a second example of this type of power in 2014 the ICO took action against The Student Loans Company Limited after a series of data breaches involving customers' records. The ICO determined that proper data breach detection measures were not in place and that its processes meant that more sensitive documents were actually less secure. The organisation was ordered to improve its processes, install new software and implement a new employee training program.

As we've already noted, it is important to remember that a breach is not just limited to lost data. Data beyond reach – for example because of a ransomware attack or a lost encryption key – could also be a security breach. Not every breach of this type would have to be reported, however as the WP29 guidance makes clear:

> *"Therefore, an incident resulting in personal data being made unavailable for a period of time is a security breach (and should be documented), yet depending on the circumstances, it may or may not require notification to the supervisory authority and communication to affected individuals. If the lack of availability of personal data is likely to result in a risk to the rights and freedoms of natural persons, then the controller will need to notify. This will need to be assessed on a case-by-case basis. Furthermore, it should be noted that although a loss of availability of a controller's systems might be only temporary and may not have an impact on individuals, the fact that there has been a network intrusion could still be considered a*

potential confidentiality breach and notification might be required. Therefore, it is important for the controller to consider all possible consequences of a breach".

Article 33 – Breach Notification to the Regulator

Article 33 says that 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. There are some exemptions but these are likely to be limited in practice. As a result, it is of key importance to have a simple to understand security breach plan in place. There's a template plan in GDPR Navigator. The WP29 guidance emphasises this saying:

"The focus of any breach response plan should be on protecting individuals and their personal data… Controllers and processors are therefore encouraged to plan in advance and put in place processes to be able to detect and promptly contain a breach, to assess the risk to individuals, and then to determine whether it is necessary to notify the competent supervisory authority, and to communicate the breach to the individuals concerned where necessary."

There is a separate definition in GDPR of supervisory authority (or DPA). WP29 emphasise in their guidance that the lead regulator mechanism should apply to data breach reporting. However, in some circumstances (especially when the breach is caused by a large data processor), a company may have to make reports to each of the DPAs where individuals reside who are likely to be 'substantially affected' by the breach, as well as the company's lead DPA. This so called "one-stop-shop" system is somewhat complicated and there is a separate note in Cordery GDPR Navigator explaining this regime and how it may work in practice.

Data processors also have to notify data controllers 'without undue delay' after becoming aware of a data breach. The WP29 guidance emphasises this saying "*Processors also have an important role to play and they must notify any breach to their controller*". It is vital that a data controller has a proper contract in place with all of its data processors, including an obligation on the data processor to tell the data controller without delay. WP29 emphasise in their opinion that the 72 hour clock likely starts running when the data processor is aware of the breach, not when the data processor tells the data controller of it, so prompt notification by the data processor is key:

"The controller uses the processor to achieve its purposes; therefore in principle, the controller should be considered as "aware" once the processor has become aware."

Article 33 also lays down what the notification has to include. Again, we could see differences across Europe as some data protection authorities already have their own procedures for notifying a data breach. Local law may also impose additional requirements – for example the UK Data Protection Act 2018 has data breach reporting provisions in sections 67 and 68 of the Act. As a minimum, the type of information that a DPA will want will be:

1. the nature of the breach;
2. the type of breach;
3. the type of data affected e.g. health data, educational records, financial details, bank account numbers, passport details;
4. whether any vulnerable people may have been affected e.g. children – WP29 suggests other vulnerable classes could include "*people with disabilities, employees or customers*";
5. the approximate number of people affected;
6. an approximate number of records affected;
7. the name and contact details of the DPO or another contact point for information;
8. the likely consequences of the breach. The WP29 guidance says that if there is a particular risk of harm e.g. identity theft, that should be identified in the report; and
9. the measures taken or proposed to address the breach.

We have included in GDPR Navigator a specimen data breach report form which might help when gathering that information.

