Executive Brief

A Practical Approach to GDPR

Sponsored by: Digital Guardian

Duncan Brown

April 2017

INTRODUCTION

The General Data Protection Regulation (GDPR) represents a substantial increase in business risk to most organizations within the EU and beyond. Companies are faced with a wide variety of decisions, including how to approach the process of becoming compliant with GDPR, the organizational prerequisites, and the introduction of technologies that may enable or hasten compliance.

This IDC Executive Brief provides a short introduction to the main characteristics of GDPR, and proposes a number of technologies that companies should consider in their compliance activities. It concludes with several action points that provide some guidance on essential elements of a compliance program.

GDPR OVERVIEW

The General Data Protection Regulation (GDPR) represents the biggest change to EU data protection and privacy legislation in three decades. The impact on organizations globally is profound, because the risk in dealing with personal data escalates to a level comparable with anti-money-laundering and anti-bribery and corruption legislation. A fine of 4% of global annual revenue is possible, and also introduced are mandatory breach notifications, class-action lawsuits, and the suspension of processing personal data (including employee payroll and customer information), effectively stopping a business from trading.

Why is GDPR so fundamental a change to data processing law? If the substantial penalties for non-compliance are insufficient to demand attention, what about the new requirements? In fact, in principle, there is much commonality between the current legal framework (based on the Data Protection Directive 95/46/EC). But there are some new requirements, such as data portability and the right to erasure (aka the right to be forgotten) that will challenge the information governance processes of any organization however mature. Joint liability between data controllers and their data processors represents a fundamental change in the relationship and responsibilities of companies throughout the supply chain.

In addition, GDPR is not specific in how organizations should conduct themselves. This imprecision is deliberate: it forces firms to decide how they should act – and what processes and technologies they should deploy – in order to achieve compliance. In this regard GDPR is an order of magnitude more complex and challenging to address than prescriptive standards such as PCI-DSS. Companies must take risk-based decisions, which means the depth and understanding of knowledge of the multiple factors affecting risk must be sought. IDC estimates that GDPR is 10 times more impactful on most organizations than PCI-DSS has been to date.

GDPR is 10 times more impactful on most organizations than PCI-DSS has been to date.

If the stick wielded by GDPR is substantial, then the carrot is that compliant companies will be protecting the personal data of customers, employees, and citizens in an effective and socially responsible manner. There is also an opportunity to create competitive advantage through being best in class in managing sensitive data types.

Much of GDPR is about process, but there are many elements of such processes that can only reasonably be supported through technology, while others are made manageable or cost-effective through the application of technology. GDPR is not specific about which technologies might be called for, while companies are required to consider "state of the art" (while no definition of this concept is provided).

The new rules come into force in May 2018, so the clock is ticking. Firms need to start preparing now to be compliant by the deadline. This requires prioritization, so companies understand the organizational and investment resources required, as well as understanding where to focus their attention for maximum benefit.

What is the best way to move ahead with the task of GDPR compliance? The rest of this paper discusses these key steps in more detail.

