Taming the Wild West

Professional standards

01 October 2017

Michael Stout, *Garreth Cameron*, and *Sarah Williamson* consider the impact of the General Data Protection Regulation and how advisers should prepare

Key Points

What is the issue?

Organisations storing personal information have an increased responsibility to protect their systems against data breaches. GDPR provides new opportunities for

cyber criminals.

What does it mean for me?

Nefarious rivals can use HaaS (Hacking as a Service) against competitors to create GDPR violations. Extortionware will likely become a major threat to business after May 2018.

What can I take away?

A system threat analysis should be part of any GDPR implementation plan.

It used to be if a hacker attacked a business and exposed customer details, the greatest loss was a temporary dip in reputational value.

Of course, some companies went out of business, but a number of major internet brands have endured the embarrassment of having customer details stolen due to inadequate information security. Whether it be proprietary technologies or outsourced services, if a company could survive the embarrassment of a data breach, in time and given the right strategy and spin they could turn it around, the hack would fade from the public memory, and they could thrive once again.

Next May, Friday 25 May to be exact, the General Data Protection Regulation (GDPR) comes into full effect. Friday 25 May 2018 is not to be ignored. 25 May 2018 should be repeated ad nauseam to your clients as the introduction date of a new business risk applicable to every European organisation that controllers and processes the information of private individuals.

By the end of April 2018, clients should have a sense of reassurance in their GDPR preparation. Otherwise, they should have fear and take immediate action before it is too late.

The Age of Privacy Rights will not be kind to those who ignore it. No longer can companies and organisations in Europe throw their proverbial hands in the air and say they messed up. Their mess up, their negligence, their lack of safeguards to protect the private details of individuals held in their databases and systems will come at a financial cost. Data breaches aside, not abiding by the GDPR can also destroy a business.

Hopefully, you have heard it before, companies and organisations can be fined the higher €10,000,000 or 2% of global turnover and depending on the violation it could exceed €20,000,000 or 4% of global turnover. GDPR is not something to ignore or delay: 25 May 2018.

From a hacker perspective, nothing changes. The hacker has never cared about the consequences to a target of a successful data breach. They will continue to attack systems. They will not stop exploiting databases and harvesting private details just because of a new law.

In fact, the threat of fines creates new opportunities for hackers to expand their craft of system exploitation.

In the Wild West of Cyberspace, it is not unfeasible for someone to tip off a hacker about the intimate details of a company or organisation's system. A disgruntled employee, contractor, or competitor might post information on the Darknet on a tempting target hoping it will be of interest to a hacker and results in causing the organisation embarrassment and harm in the form of a debilitating GDPR fine.

A more targeted approach would be a competitor hiring the services of a hacker to attack their rivals. Hacking as a Service (HaaS) has been around for a long time. Although the term is relatively new, the idea of hiring a hacker to attack a rival and cause them harm is an old game.

The new game, or attack, is the idea of extortionware. Extortionware is similar to the ransomware attack know as Doxing. A Doxing attack is when a hacker compromises a system and threatens to release private information found on the target system unless the victim makes a payment.

Enter the GDPR twist: imagine a scenario when a hacker gains access to data controller or processor's system. They record their hack as proof of the victim's vulnerability. The also syphon off all customer records from the victim's database.

Instead of going public, they contact the victim and allow them to view the attack and provide some stolen records.

They then make an offer. It is a conservative number to encourage the victim to pay-to-go-away.

- $250,000 in bitcoins in the next 24-hours

- $500,000 in bitcoins in the next 48-hours
- $1,000,000 in bitcoins after 72-hours
- After 96-hours, we send the dossier to the ICO.

Considering an ICO fine in the millions of Euros, $250,000 would undoubtedly be tempting.

I have no doubt cybercriminals are already planning for 25 May 2018. The attack vector of extortionware is surely in the testing phase or already deployed.

In itself, this should be cause for concern to data controllers and processors. Under GDPR, the ICO will not view a data controller or processor as a victim of a cyber attack, but as the responsible negligent party whose action or lack of action allowed the hack to be possible.