Article 33 also reminds companies that they will need to keep proper records available for inspection. We have also included in GDPR Navigator a template data breach log which might help meet this requirement. Do be aware however, that different data protection authorities seem to want slightly different data so you may want to adapt the data breach log to meet local requirements for those countries where you operate. The WP29 guidance recommends that the log also includes reasoning for the decisions taken in relation to a breach, it says:

> *"In particular, if a breach is not notified, a justification for that decision should be documented. This should include reasons why the controller considers the breach is unlikely to result in a risk to the rights and freedoms of individuals (see Recital 85). Alternatively, if the controller considers that any of the conditions in Article 34(3) are met, then it should be able to provide appropriate proof that this is the case*".

WP29 say that a DPA may exercise its powers under GDPR Article 58 or GDPR Article 83 if a breach is not properly documented.

It will be difficult to make a report within the 72 hour deadline, especially if the report has to be made in different formats to different regulators in different languages. To have a chance of complying businesses will need to be able to detect, report and analyse breaches quickly – ideally in a format that regulators can easily understand. As a minimum it is likely that a business will need systems which:

1. monitor for and detect threats;
2. alert, quarantine, and block attacks and unauthorized activities immediately;
3. identify unusual uses of data;
4. make it easy to flag issues quickly;
5. help work out the sensitivity of the data involved;
6. help produce reports – it may be that different formats are needed for different recipients;
7. be easy to use; and
8. help maintain records in the event of an audit or review since GDPR has wider powers for DPAs here too.

Our experience is, however, that DPAs may be sympathetic if you report what you know rather than wait for a full view of what has gone on. DPAs may permit a cautionary notification whilst you investigate. Both GDPR Article 34(4) and the WP29 guidance also allow for information to be provided in stages. WP29 says:

"Information required for the notification can be provided in phases, but in any event controllers should act on any breach in a timely manner."

It is important to remember that this obligation to report to a data protection regulator can work in parallel to other data breach reporting obligations – for example for financial services businesses and those in the health sector who may have an additional obligation to report a breach. Telecoms and similar companies also have a general data breach reporting requirement under another EU Directive.

How might this work in practice?

A case in April 2016 shows the need to act quickly. In this case EE Limited (a telecoms company) received a call from a customer who said that he thought he had been the victim of identity fraud. EE received the call on 14 January 2016. The customer service representative reported the incident to their line manager by email the same day but they didn't report the matter to EE's internal security team. The line manager came back to the office on 18 January 2016 when he told the security team and they told the ICO. The ICO found that EE had breached a data breach reporting law that already exists for telecoms companies which in some respects is similar to Article 33. The ICO imposed a monetary penalty for failure to make the notification quickly enough.

The ICO took similar action after a breach was reported late by another telecoms operator, TalkTalk. TalkTalk appealed this case but the appeal tribunal upheld the ICO's monetary penalty. You can find out more about this case here - http://www.corderycompliance.com/talktalk-data-breach-notification-appeal-fails/.

Remember that in practice legal privilege is also likely to be a consideration. Later in this note we talk about the potential for civil actions after a data breach, and we have already had examples of civil actions after a breach has been reported. You will need to make sure that your reporting processes and documents are consistent to give you the best chance of asserting privilege. It is likely that, as a result, any investigation should be led by appropriately qualified counsel.

Article 34 – Breach Notification to the Affected Individual

Article 34 contains a second data breach reporting provision; this time to those affected.

The second obligation applies where the breach is likely to result in *"a high risk to the rights and freedoms of individuals"*. Again the individuals affected have to be told about the breach without undue delay but the 72 hour time limit does not appear here. In practice quick reporting to those affected is also likely to become the norm. The WP29 guidance says that individuals should be told "*as soon as possible*" if an Article 34 notification has to be made.

It also emphasises the importance of focusing on individuals saying:

> *"The focus of any breach response plan should be on protecting individuals and their personal data."*

The communication has to be in clear and plain language and the same sort of details will have to be in the communication as are provided to regulators under Article 33. The WP29 guidance stresses the breach notification should be in a separate message just dealing with the breach rather than being bundled into another communication. However, the Article 34 communication is not necessary if:

1. measures like encryption were applied to the data which keep it safe; or
2. the company has taken subsequent measures to protect the data; or
3. it would involve disproportionate effort to contact all of those affected.