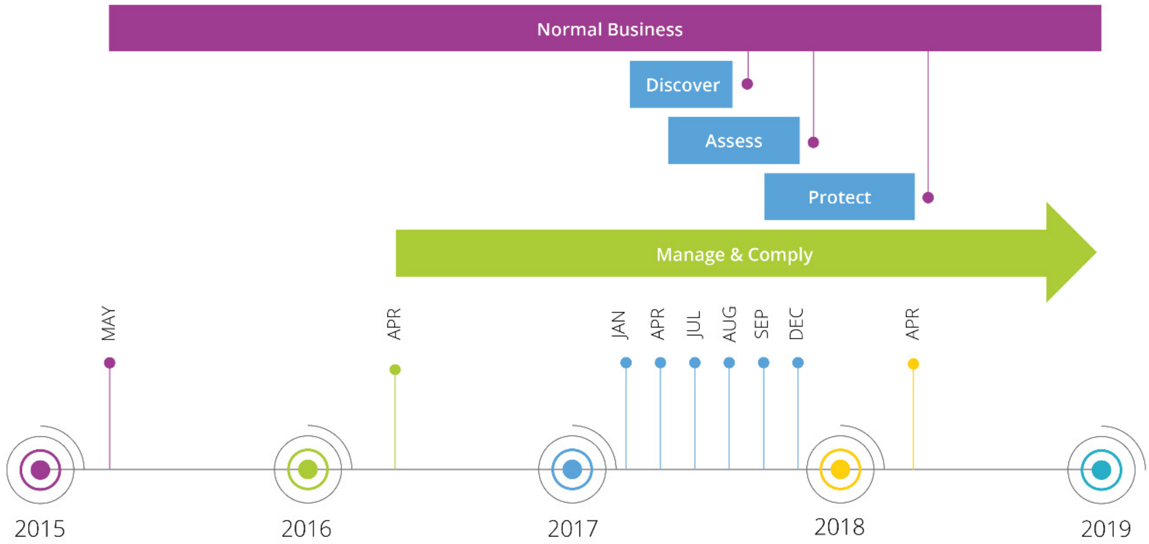
MANAGING GDPR

The importance of having all stakeholder parties involved in the GDPR program cannot be overstated. Organizations cannot afford to allow power struggles and poor collaboration to derail the program. One CIO told IDC that his CEO "locked" him and the head of compliance in a room "and told us to sort it out …". This may sound extreme, and we're not advocating executive incarceration, but it shows that the CEO in this case understood the strategic importance of cooperation.

One of the most frequently asked questions IDC receives is: Who leads the GDPR project? There are two things to note here, in the mindset of the questioner. Firstly, GDPR represents a substantial change in the corporate behavior of an organization. It therefore cannot just be a project, in the same way that the Y2K challenge was a project. There is no end date or closure. GDPR must therefore be considered as a program of change that will eventually be subsumed into corporate practice (see Figure 1).

FIGURE 1

GDPR Compliance Timeline



Source: IDC, 2017

The second thing to note in the question is that it assumes there is a correct and definitive answer. According to IDC's *GDPR 2017 Survey*, leadership can come from the CIO or CISO, or from compliance or legal, or marketing, or even from the board. What seems to be important is that it needs someone with overall authority to lead it. Many companies are operating in silos with little coordination or collaboration between them. Appointing a leader that drives a coalesced vision and program of activity is essential.

Origin of leadership is less important – what *is* important is that it is led by an individual with the charisma and authority to carry the organization with them. The origin of the leader usually depends on the specifics of the organization, but can also be influenced by the personal characteristics of the individuals in post. We have seen successful GDPR programs being led by CIOs, CISOs, CMOs, CPOs, and even CEOs (where GDPR is strategic to the company's success or failure).

But while leadership is important it is essential that the program avoids creating or reinforcing departmental silos. GDPR is primarily not a security problem, or even an IT concern: it is a business challenge. Whoever leads it, it requires cross-departmental collaboration. Best practice entails a steering group of empowered representatives from all stakeholder groups. This may include external sources such as shareholders and investors, or community groups, given the effect that sanctions for non-compliance may have. For example, we know that central banks are concerned that non-compliance with GDPR may affect the financial stability of banks under their supervision.

The Role of the Data Protection Officer

Organizationally, the role of the data protection officer (DPO) is something to pay specific attention to. Among the main considerations are qualifications and expertise, and the identification of conflicts of interest (see Articles 37–39).

There is likely to be a scramble for DPOs in 2017 and beyond. The International Association of Privacy Professionals (IAPP) estimates that the number of DPOs required in Europe is 78,000, assuming perfect compliance. The IAPP's membership counts 27,000 worldwide. Even allowing for variance in compliance it is clear that there is a massive deficit in the number of qualified people to perform the DPO role.

With regard to suitability GDPR states that the DPO must be appointed "on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil (their) tasks …". While there is no requirement that the DPO is a lawyer the clear guidance is that they must be familiar with the law. The IAPP reports that 60% of its members are not lawyers, but IDC assumes that membership of and accreditation by such an organization would be required as evidence of the credentials of a well-qualified DPO. In addition, the DPO must "report to the highest management level" within the organization, so they will require a degree of gravitas and confidence.

According to guidance from the Article 29 Working Party, companies engaged in processing of customer data in the regular course of business would be regarded as requiring a DPO.

Another key consideration is the possibility of conflicts between the role of the DPO and other duties. While it is not necessary for the DPO to be a full-time role, or even an employee of the organization, any other responsibilities must not conflict with the DPO role. The Article 29 Working Party has issued guidelines on the role of the DPO, which is helpful if not definitive. There is a wide range of possible conflicts, and decisions need to be made based on an individual organization's circumstances. But a person that makes a decision on "the purpose and means" of data processing would most likely suffer conflicts of interest. This may preclude the DPO also being the head of legal or chief counsel, since such individuals may be required to advise the organization on what processing may be conducted. It may also be inappropriate for the CIO to be the DPO as it may conflict with operational decisions that determine the purpose and means of processing personal data.

