BRIAN HONAN, BH CONSULTING

# GETTING UP TO SPEED ON GDPR

## PREPARING FOR THE GENERAL DATA PROTECTION REGULATION

ADVANCED THREAT PROTECTION, SECURITY AND COMPLIANCE

Search online for the phrase "data is the new oil" and you'll see it's used by (and attributed to) many people. Data is a precious and highly valuable commodity. Data is the fuel pumping through today's digital business, powering communications and commerce. Organizations the world over are mining data to turn raw information into real insight—to drive sales and grow their business.

The trade-off for this great power is, as the saying goes, great responsibility. That's another reason why data is like oil—because it's a nightmare to clean up when it leaks. Therefore, organizations must ensure they're protecting their data with appropriate systems and policies. As such, information security will figure prominently in developing a comprehensive approach to EU GDPR.

The upcoming EU General Data Protection Regulation, to give its full title, comes with stringent provisions around protecting any data that could identify a living person. Although the law is EU-based law, GDPR applies to all organizations globally that wishes to do business with, or monitor the behavior of, EU citizens, no matter if the company is domiciled within or outside the European Union. Organizations covered by the regulation need to demonstrate they are protecting that information in accordance with the rules; failure to do so carries serious financial consequences.

While some people will inevitably roll their eyes at the thought of having to meet new regulatory requirements, it's worth keeping in mind that the reform process stemmed from a desire to increase the trust of EU residents that their personal data is secure. The EU's larger agenda is to create greater confidence in digital services, e-commerce and the cloud.

As the European Union is the second largest economy, as a bloc, in the world with a GDP of €16.5 trillion (US$ 17.7 trillion), this is a significant move in protecting the rights of its citizens. Further, it enables those citizens to engage with online providers and other vendors with the confidence that certain protections their personal information are in place.

So, that implies that organizations following the rules in a secure, transparent way will earn this trust from consumers, and as a result can potentially grow their business. Too often, we see regulatory compliance as a cost, but in this light GDPR should be seen as a business opportunity enabling businesses to access that market

This white paper outlines the key points you need to know about EU GDPR, and the implications the new rules will have for businesses that handle personally identifiable data. From there, it outlines some of the steps your business can take to prepare for when the rules come into force. Special attention is given to "appropriate security to the personal data" and the foundational controls required for "security processing."

## TELL ME MORE ABOUT GDPR

GDPR has been described as the biggest development in information law in two decades. Not only is it intended to increase privacy for individuals, it hands data protection regulators much tougher powers to act against organizations that breach the new rules—but more about that later.

GDPR is a new European Union law that harmonizes the previous European data protection regime across 28 EU member states. After a four-year reform and consultation period, GDPR came into force on May 24, 2016 and it will apply from May 25, 2018.

It was drawn up partly in response to demand from European citizens for the same data protection rights across the EU, and it enshrines that protection as a fundamental right. It also gives us a much broader definition of what constitutes personal data that could identify a living individual:

*'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;'*

Organizations that process personal data must:

- Obtain clear consent from the subject of that data
- Obtain parental consent if the subject is a child under the age of 16
- Provide a copy of an individual's personal data in a portable format if requested to do so
- Erase all personally identifiable records of an individual if asked to do so
- Provide adequate security to protect that data
- Notify their regulator in the event of any security breach that impacts on the personal data entrusted to them

### UNIFORM APPROACH

Under the Data Protection directive 95/46/EC (which preceded GDPR), there were 28 different versions of

European Data Protection rules as each member state within the EU implemented the directive into their own statue books according to each country's requirements. The core principles of the Data Protection Directive were enacted into each country's legal system, but because the directive was enacted under each EU member state's own legal system, each one was slightly different. This resulted in a confusing tapestry of data protection laws throughout the EU which companies operating in each of those countries had to navigate very carefully. This often resulted in increased compliance costs and efforts, and in some cases companies complying with the data protection rules in one EU member state while inadvertently breaching those in another.

