Executive Brief

GDPR: A Primer for Getting Started Towards Compliance

Sponsored by: Dell Security

Duncan Brown
March 2016

THE BACKGROUND TO EU DATA PROTECTION LAW

The last 20 years have seen a substantial change in the way in which companies and consumers transact across the Internet. In 1996 the web was still emerging as a useful technology, and most people's experience of the Internet was based on email. The dotcom boom had yet to happen and most businesses were unaware of the radical changes that the new technology would bring.

Fast forward 20 years to the present day and the ways in which technology is used have been transformed. Today's innovative technologies of cloud, mobile, analytics and social are approaching ubiquity, if not in deployment at least in awareness. Everybody in the developed world (and a large chunk of the developing world) seems to have a smart phone with high bandwidth connectivity at all times. The ways in which we gather information, learn, communicate, navigate, shop and bank have changed fundamentally. Our televisions, refrigerators and cars communicate with us, and increasingly with each other and the external environment.

The past 20 years have also seen a radical restructuring of the dominant players in technology. Google, Facebook and Twitter did not exist in 1996, and most companies did not even have a website. Now these companies and many others offer everyone the means to constantly stay in touch with their friends and relatives. Companies gather information about us every time we search, browse and click. For the most part, the information gleaned from our online habits is useful to us, as it is used to provide better and more relevant information back to us. For example, a website with understanding of demographic and geographic information can provide highly contextual search results, making the service more useful.

The one area that has not advanced over the past two decades is data protection legislation. The existing laws within the EU date from 1995 and were drafted with no knowledge or prescient understanding of the technology that would emerge. Across the EU, more and more consumers, lobbyists and governments have been becoming increasingly concerned at the amount and type of data being gathered on users of the Internet, often without their explicit consent. While there is an active and healthy debate regarding the balance between privacy and utility of gathering information, there is no doubt that existing law has not kept up to date with technological capabilities in 2016.

In December 2015 the EU finally agreed to the terms of the new law that will bring data protection legislation up-to-date and into the modern age.

What is GDPR?

The General Data Protection Regulation (GDPR) is a new piece of legislation that was agreed in December 2015, and will be effective from early 2018 (precisely two years after its publication in the Official Journal of the European Union). This single Europe-wide regulation removes the complexities that businesses currently face around complying with multiple local regulations across the EU. Currently, each of the 28 EU states interprets the existing rules in their own way, making compliance across the region complex and expensive. GDPR unifies EU data protection legislation, simplifying processes and legal obligations for any country dealing with more than one EU state. However, the scope of GDPR substantially increases the obligations on firms dealing with EU citizens' personal data. The penalties for non-compliance are substantial, the primary effect of which will be to raise data protection as a business risk directly into the boardroom.

Don't put off early consideration of GDPR by the two-year implementation period. The scale, complexity and business criticality of GDPR means that it will take (at least) two years for most companies to achieve full compliance. Most companies need to start now.

KEY FEATURES OF GDPR

GDPR comprises 91 articles, so its scope and detail are extensive. Much of GDPR relates to the processes and legislative framework for data protection, which has limited impact on technology strategy. However, some of the key features of GDPR have a substantial impact on security requirements, which will translate into both process and technology changes.

- **Personal data**. GDPR's scope is limited to personal data, but the EU has a very broad definition of what personal data can mean. For example, an IP address that can identify a specific user's device is regarded as personal data. Many organizations have a poor understanding of the scope of personal data, and inefficient (or worse, no) processes to track their use and protection of such data. GDPR pertains equally to customer and employee data, so it encompasses most firms.
- **Data breach**. GDPR defines a data breach as an action that leads to "the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." A data breach need not necessarily be caused by a security breach. However, the EU regards a loss of encrypted data as not constituting a data breach, and many companies will use this guideline as justification for encrypting as much data as deemed necessary. Note that a security breach need not result in a data breach. A hacker may be roaming within the corporate network but may be unable to exfiltrate data if it is protected or encrypted.
- **Continuous compliance and audit**. GDPR introduces the concept of continuous compliance, in which an organization must regularly carry out audits of compliance. This means not once a year, or even once every six months, but arguably on a weekly or even daily basis. At any point an auditor can ask a company to demonstrate compliance, and the company must be able to do that more or less immediately. This places a steep requirement on an organization to demonstrate compliance, and we expect the collection and management of user activity logs and access credentials to be a key enabler of proving such compliance.

Who Does it Apply to?

Other than most small companies with 250 employees or less, and some exceptions that relate to national security, all companies that process EU citizen data are subject to GDPR compliance.

GDPR also applies to the collection of personal data of EU citizens. It is important to understand that the new regulations apply irrespective of whether the data controller or processor have a physical presence in the EU. In practical terms, this extra-territoriality applicability means that any provider of data services that processes EU citizen data must be compliant. The implications here are important: any provider that is not based, or has no presence, in the EU is included. This means, for example, cloud service providers based in the US.

Why Should I Care About GDPR?

GDPR changes the game for organizations because of two key features:

- The fine for non-compliance with GDPR reaches a maximum of 4% of global revenue. The prospect of receiving such a fine gets boardroom attention. No board member will want to have to explain to shareholders why profits and stock price have fallen due to a data breach resulting in a substantial fine.
- GDPR introduces the concept of mandatory breach notifications. For almost all companies within the EU this will be the first time that they will have had to, by law, admit to data breaches. While the extent of reporting breaches is limited to the Supervisory Authority and affected customers, bad news travels quickly, and such information would leak quickly into the public domain. Organizations then have the media spotlight shone directly upon them.