DATA DISCOVERY

For most companies facing a GDPR program the hardest part is to know where to start. The scope is substantial, ranging across not just IT but legal, sales, marketing, HR, and a host of other business functions. The number of new requirements may be extensive, depending on how familiar companies are with compliance in general and the amount of personal data processing they undertake. According to IDC's *GDPR Survey*, most firms will take two years to reach a state of compliance (from whenever they start), and will consume around a third of their security budget on GDPR-related activities (source: *IDC GDPR Survey*, 2017).

The first thing organizations usually start with is to identify the personal data that they collect. GDPR has a particularly broad definition of personal data, which includes "any information relating to an identified or identifiable person." The types of information include a name, identification number, location data, an online identifier, or one or more factors specific to "physical, physiological, genetic, mental, economic, cultural or social identity" (Article 4). Guidance has determined that an IP address and cookie information is included in the definition of personal data. In addition, the regulation identifies special categories of (sensitive) data that require an extra level of consideration: this includes "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade membership," and genetic, biometric, and health data as well as a person's sex life or sexual orientation (Article 9). To give this some practical context, consider an Internet of Things (IoT) application that tracks the health of a person. It records physical characteristics such as height and weight, food intake, location and movement data, sleep patterns, all of which is included in the scope of GDPR.

One of the starting premises of GDPR is that companies should only collect the data that they need (data minimization, Article 5c) and that they must have consent for collecting data and for specific purposes only (Articles 7 and 8). It is also important to record the details of the processing (Article 30) and that a company has good visibility over the location and accessibility of that data in order to effect the rights of data subjects (see Articles 15 to 20). The physical location of data is also an important consideration, as the EU is concerned that data is not exported to countries with a lower standard of protection of personal data (see Articles 44 to 50).

A good first step is therefore a data visibility assessment. This identifies the personal data held within the company, documents the sensitivity (special categories) of the data, where the data physically resides, how it flows throughout the organization, and the purpose of the data being stored and processed. It is essential that data be detected using some sort of automated process. Data identification conducted manually could take months or years to complete, and is unlikely to be entirely thorough. For example, data discovery needs to encompass information distributed across shared network resources, inside databases, and stored in the cloud.

A good first step is a data visibility assessment.

Automated data classification is an increasingly important function, as the type of data determines the protection regime required (and any sanctions resulting from non-compliance, in particular, breaches). Identifying and classifying data at rest is one thing, but catching it as it traverses throughout, and beyond, the organization is another. This is the realm of data loss prevention (DLP), which is having something of a renaissance in the lead-up to enforcement of GDPR. DLP is able to classify data on the fly and prevent that data from leaving the organization, subject to data protection policies. While it is not a solution to the entire GDPR challenge, IDC thinks that DLP is core to much of the scope of GDPR.

ASSESSING TECHNOLOGY'S ROLE

GDPR says very little about specific technology solutions that may facilitate compliance. It is important to note that this lack of prescription is deliberate: GDPR is designed to withstand the constant change of technology solutions, and also more generally the advancement of new use cases of technology. The previous data protection regime was formulated before the advent of cloud computing, social networks, the Internet of Things, and other technologies that we take for granted today. GDPR hopes to be able to cope with such changes in future, because it is based on principles and outcomes, rather than specific requirements.

However, this places an onus on companies to identify and deploy technologies appropriate to the levels of protection that yield the desired outcomes. In regard to the use of technology, GDPR refers to "state of the art." Companies are not required to implement state-of-the-art technologies and processes, but they *are* required to define what these are, and then to make a subsequent decision on whether to deploy them, based on cost and risk (together with other relevant contextual factors).

There are other requirements that relate to security indirectly. Article 25 introduces the concept of data protection by design and by default. This requires organizations to consider data protection concerns at the point at which processing is being determined. In effect, this means that data protection must be a consideration during the inception phase of a company's innovation process. And Data Protection Impact Assessments (DPIAs, Article 35) require organizations to evaluate the impact of technology that could have a high risk to the rights of data subjects. These articles are aimed at embedding consideration of data protection at every stage of technology life cycle, from design and introduction, through ongoing change management, to end of life.

With regard to security, the requirement is that companies "shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk" (Article 32). Companies need to make decisions on what technologies to invest in, to increase the chances of being compliant by 2018. What technologies should they be considering?