The EU GDPR will apply one harmonized set of rules no matter where in the EU the data subject happens to be. What's more, as a regulation it will come into force without any country needing to implement national legislation.

Just as importantly, the rules apply to all companies that process data relating to EU citizens, regardless of where that data is ultimately stored or processed. The rules are partly a reaction to technology developments like the cloud, which lets companies transfer large quantities of data from one jurisdiction to another—even outside the EU—instantaneously. To put it another way, don't let the name fool you: in effect, the EU GDPR is a global law.

## WE'VE GOT YOU COVERED

From May 25, 2018, EU GDPR will apply to all companies—no matter where their headquarters are—that control and process personally identifiable information about EU citizens.

### ONE REGULATOR TO RULE THEM ALL

◆ Under GDPR, organizations now only need to pick one supervisory authority they want to work with, such as the Information Commissioner's Office in the UK or the Data Protection Commissioner in Ireland. That's a solid improvement from the older data protection regime that required working with regulators in every EU Member State in which they want to do business. This ended up being a bureaucratic nightmare, in the EU's own words, for multinationals. GDPR simplifies matters for any organization that deals with multiple EU Member States. It scraps the need to notify or register for data processing with each local data protection authority, which was costing business €130 million per year. GDPR means just a single set of data protection rules to comply with, and one authority for reporting across the entire EU.

## FINE, LET'S GET THIS OVER WITH

First the unpleasant part. The fines for failing to comply with GDPR are more severe than under the current data protection regime, and the compliance obligations are more onerous because the regulation affects all organizations that do business, provide services, or carry out activities on behalf of individuals in the EU.

Under the EU GDPR, data protection authorities in all EU member states will have more wide-ranging powers to impose potentially significant fines for any business that fails to comply with the regulations. This is a significant change in the data protection regulatory regime as previously the data protection authorities would have to bring a case to court and it would be up to the court to determine if the accused party was guilty and what fine to impose. The new regime gives more power to the data protection regulator and will no doubt result in more organizations who breach data protection regulations facing penalties. In addition to these new powers for the data protection regulators the penalties are much larger than under the current data protection regime.

The most serious instances of non-compliance carry fines up to a maximum 4% of the guilty company's worldwide revenues or €20 million, whichever is higher. That figure alone has earned GDPR a lot of headlines since the law was published, but it relates to specific offences involving data processing, consent, data subject rights, non-compliance with the order of a data protection authority, or transfer of data to a third party.

There's a second band of fines of up to €10 million or 2% of global turnover for a range of other offences relating to child consent, transparency of information and communication, data processing, security, storage, breach and breach notification, and transfers related to appropriate safeguards and binding corporate rules.

As can be seen, failure to comply with the EU GDPR can have significant financial implications for organizations who run afoul of their Data Protection regulator.

### TIME IS TICKING

Another key element of the EU GDPR is the introduction of mandatory notification requirement for companies that suffer a security breach resulting in the exposure of personal data belonging to customers. The EU GDPR will force all organizations to report breaches involving personal data to their local data protection authority—where feasible within 72 hours of the breach being identified. If there's any delay, the controller must provide a "reasoned justification" for this.

That structure alone puts pressure on organizations to be very proactive in watching for possible breaches, and is just one example of where GDPR has a direct effect on an organization's information security posture. Many organizations struggle with timely breach discovery: the Verizon *Data Breach Investigations Report* found that attackers can compromise systems in days or less (often minutes) but victims often don't find out until much later.

GDPR is also intended to give EU residents easy access to personal information that almost any organization holds about them. If requested, that organization must provide detailed information not just about the type of data it holds, but also the reason why it's doing so, and the methods for which that data is being processed.

### GO DPO

Until now, it hasn't been mandatory for organizations to appoint a designated individual with responsibility for data protection, commonly known as a Data Protection Officer (DPO). This too is another big change under GDPR. Organizations whose core activity involves processing personal data on a large scale—involving more than 5,000 data subjects in a 12-month period—must appoint a designated Data Protection Officer (DPO). This can be a staff member or a service provider under contract, but the appointment should be based on their professional qualities and specifically having expert knowledge of data protection laws. The role must be independent and autonomous and must have a direct line of reporting to senior management.

