GDPR:
Risk, opportunity and what it means for security professionals

Authors
Neil Fraser, MSc (Royal Holloway, 2017)
Geraint Price, ISG, Royal Holloway

Abstract

The EU General Data Protection Regulation (GDPR) enters force in May 2018 and represents the most significant development in privacy legislation for a generation. Many commentators choose to focus on its increased financial penalties, presenting it as a regulatory risk and, often, a problem for the information security function to deal with. This point of view is inherently flawed. Security is only one aspect of the Regulation and its fundamental security requirements remain largely unchanged. Security is important, of course, but GDPR is evolutionary, not revolutionary in this regard. This article discusses why GDPR is necessary, what it means for security professionals and how it can be approached from a positive perspective. [a]

[a] This article is published online by Computer Weekly as part of the 2018 Royal Holloway information security thesis series https://www.computerweekly.com/ehandbook/GDPR-Risk-opportunity-and-what-it-means-for-security-professionals. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/.

Data, data, everywhere

It has never been cheaper to store data. In 1995 - I'll explain why 1995 shortly - a gigabyte of storage cost around $1,000. Today, it can cost as little as $0.02. That's a decrease of 50,000% over just a couple of decades.

We are also creating more data than ever before. In 1995 the global internet population was around 16 million with fewer than 1% of Europeans using it regularly. Today, internet penetration in Europe is over 80% and all online activity generates and enables collection of data. In 2016, IBM calculated that the world generates 2.5 exabytes (2.5 billion gigabytes) of data every day and 90% of data in existence was created in the last two years. 720,000 hours of content are added to YouTube every day; 27 million tweets are sent every hour; 45,000 Uber rides are taken every minute. This is a one-way trend and some analysts predict that the amount of data created annually will reach 180 zettabytes (180 trillion gigabytes) by 2025.

Information is the lifeblood of many organisations and for years the cost of storage represented a considerable expense. Today the opposite is true: storage is so cheap that most businesses have more data than they are aware of and certainly more than they know what to do with. The situation has been compared with trying to drink from a fire hose. Storage is now so inexpensive that it's cheaper - not to mention easier - to keep *everything*. There is so much data around that new tools, methods and an entirely new discipline - big data analytics - are needed to help organisations use it.

Personal data is ...

... any information relating to a living person who can be directly or indirectly identified, in particular a name, an identification number, location data, an online identifier or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Risks to data are also increasing. The 2017 Cyber Security Breaches Survey found just under half

(46%) of all British businesses had suffered a data breach or cyber-attack in the last 12 months, rising to 67% for larger organisations.

From a security perspective, this creates a perfect storm: organisations hold more data than ever and breaches - malicious or accidental - are also increasingly common. Furthermore, much of the information organisations are so enthusiastically collecting falls into the category of *personal* data and is subject to legislation to protect the individuals to whom it relates. 61% of all UK businesses hold personal data on their customers electronically and those that do are more likely than average to have suffered a breach in the last year (51% versus 46%).

Why GDPR?

Entering force on 25 May 2018, GDPR represents the most significant development in privacy legislation for a generation and it's long overdue. To illustrate this, consider the choice of 1995 in comparing storage costs and internet usage. That was when the current EU data protection law, the Data Protection Directive 1995 (DPD95), was adopted. Incorporated into UK law as the Data Protection Act 1998 (DPA98), it was the EU's first attempt at creating a pan-European approach to data protection but has never been fully successful. Discrepancies between member states make pan-European compliance a challenge and, over time, a situation has arisen where no domestic laws are sufficiently aligned for an organisation to be simultaneously compliant across the Union.

DPD95 also suffered from its almost uncannily inopportune timing. Drafted in 1992, just three years after the 1989 invention of the Web by Tim Berners-Lee, it became almost immediately outdated from a technological perspective. It is based on a model of data processing that no longer exists: one that assumed most organisations would have only a few computers accessed by a limited number of staff. Coupled with the advent of e-commerce, social media, mobile devices and the Internet of Things, all of which involve the collection and processing of personal data, GDPR represents an unavoidable legislative reboot.

As well as bringing the law up to date with new technologies, GDPR forms an important component of the EU's digital single market strategy. As a regulation, rather than a directive, it applies directly and simultaneously throughout the EU without the need for enabling national legislation. This is an advantage for organisations operating internationally as it presents a single set of rules rather than the current patchwork of laws.

More importantly, GDPR is about strengthening individual rights and improving consumer confidence. A 2015 survey found a majority (67%) of EU citizens are concerned about losing control of their data and less than half (37%) trust businesses to protect it. We may safely assume that public confidence has been further eroded by revelations in March 2018 that Facebook user data may have been misused to influence voter behaviour. Such concerns inhibit the adoption of new technology and result in lost business opportunities. Conversely, increasing individual control over data enables trust and encourages economic activity. With personal data breaches becoming common features in the mainstream media, providing good data protection could act as a powerful market differentiator. In short, getting this stuff right is not just a legal requirement: it's good business.