The rest of this section introduces some key technologies that IDC considers important in compliance activities. Note that many of these technologies can be sourced via one integrated solution: for example, advanced DLP solutions embed discover and classification, and evidentiary case management and reporting capabilities, as well as typical data loss controls.

Data Discovery, Classification, and Control

As described above, data discovery and classification is often the starting point for a GDPR program. However, it's also important to understand that this represents a combination of a methodological assessment of data visibility and the application of technology such as DLP. Companies need an approach that scans data in all its forms and states, including on workstations, servers, websites, and removable storage devices (such as USB drives). An important extension of the infrastructure for many companies is cloud, and the ability to reach into cloud file storage systems, such as Box and Microsoft OneDrive.

Access Control, Identity Management, and Privileged User Management

GDPR includes in the definition of a data breach "unauthorized … access to personal data." Clearly, then, access control to prevent "unauthorized processing" and "unauthorized access" is critical to compliance (see Articles 4 and 5). Although explicit emphasis within GDPR is on security of data, there is plenty of implicit reference to the security of identity. In addition to Articles 4 and 5, GDPR also refers to unauthorized disclosure of, or access to, personal data in recitals 39, 49, and 83.

IDC believes that a comprehensive identity governance solution is a core part of GDPR compliance. It is important to include not just the management of identities but the control of access to specific services and systems that deal with personal data. Maintaining evidence of access attempts and activity is a fundamental part of this. A particular source of concern for many companies is the abuse of privileged access to systems, often associated with system administration credentials. Privileged user management is therefore an important extension to the consideration of identity and access management.

Encryption and Pseudonymization

One of the few specific references to technology included in Article 32 is the inclusion of encryption and pseudonymization (often also known as tokenization). It would be easy, upon a cursory read of GDPR, to conclude that encryption is both recommended and a straightforward route to compliance (or at least reduced risk). Certainly, encrypted data may be regarded as non-personal data, and may mean a reduced requirement for mandatory breach notification (see Article 34). However, encryption is not a trivial undertaking.

Firstly, encrypting data can reduce its utility: for example, one cannot sort or search encrypted data, and it is useless for reporting and analytics purposes. There are encryption approaches that preserve the format of data and also preserve business functionality, but these approaches are not yet commonly in use. In addition, encryption entails key management, and few companies have the experience or inclination to manage encryption keys properly. Key management can become a critical element of a business' operations because of the consequences of poor key discipline (which could be catastrophic if the keys are lost or deleted). Many companies investigating encryption key management realize that they have neither the knowledge nor the willingness to proceed and hence third-party key management services are gaining in popularity.

Auditing and Forensics

One of the most important, but least discussed, areas of compliance is the recording of processing (see Article 30). These records are designed to maintain evidence of personal data processing across the organization, and need to be kept up to date in order to be made "available to the supervisory authority on request."

This means that the ability to conduct audits of processing, including access to personal data records, is essential. In addition, the ability to conduct forensic investigation after an incident (including but not limited to a data breach) also indicates a high degree of capability and intent to comply. Auditing and forensics therefore act as indicators that help to reassure a regulator that best practices are being followed, which may mitigate the levying of fines and other sanctions.

Thinking About Cloud and Data Transfers

One of the main concerns of GDPR, as illustrated by the seven articles on the subject, is data transfers (Articles 44 to 50). Data transfers involves the movement of personal data to so-called third countries (that is, countries that are not members of the EU). The concern is to ensure that data controls adequately protect the data outside the EU's jurisdiction. To avoid this, broad mechanisms exist to enforce the strict control of data transfers beyond the EU, and an extra-territoriality clause extends the scope of any personal data irrespective of the location data or its processing (see Article 3).

It is important to note that transfers of personal data outside the EU are completely acceptable and legal. What is essential to note is the legal mechanism that underpins this transfer, and there are several such approaches (such as consent, binding corporate rules, model contract clauses, and specific bilateral agreements such as EU-US Privacy Shield). Some countries are deemed to have data protection laws that are "adequate" (that is, equivalent) to GDPR, and transfers to these countries are also legitimate.

Data transfers are specifically important to cloud services that involve the movement of data beyond the EU. Even in cases where data is stored within a datacenter located in the EU, access of that information from a third country counts as a data transfer. Due consideration of data transfers via the cloud is an important part of compliance. In particular, the obligations on cloud service providers are substantial: GDPR introduces the concept of shared liability between data controllers (companies that determine the purpose and means of processing) and third-party data processors that actually carry out the processing. This means that cloud service providers (as processors) are effectively "on the hook" with regards to compliance, and are subject to the same penalties and sanctions as companies that control the data.