Unless regularly processing personally identifiable data is a core business activity, Small & Medium Enterprises (SMEs) employing fewer than 250 people are exempt from the obligation to employ a DPO, although appointing a DPO is nevertheless seen as good practice.

The International Association of Privacy Professionals has produced a study which estimates that up to 75,000 new DPO positions will be created as a result of companies needing to meet their GDPR requirements. Early industry commentary suggests that number is a conservative estimate.

The DPO post has a wide-ranging remit that covers:

- Developing and implementing a data protection policy for the business
- Providing guidance on best practice for processing personal data
- Organizing employee training
- Coordinating any requests for information under the terms of the regulation

The EU's Article 29 Working Party was due to provide guidance on the DPO role by December 2016. This should help businesses map out suitable job descriptions and identify whether they already have qualified people who could fulfil the role, or whether they'll need to recruit externally.

### THE PEOPLE'S RIGHTS

- An individual in the EU, or data subject in GDPR-speak, can:
  - Ask the data controller to erase her/his personal data, cease further dissemination of the data, and potentially have third parties cease processing of that data. This is also known as 'the right to be forgotten'
  - Have access to, and information about, the personal data that a controller has concerning them (also known as 'the right to access' or 'subject access right').
- These rights are important to know because they directly affect how your organization handles data, and how your staff are trained to respond to any such requests.

### CUT TO THE CHASE

So, let's get to the most relevant parts of the legislation from an information security standpoint: GDPR requires data controllers to implement "adequate measures" to ensure the confidentiality and integrity of its processing systems and the information they hold. As the regulation states:

*"Personal data shall be… processed in a manner that ensures appropriate security*

*of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')'.*

This wording is intended to be both technologically neutral and future-proofed, but a useful working initial interpretation is:

- You should have critical security controls that can detect, manage and mitigate appropriately any vulnerabilities to your data processing environment
- Your systems should be configured in accordance with the enterprise policy, and maintain that configuration
- Your security systems should be capable of identifying any deviations from the policy
- You should continuously monitor your log files to alert to any potential breaches or vulnerabilities
- You should detect, respond to, and remediate any detected incidents effectively
- You should engage securely with the cloud
- Sensitive personal data should be encrypted at rest and in transit. In particular, sensitive personal data stored on portable devices such as laptops or smartphones should be encrypted
- Access control to where sensitive data is stored should be implemented on a need to know basis and reviewed regularly

While the regulations don't say it explicitly, GDPR effectively requires organizations to have a defined security strategy that conforms to accepted industry standards. Some useful frameworks to benchmark yourself against include:

## GDPR Good Practice: A Security Checklist

*Article 32 of GDPR is entitled "security of processing," and it calls for the data processor to implement "appropriate technical and organizational measures to ensure a level of security appropriate to the risk." The examples it provides includes:*

- Pseudonymization, minimization and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

You should be able to monitor your security controls constantly and review them to ensure they are continuing to protect the personal data you hold. This level of monitoring is foundational to your security processing efforts.

### CHANGE CONTROL

Can you identify when unplanned changes introduce security weaknesses? Do you have the ability to perform regular scans to look for potential new vulnerabilities, prioritize them and get them remedied as quickly as possible? Active monitoring for unauthorized changes on important systems can identify weaknesses or possible points of attack.

### FILE INTEGRITY MONITORING

The ability to see when changes are made to critical files or systems is the first step to understanding whether those changes have been made for malicious reasons. This can provide the crucial early warning capability when a system has been breached.

### VULNERABILITY MANAGEMENT

Regular testing of security controls for vulnerabilities, and where they occur, gives you the information you need to address those weaknesses proactively. These vulnerabilities may be in the software, system configuration, process, or human layers, so it's important to have a tool that allows you to correctly identify the nature of any potential changes.