The risk to business is no longer merely the embarrassment of having one's system hacked. The consequences of mishandling the private details on individuals carry financial implications that will cause some companies and boards significant discomfort and force others into bankruptcy.

Why organisations should act now to prepare for GDPR

The GDPR is the biggest change to data protection law in a generation. While it builds on the previous legislation, it brings a 21st century approach to the processing of personal data, providing much more protection for consumers, and more privacy considerations for organisations. The GDPR comes into effect on 25 May 2018 in the UK via the Government's Data Protection Bill. So with just under one year to go, there is no time to delay preparing for it.

Consumers and citizens have stronger rights to be informed about how organisations use their personal data under GDPR. They'll have the right to request that personal data be deleted or removed if there's no compelling reason for an organisation to carry on processing it. And they'll have the brand new right to data portability: to obtain and port their personal data for their own purposes across different services.

The GDPR will include new obligations for businesses around consent and data breach reporting. Consent will need to be freely given, specific, informed and unambiguous, and businesses will need to be able to prove they have it if they rely on it for processing data. They'll have to ensure that specific protections are in place for transferring data to countries that haven't been listed by the European Commission as providing adequate protection, like Japan and India.

The ICO will have the power to impose fines much bigger than the £500,000 limit under the current Data Protection Act the maximum being £17 million or 4% of global turnover under the new law. The GDPR gives regulators the power to enforce in the context of accountability too – data protection by design, failure to conduct a data protection impact assessment, DPOs and documentation. The ICO's commitment to guiding, advising and educating organisations about how to comply with the law will not change under the GDPR. We have always preferred the carrot to the stick. We've highlighted a few points for organisations below but our guide –*12 Steps to Take Now* is really the best place to start:

Individuals' rights

One of the main changes for businesses will be the way subject access requests (SARs) are dealt with. Subject access is a person's right to access information held about them, which could be client records. The new law gives less time to respond to these requests, information must be provided without delay and at the latest within one month. In most cases, organisations won't be able to charge a fee. There's more on these and other new rights on the ICO's website).

Data breaches

Businesses will need to report certain data breaches to the ICO within 72 hours of becoming aware of it and in some cases, where the breach is considered high risk, to the individuals affected. Read more on breach reporting under GDPR.

Data protection impact assessments (DPIA)

A data protection impact assessment (DPIA) can help businesses identify the most effective way to comply with data protection law. It allows any problems to be identified and fixed at an early stage. The ICO's GDPR accountability and

governance guidance cover the new requirements.

The ICO remains committed to helping organisations to improve practices and prepare for the GDPR. For small and medium size businesses, we've launched a revamped data protection self-assessment toolkit, which includes a checklist to help you get ready for the GDPR.

Our GDPR guidance updates are published regularly on the ICO's website, *DP reform (GDPR)*. Organisations can also sign up to our newsletter for the latest information or follow the ICO on Twitter at @ICONews.

Image

FROM THE CIOT/ATT PROFESSIONAL STANDARDS TEAM

The Professional Rules and Practice Guidelines say that members should implement a policy for retention of documents and records in their files. These policies will need to be updated to reflect GDPR.

The updated money laundering regulations (The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017) also deal with data protection issues. As set out in Regulation 40 (5) any personal information obtained for the purposes of the regulations must be deleted *after* five years from the end of a business relationship unless

- The business is required to retain it under statutory obligation, or
- The business is required to retain it for legal proceedings, or
- The data subject has consented to the retention.

In addition, under Regulation 24 and training —

(1) A relevant person must—

(a) take appropriate measures to ensure that its relevant employees are

(i) made aware of the law relating to money laundering and terrorist financing, and to the requirements of data protection, which are relevant to the implementation of these Regulations.

The 'Tripadvisor effect': how to prepare for the shift in power from firms to consumers

Professional services firms have only nine months to go to get to grips with the requirements of the new GDPR before it comes into force. The much publicised fines – up to €20 million or 4% of global turnover whichever is the higher – together with the more onerous test for consent and the so called ‘right to be forgotten’, have caused alarm bells to ring for many. Despite this, a large number of organisations have still not embarked on their GDPR compliance projects. We spoke to 30 in-house lawyers for our recent GDPR White Paper – including in professional services firms. Ten per cent weren’t at all prepared, none were fully prepared, and the rest fell on a varied perspective in between.