GDPR Post-Brexit

Uncertainty over GDPR's applicability post-Brexit has caused delays in compliance investment. This is dangerous: it will have full legal effect while the UK remains in the EU and throughout any transition period. A new Data Protection Bill is also passing through parliament and its requirements are likely to be identical to GDPR.

Before discussing some of the key changes introduced by GDPR, it's worth clearing up its applicability in the UK post-Brexit. The short answer is that Brexit will have no effect. The longer answer is that the EU Withdrawal Bill states: "EU legislation, so far as operative immediately before exit day, forms part of domestic law on and after exit day". In other words, everything that is law the day before Brexit - including GDPR - will continue to be law the day after Brexit. In June 2017 the UK government announced a domestic equivalent of GDPR to replace the existing DPA98. Full details of the new law

have not yet been announced, however, every indication is that it will match GDPR at a fundamental level, offering UK citizens the same protections as their European counterparts. Furthermore, GDPR applies to all organisations handling EU personal data, irrespective of where the organisation itself is located. The message is clear: GDPR means GDPR.

What does GDPR mean for security professionals?

Perhaps unsurprisingly, many commentators choose to focus on GDPR's significantly increased financial penalties. In the UK, the Information Commissioner's Office (ICO) sees its maximum fine increase from £500,000 to €20m or up to 4% of the offending organisation's global annual turnover, whichever is greater. With penalties like this on the table it's not surprising that data protection is suddenly on the mind of many security professionals.

Happily, I can assure you that your organisation won't be fined €20m for a security breach. It has been widely overlooked that GDPR has two tiers of fines. The upper tier - €20m or 4% - is reserved for infractions relating to, among other things, transparency (i.e. letting people know you are collecting their data and why), the lawful basis for processing (e.g. consent or execution of a contract with the subject) and the rights of individuals (e.g. for access, correction of errors and erasure). Security breaches, along with many other aspects, are subject to the lower tier penalty of up to €10m or 2% of turnover. Moreover, the ICO has already dismissed speculation that maximum penalties will become the norm. Remember, it has never issued the current maximum fine of £500,000.

More than security

GDPR places more emphasis on data subject rights than security. Keeping data safe is important but failure to correctly obtain consent, service subject access rights or demonstrate accountability for data in your care can lead to a fine even where no security breach has occurred. Good data governance is key to compliance.

€10m or 2% of turnover is still a lot of money but this offers a clue as to where GDPR's real priorities lie. While it is significantly more detailed than DPD95 - 88 pages and 99 articles compared to 20 and 34 respectively - less than 5% relates to security. GDPR is about individual rights and good information governance: knowing what data is held, from whom and for what purpose it was obtained, where it is located and, yes, how it is protected.

This is an important observation because many organisations see GDPR as an issue for the IT or security department to deal with. In reality, it affects every part of the business including non-customer-facing departments. Your employees have rights too so things like payroll data - much of it personal - is as much in-scope as your customer database.

The first step for any organisation should be a comprehensive audit to identify how much personal data is held, where it is logically and physically located and whether it is still needed. This could be a significant undertaking but may also have some benefits. At the very least, organisations will understand what data they're holding and 52% believe the audits will also lead to their business data being better understood and controlled.

Security of processing

Having said GDPR isn't really about security, some aspects do fall into the remit of the information security function. These are focused on three articles: article 32 dealing with security of processing and articles 33 and 34 concerning breach notification.

Like earlier legislation, GDPR recognises two entities involved in handling personal data: controllers and processors. The controller determines the purposes and means of processing of personal data and the processor processes it on behalf of the controller. A common example is a company with

an outsourced customer call centre. The company is the controller and the call centre the processor. Where GDPR differs is in the responsibilities placed on each. The controller must use processors providing sufficient guarantees of security and, for the first time, processors have a legal - rather than contractual - obligation to protect data. This is a sensible evolution: in many cases a processor, e.g. a cloud provider, will be better positioned and equipped to secure data than a controller, who could be a small business with limited security expertise.

GDPR is not prescriptive in what organisations must do to protect personal data. Instead, it requires technical and organisational measures to ensure a level of security appropriate to the risk, although specific technologies such as encryption and pseudonymisation (processing data in such a manner that it cannot be attributed to a specific individual without the use of additional information) are identified as worthy of consideration.

Elsewhere, GDPR suggests mechanisms to provide access control, prevent malware, prevent or limit denial of service attacks and protect against physical intrusion. It also suggests internal controls to prevent unauthorised or excessive access to personal data, for example restricting access on a need-to-know basis via a role-based access control model. The point is none of these measures should seem unreasonable to most well-established security departments. The Regulation is evolutionary, not revolutionary in its treatment of security. The MSc dissertation linked to this article discusses this evolution in more detail.

It is important to note that none of these controls are mandatory. The Regulation requires a risk-based approach to security but critically and unlike a traditional security risk assessment, the risk relevant to GDPR is that affecting data subjects, not the organisation itself. This is best explained by means of an example. Theft of a large quantity of personal data is an obvious breach of security but if that data is encrypted the risk to individuals is likely to be minimal and, thus, the organisation unlikely to face penalty. This should act as a significant driver in adoption of encryption by organisations that do not already use it to protect personal data. Unfortunately, that currently accounts for almost two thirds of British businesses.