### CONFIGURATION MANAGEMENT

When critical systems have been designed and implemented in a secure way – whether that's email servers, file servers or database servers – it becomes easier to add new systems or applications in a similarly secure way, as appropriate. Is encryption turned on? Is this application authorized? You will also be able to spot changes to those systems quickly, and apply appropriate security in a timely fashion. If any of those systems don't meet your requirements or if configurations are not to the appropriate security level you've determined, your layered security approach should alert you to those potential risk exposures.

### LOG MANAGEMENT

Regularly review the logs to identify suspicious behaviour or be available if a breach occurs to investigate and contain. Do you have real time intelligence and automation for fast and accurate reporting for incident response?

- ISO/IEC 27001/27002
- NIST Cybersecurity Framework
- CIS Critical Security Controls

The systems, controls and processes that you use to monitor data assets should align with these standards. Interestingly, one of the general conditions for imposing administrative fines under GDPR involves:

*'the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32'.*

In other words, being able to show you had appropriate security measures in place prior to an incident may reduce the financial impact of that event. That's a business case for increasing security investments that you can take straight to the board.

### REMIND ME WHEN I NEED TO BE READY FOR GDPR?

May 25 2018 is the date by which EU GDPR will become law within all member states, so from that date onward organizations need to be compliant. So while at the time of writing this white paper that dates seems a long time off, it will be upon us sooner than we think. Some organizations may have some of the requirements for compliance already in place due to their efforts to be compliant with the existing Data Protection laws in the EU member states. However, many more organizations are not, especially those organizations that are located outside the European Union but who provide services to EU citizens. A survey from CA Technologies found that just 46% of organizations are confident they will be ready in time for GDPR's implementation date.

It's important to remember that GDPR will be in force across all EU member states from May 25, 2018. Once that date is reached there will be no grace period or time to ramp up your compliance. You and your organization needs to be prepared for GDPR before the deadline; GDPR will be ready for you, you need to be ready for GDPR.

### HOW WILL GDPR BE ENFORCED?

As mentioned earlier, each Data Protection regulator will have new powers to ensure compliance with the EU GDPR and to prosecute breaches of the same. In the main, there are three key actions that the Data Protection regulators can take to ensure organizations are complying with the requirements of the EU GDPR. These are;

- **Proactive Audit**—The data protection authority's office will have the ability to conduct audits against organizations to ensure they comply with the EU GDPR. These audits can either be announced audits, which are arranged and agreed in advance with the organization to be audited, or unannounced audits whereby the regulator can conduct an audit against an organization without any pre-arrangements or warning. They can audit and apply fines directly.
- **In response to a complaint**—The regulator can investigate an organization in response to a complaint made against an organization to the regulator's office. The regulator can investigate the organization to determine if the individual's complaint is valid.
- **If there is a data security breach**—In the event of a security breach impacting the personal information of individuals, the Data Protection regulator will get involved to determine if the organization that suffered the breach had taken "adequate measures" to protect the data entrusted to it.

The Data Protection regulator will have the power to punish organizations it determines not to meet the requirements of the EU GDPR by placing fines against the organization, requiring the offending organizations take the necessary steps to ensure compliance, and/or the deletion of any data that has been gathered or processed unfairly.

### WHAT STEPS DO I NEED TO TAKE TO BE COMPLIANT?

The first key step for organizations to ensure compliance with the EU GDPR is to realize and accept that compliance is a critical business issue, and not an IT one. Getting buy-in from senior management or board is an essential first step in ensuring your compliance efforts will be successful, and organization-wide. Some key questions to ask are:

- Can you identify every piece of customer data across all of your systems and applications?
- Can you prove that you have the necessary consents to hold the customer data you have in your systems?
- Could you erase every instance of a customer's data if requested to do so?
- Could you provide a customer with their data in a portable format?
- Are you confident that the customer data entrusted to you is secured using all adequate measures?

This means that you need to understand what personal information you store and process, who it refers to, and how it is managed and how well it's secured. If Data Protection regulations and laws are not a core strength within your organization, you should consider engaging with an external consultancy or audit team that can evaluate your security measures and your controls around critical information.