For tax practices, operating in a regulated environment, confidentiality obligations and duties of professional conduct mean that they should be accustomed to looking after their client’s data. They should therefore already be some way along the path to achieving compliance but there will still be some challenges along the way.

Accountability and Transparency

Although existing data protection legislation is very much outcomes-based with penalties for failure to comply, the GDPR goes much further. The accountability principle means organisations need to not only comply but demonstrate compliance. Data protection needs to be embedded into an organisation’s practices, systems and procedures, requiring comprehensive but proportionate governance measures for all data protection activities. These are the concepts of ‘privacy by design’ and ‘privacy by default’ –recognised and expected within the GDPR.

Firms will need to consider whether they need to appoint a Data Protection Officer as well as implementing measures such as privacy impact assessments and record keeping. They will also need to review any supplier agreements that involve the processing of personal data such as hosting and SaaS agreements. Under the GDPR there is an obligation on controllers to exercise a high degree of care in selecting any third party to carry out data processing activities on its behalf. The GDPR also mandates certain contractual provisions to be included in the agreement. Much fuller due diligence of suppliers will become essential.

With direct obligations placed on processors as well as controllers under the GDPR, negotiations with suppliers are set to become more protracted with suppliers seeking to limit their liability in the face of the significant fines. And for firms which

use cloud servers in the US to store or transfer confidential data there is an added complexity which must be grappled with sooner rather than later.

Data Subject Rights

One of the main aims of the GDPR is to address rapid technological advancements and unprecedented global flows of data. These developments have given rise to the need to strengthen the rights of individuals and the protection of their personal data. The GDPR therefore affords individuals enhanced rights. Some rights already exist under current data protection legislation such as the right of access and the right to rectification. There is now a broader right to erasure under the GDPR without any requirement for the processing to cause unwarranted and substantial damage or distress.

For professional services firms the right to erasure on initial glance appears to present a conflict with other laws and regulatory requirements by which they are bound and which require them to retain client data for a specified period. It is important to note though that the right to erasure is not absolute and only applies in specific circumstances. Most specifically, the right of erasure can be refused for specified reasons including for '*compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject*'.

Other areas of tension between the GDPR and regulatory requirements include the principles of data minimisation and storage limitation. Whilst on the one hand professional service firms are bound to maintain full records for a minimum period of time, the GDPR requires firms to only hold the minimum that is necessary and for no longer than is necessary. Another possible area of tension in the financial services sector comes in the form of MiFID II – which mandates the recording of any telephone conversations or electronic communications intended to lead to a transaction and to retain the recordings for 5 years. It is unclear how to square this with requirement to not hold data for longer than necessary for the purpose for which it was collected but is something that firms need to consider in advance of May 2018.

Firms must start to take action now. As a starting point, firms need to establish a full understanding of the personal data that they hold, the lawful basis on which they hold that data and what they do with the data. This should include how long they hold the data for and where it is held and transferred to. They should also review

their supplier agreements and the procedures they have in place to meet the strict 72 hour breach notification requirement and to satisfy the enhanced data subject rights.

Consumer awareness around GDPR is already gathering speed. But with substantial PR campaigns being prepared by the ICO and consumer groups, consumers are certain to be considerably more clued up on their rights by next May. The shift in power from firms to consumers has the potential to be as great as the impact of disruptive technology innovations like TripAdvisor and Amazon reviews.

The final word, though, should be an optimistic one. Organisations have an opportunity to turn GDPR compliance to their advantage. Lack of preparation will inevitably have a disruptive effect. But organisations with a full understanding of the requirements under the GDPR – particularly those engaged in highly personal and sensitive services like processing detailed financial information and providing tax advice – could reap real benefits through enhanced reputation and customer trust. Read the white paper, *GDPR: Getting ready for data's new dawn*.