PROTECT AGAINST DATA BREACHES

Breach Detection and Notification

In IDC's discussions with supervisory authorities, we are reassured that the regulators understand that sometimes breaches happen. No system could be 100% secure, and mistakes will occur. Breaches are the moments of truth that determine how effectively an organization has prepared for the worst case. Article 83 contains a handy list of aggravating or mitigating factors that will be used to determine the severity of sanctions. In essence, such factors are evidence of the extent to which the unfortunate company tried hard (or not) to comply with GDPR. Evidence of good intent and sound working practices, supported by a comprehensive trail of data processing activities, will be looked on favorably by a regulator.

Early detection of a breach, and a rapid response, are also indicators of good practice. A primary factor of consideration is whether the company itself detected the breach and advised the supervisory authority. Detecting a breach, as early as possible, is a sign that a company is trying hard. Having a defined and tested incident response plan is good practice: that plan should include the mandatory notification requirements, technical remediation, and a communications plan for information flow to stakeholders.

Mandatory notification requirements come in two parts. The first is an obligation to inform the supervisory authority (the regulator) within 72 hours of discovering the breach, where feasible (Article 33). The 72-hour guideline is not fixed, but companies must have a good reason why they were unable to meet this timescale. The second obligation is to inform the subject of a data breach, "without undue delay" (Article 34). Note that there is no 72-hour window in which to advise affected data subjects. Both notification requirements demand that the affected company declares the nature and extent of the breach, as well as the likely consequences to data subjects.

Information Governance

Ultimately, compliance with GDPR concerns information governance. Organizations need to have a comprehensive view of the information under their control and the governance regime that sets data processing policy and protection. Extending this regime to emerging technology use cases can be challenging. In the world of IoT, for example, the collection of massive amounts of personal data can be achieved quickly and easily, through the plethora of devices, sensors, and other information gathering mechanisms. Collecting personal data, then, is not the problem. The challenge is knowing what data is being gathered, for what purposes, and under what legal pretext. Companies must decide whether the data that they are collecting in their IoT deployments is of sufficient value to outweigh the risks of non-compliance with GDPR. This represents a fundamental shift in mindset of companies: normally, the assumption is that data will be retained in case it is useful either now or at some point in the future. But holding data for longer than is necessary is itself non-compliant, and increases the consequences of a data breach.

GDPR and Managed Services

Many organizations will examine the incoming requirements of GDPR, and the increased emphasis on security of personal data, and conclude that this is more effectively managed by a third party. Managed security services (MSS) is one of the fastest growing areas in security, driven not only by a global scarcity of security skills, but also by the opportunity to optimize security operations and to outsource non-core business functions. It may also be possible to outsource the DPO function to a managed services provider, assuming that such a service contract does not create conflicts of interest.

CALL TO ACTION

1. Establish the management of your GDPR program by selecting a leader who can coordinate input from stakeholders from every part of the business and related community. It matters less from where this leadership is sourced. Remember that the introduction of GDPR represents a program of work that will become normal business practice, so plan the incorporation of new data processing activities into everyday work.
2. Discover the extent and nature of your risk exposure – and the scale of effort required to achieve compliance – through a data visibility assessment. This identifies the personal data held within the company, documents the sensitivity (special categories) of data, where the data physically resides, how it flows throughout the organization, and the purpose of the data being stored and processed.
3. Assess technology's role early in the program. GDPR cannot be solved without technology, and security technology is particularly important. Remember that it is not just a matter of selecting and implementing security technology as part of the GDPR program that is important. GDPR should change organizational behavior, and technology changes should be considered at all stages of the life cycle of personal data. DPIAs will mandate a continuous awareness of technology's impact.
4. Review the impact of GDPR, and its effect of increasing business risk, on your existing data breach protection and detection mechanisms. Protection comes in three parts: the first is controlling access to the data, using identity and access management. The second part is classifying, monitoring, and controlling the data in order to limit its exposure. DLP is a core element in this protection, as it stops sensitive information from leaving the organization. The third part is protecting the organization from the consequences of a data breach. This involves defining – and testing – a breach incident response plan that incorporates mandatory breach notification requirements.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC U.K.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Restrictions

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015
www.idc.com.