You also need to determine if all or any of your data processing takes place in-house or whether it's outsourced to an external provider that processes the data on your behalf. EU GDPR states that data controllers

*'should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing'.*

The above statement is a key one to take into account as it not only refers to traditional data processing outsourcing but also how you engage with cloud service providers.

### KEY DATES

Again, May 25 2018 is the one you need to remember.

### FINE AMOUNTS

Up to €20 million, or 4% of global turnover.

### WHAT CAN I IGNORE?

If you don't process personally identifiable information, then you're not affected by EU GDPR. But given the expanded scope of the regulations, that puts you in the minority of organizations.

### NEXT STEPS

With such wide-ranging impact from GDPR, the sooner you start compliance efforts, the better chance you have of meeting the deadline.

- Talk to your auditor
- Assess what data you have and where and how it's stored. Determine whether or not that data should be protected using encryption and/or pseudonymization.
- If your organization adheres to a security framework, review and document the alignment and map it to the data flow
- Design a step-by-step process to becoming and staying compliant
- Set-up a cross-departmental task force with executive sponsorship

### APPOINT A DATA PROTECTION OFFICER

Your organization will need to formally appoint someone to the role of Data Protection Officer, or DPO, as part of GDPR compliance. The International Association of Privacy Professionals produced a study which estimated that up to 75,000 new DPO positions will be created as a result of companies needing to meet their GDPR requirements. Early industry commentary suggests that number is a conservative estimate.

The DPO post is likely to be a wide-ranging remit that covers developing and implementing a data protection policy for the business, providing guidance on best practice for processing personal data, organizing employee training, and coordinating any requests for information under the terms of the regulation.

### REVIEW YOUR POLICIES AND PROCESSES–THEN MAKE SURE YOU CAN ENFORCE THEM

Now is the time to review how your organization works with data and what happens to it through its lifecycle. Pay close attention to the security of controls, and identify where any vulnerabilities could be. You might not be starting from a position of strength; research from Netskope found that as many as three quarters of apps would fall foul of GDPR, and a survey from Ipswitch suggests that many organizations would need further investment in their security systems in order to meet the compliance requirements laid out in the new rules.

### TRAINING

As with most elements of good security, the human element plays a critical if often overlooked role. Security awareness training can ensure your organization is on the right foot when handling personal data and handling access requests from data subjects in a timely way.

When it comes to security, training and awareness offers some of the best returns on investment you could hope to get. Ensure your staff knows what constitutes personally identifiable data, and that you give them the tools, both technical and intellectual, to ensure they safeguard it appropriately at all times.

### SUMMARY

GDPR may seem onerous at first glance, but if your organization already complies with current data protection regulations, it should be a relatively small step to take in order to align with the updated controls and requirements because many of the fundamentals remain the same. The key consideration is that the new changes, around financial penalties and mandatory breach disclosure terms, will make data protection more a business issue than an IT issue. With an implementation deadline of May 2018, now is the time to start preparing for GDPR .

## ABOUT THE AUTHOR

Brian Honan is recognized internationally as an expert in the field of information security. He has worked with numerous companies in the private sector and with government departments in Ireland, Europe and throughout the United Kingdom. Brian has provided advice to the European Commission on matters relating to information security, and is on the advisory board for a number of innovative information security companies.

Brian is the author of *ISO 27001 in a Windows Environment* and co-author of *The Cloud Security Rules*. He has been regularly published in many trade publications, is a prolific information security blogger, and blogs for Information Security magazine. He is also European Editor for the SANS NewsBites newsletter, which is published twice a week to over 500,000 information security professionals worldwide.

Brian's speaks regularly at various industry conferences such as RSA Conference Europe, BruCON, SOURCE Barcelona, BSides London, IDC Security and the ICS Data Protection Conference, among others.

www.bhconsulting.ie
www.bhconsulting.ie/securitywatch



WPGDPR1a 201702