Beyond confidentiality

Personal data leaks are increasingly reported in the media so it's natural that organisations focus on confidentiality when planning for GDPR. It's important to remember, however, that GDPR does not equate security with confidentiality: integrity, availability and resilience are also required. This means contemporary threats like ransomware rendering data inaccessible also become a data protection concern and should be considered in your approach to compliance.

It all comes down to what is considered an 'appropriate' level of security taking into account the nature of the personal data and the potential harm to individuals should it be stolen, lost or rendered unavailable. A reasonable rule of thumb might be that if the cost of a security control (in terms of money, time or effort) is less than the potential harm caused by a breach, not implementing that control could be viewed as unreasonable. On the other hand, assuming sensible security measures generally, an organisation suffering a zero-day exploit is unlikely to be penalised assuming they could not reasonably foresee the harm.

The fact that GDPR provides little direction on security controls is actually a strength. Instead of mandating mechanisms that might quickly be rendered obsolete, it provides for a minimum baseline. Instead of specifying how data is protected it specifies the level of security to be achieved, leaving organisations free to choose the most appropriate controls. Organisations can use approved codes of practice or standards to help demonstrate compliance with GDPR's security requirements. This may drive further adoption of risk-based standards such as ISO/IEC 27001 or others developed specifically for GDPR.

Breach notification

While article 32 is very much an evolution of earlier requirements, a key change is that GDPR introduces an obligation to report personal data breaches. That's right: before now organisations had no legal duty to inform anyone if they suffered a breach. The new rules are different for processors and controllers. Processors need only notify the controller without undue delay. This is unlikely to cause much impact as similar contractual obligations are likely to already exist. The requirements for controllers are more complicated and consist of two categories: notifying the ICO and communication of a breach to affected data subjects.

Upon becoming aware of a breach, the controller has 72 hours to notify the ICO of the incident, its anticipated consequences and any measures taken or proposed to mitigate its effects. Clearly this leaves little time so developing an efficient breach notification process will be an important aspect of organisations' incident response procedure. Remember, however, that if the risk to data subjects is low, e.g. the data is encrypted, then notification may not be necessary. Similarly, if the breach is a failure in storage media but recent backups exist then there is no need to report it.

If a breach is judged to represent a high risk to data subjects the controller must inform them individually. There is no strict timeframe on this, but it must be done without undue delay and in clear and plain language. This has a potentially high cost to business, especially if the controller cannot determine which subjects are affected or has limited means of contacting them. Again, good information governance will be key.

Unfortunately, the distinction of what constitutes low and high risk is not clearly defined and many organisations may be unsure of whether to report a breach or not. Some commentators suggest notification should be made by default to avoid accidentally breaking the law, however, whether the ICO has the capacity to deal with the volume of notifications resulting from this approach is another matter. Instead, implementing the measures needed to obviate notification (mainly encryption, resilient systems and regular backups) would seem to be a more effective and sustainable approach.

Conclusion

GDPR is an evolution of the existing rules around data protection and little discussed above should come as a major shock. There are some new obligations - those around breach notification in particular - but GDPR is largely a restatement of security requirements that already exist. Organisations compliant with the current rules and that take their obligations seriously are already well placed to deal with and benefit from it. Data protection is ultimately about safeguarding individual rights. As we move towards an ever more information-centric world, the public are increasingly aware that their personal data has value. The challenge organisations face is reassuring consumers that they can be trusted to handle their data fairly and responsibly. Those that can do so will have a major competitive advantage.

GDPR is not a task for the IT or security department alone; it must involve the whole business. As a security professional, the next time someone from another department asks you what you're doing to prepare for GDPR, your immediate response should be 'what are *you* doing to prepare for GDPR?'

You can find more information on GDPR, how it affects business and how it is a natural evolution of existing data protection legislation in the MSc thesis on which this article is based.

Biographies

Neil Fraser completed the MSc in Information Security at Royal Holloway, University of London in 2017. Prior to this he was an intelligence and security analyst for the military and various government departments. He currently works as an information security consultant for a major telecommunications provider, ensuring technical solutions are aligned with customer security requirements. His interests include Internet of Things security, cyber resilience in critical infrastructure and privacy-enhancing technologies.

Geraint Price BSc (London), PhD (Cantab) obtained his B.Sc. in Computer Science from Royal Holloway University of London in 1994 and his Ph.D. from University of Cambridge in 1999. His Ph.D.

dissertation analysed the interaction between Computer Security and Fault Tolerance. Since then he has worked on various projects including Denial of Service attacks in networks and the future of Public Key Infrastructures, funded by academia and industry. Geraint is a Senior Lecturer in the Information Security Group, and has a strong interest in the practice of information security. He leads the ISG's external engagement activities with business and government. Geraint is a regular attendee, panellist and speaker at a number of industrial fora, including I-4 and the ISF.

Series editor: S.- L. Ng