If you're relying on the disproportionate effort exemption then there will need to be public communication such as a newspaper advertisement instead. When a company is considering making a report to that effect then it is likely that it will already be in communication with their DPA and the DPA can require a notification to affected individuals to be made in some circumstances.

In appropriate cases our advice would be to consider multiple reporting methods. For example, if there is a risk of identity theft, SMS, email and website notice might be appropriate. Our experience of reporting breaches tells us DPAs will appreciate the extra effort a company makes in these circumstances.

The language in making a report will be key. In a large breach the report is likely to become public, could be published by news media and could be the trigger for a class action. As a result you may want to prepare appropriate specimen notices with your legal team in advance. Do learn lessons from breaches like Expedia too – imposing terms on the release of information to those affected is unlikely to be a good idea.

Article 35 – Data Protection Impact Assessments

In addition to the need to report breaches businesses have to do more under GDPR to stop breaches happening in the first place. Article 32 (which we've looked at already) is part of that but in addition Article 35 introduces a requirement to do a Data Protection Impact Assessment (DPIA) when doing new data processing or using new technologies. DPIAs have been around for some time (they were also called PIAs or Privacy Impact Assessments) but GDPR makes them mandatory in some circumstances. A DPIA is in essence a type of risk assessment of the impact of the anticipated processing activities on the protection of personal data. A data protection regulator will also have to be consulted prior to personal data being processed where an assessment "*shows that the processing would result in a high risk if measures are not taken to reduce that risk.*"

Organisations must set up policies and procedures for undertaking DPIAs but whilst this may at first sight seem to be a compliance burden, its best to consider DPIAs as enabling you to get a better grasp on your data processing and to reduce risk. The DPIA process is likely to include identifying the databases the business uses which hold personal data or sensitive personal data (renamed special categories of personal data in GDPR) and making sure they are secure.

GDPR Navigator has a video on DPIAs with some best practice and tips.

Consequences

Under GDPR, DPAs have the power to impose high fines. Three different bands of fines are applied in relation to three different sets of categories of infringements – the highest level is either a maximum of €20 million or 4% of the global annual turnover of a business, whichever is the greater. The fines for failure to notify a breach are set at €10m or 2% of global annual turnover. WP29's view is that if there has been a security breach a DPA can issue fines both for the lack of adequate

security measures (GDPR Article 32) and for failure to report (GDPR Articles 33 and 34). Their guidance says:

> *"It is also important to bear in mind that in some cases, the failure to notify a breach could reveal either an absence of existing security measures or an inadequacy of the existing security measures. In that case, the supervisory authority will also have the possibility to issue sanctions for failure to notify or communicate the breach (Articles 33 and 34) on the one hand, and absence of (adequate) security measures (Article 32) on the other hand, as they are two separate infringements"*.

When setting the fines the model being adopted is similar to the existing EU competition/anti-trust enforcement regime. In some respects much of the GDPR regime has been inspired by the EU's success in competition law enforcement. From 2012-2016 alone the EU levied fines of around €6 billion. This is an enforcement model that those behind GDPR want to repeat.

There is detailed written guidance on fine determination in GDPR Navigator. An illustration of fines under the current regime set against possible GDPR fines is set out in our review of the ICO's action against HCA in February 2017. Our note on that is below: http://www.corderycompliance.com/client-alert-lessons-for-healthcare-providers-after-ico-enforcement-action-against-hca/.

What about other liability and compensation?

In the US one of the emerging trends we have seen is the rise in class actions following a security breach. It is important to remember that GDPR strengthens the opportunity for people affected by a breach to bring their own proceedings.

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. Important legal issues in this area have been before the courts in the UK case of Vidal-Hall. This case allows for those affected by breaches to get together to claim compensation. There is some background on the Vidal-Hall case here - http://bit.ly/vidalhall.

Because of the extra risk that a data breach may now bring businesses will need to do the maximum to minimise the potential for damages claims.

GDPR Navigator

The following GDPR Navigator resources may help your compliance in this area:

1. The Security Provisions of GDPR film;
2. Data Breach Procedure;
3. Data Breach Report Form;
4. Data Breach Log; and
5. Fine Determination Guidance Note.