Increased visibility of risk assessment, controls and mitigation will drive not only new processes but also technology to support and enforce those processes. Tools that automate audit trails, and assist in forensics investigations should things go wrong, will be attractive.

The timescale for achieving compliance is tight, and we think that organizations of any sizeable scale and complexity will struggle with even the first steps in compliance, such as understanding what data they have and its sensitivity. Automation of data classification may solve this fundamental issue, and there are other approaches to identifying and securing sensitive data. In addition, some basic user security controls will be enhanced: access to sensitive information will be more tightly controlled, meaning better identity and access management integrated into document and process flows.

The speed of implementation, together with uncertainties over wording and interpretation, will drive substantial services revenues, especially in the 12 months immediately after regulation agreement. Firms will need a lot of help in deciding what to do, and then how to achieve compliance.

The GDPR Enforcement Regime

European Data Protection Board

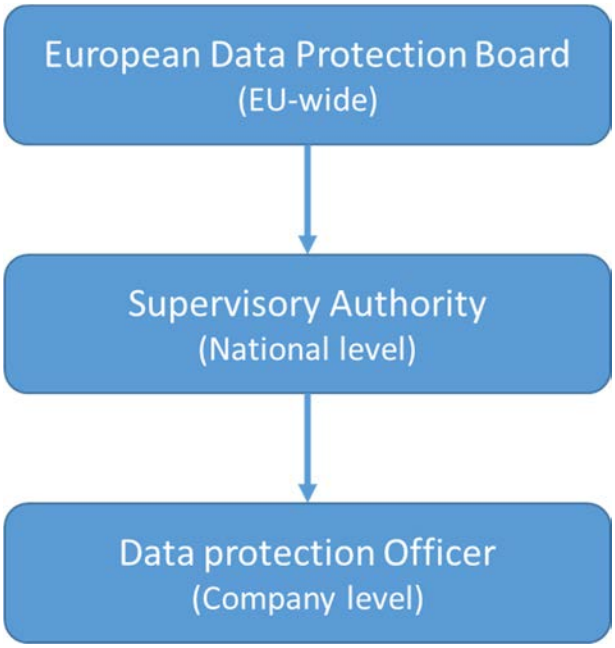
A European Data Protection Board (EDPB) will replace the Article 29 Working Party, which is the current overseeing body. The EDPB will comprise the head of the supervisory authority of each member state and the European Data Protection Supervisor. The main purpose of the EDPB is to ensure consistent application of the GDPR across all 28 member states. It will also issue guidelines, recommendations and best practices for distribution to companies via the Supervisory Authorities (SAs – see below.)

Supervisory Authority

Each EU member state will have a Supervisory Authority (SA). All EU countries have bodies that are already performing the broad functions of an SA. Examples are: The Information Commissioner's Office (ICO) for the UK; the Commission nationale de l'informatique et des libertés (CNIL) in France; Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BDI) in Germany; and De Autoriteit Persoonsgegevens (formerly College bescherming persoonsgegevens) in the Netherlands.

FIGURE 1

The Hierarchy of GDPR Enforcement



Source: IDC, 2016

GDPR describes a close working relationship between SAs, which work at a national level, and Data Protection Officers (DPOs) in individual companies. DPOs must register with their SA, and the SA will monitor compliance via liaison with the DPOs. SAs may also offer to confirm compliance with GDPR on request from a DPO, for a fee.

Ultimately it is the SA that will decide on the recourse taken on a company that suffers a data breach, and how much the fine (if any) will be. However, GDPR is clear that any fine will be related to the extent of the breach and the degree to which the errant company has tried to comply. In other words, if you can demonstrate a strong effort to comply, can detect a breach early, and can report on the extent and severity of the breach quickly, then an SA is likely to been lenient.

Data Protection Officer

GDPR introduces the concept of a Data Protection Officer (DPO). Under GDPR the appointment of a DPO is mandatory for most public bodies and any organization processing personal data on "a large

scale". Currently, it is not clear what the benchmarks are for large scale, but early drafts of GDPR indicate a level of 5,000 or more data records.

This DPO will report (most likely) to the audit committee of the board, not executive management, and be responsible for ensuring compliance with GDPR; The DPO has an assured tenure with no prospect of being fired (other than for gross incompetence). The DPO is responsible for conducting regular audits of GDPR compliance, which means that firms will have to demonstrate their compliance on a regular basis. Having one person responsible for data management and governance across the entire organization should have positive effects other than GDPR compliance. Currently, data is siloed by application, and copies of data are often made for test, development & analytics, and back-up & disaster recovery purposes. Streamlining these various data-related processes will provide a better overview of all data assets within an organization, and enable the DPO to drive a more efficient data management regime across the entire organization.

The DPO is also responsible for liaising with the supervisory authority, which includes notifying the SA of all data processing activities, and any data breaches. Because the DPO has secured tenure of appointment, does not report to the executive but to the board audit committee, and is obligated to advise the SA of data processing activities, it is unlikely that a DPO would not exercise their responsibilities.

A DPO need not be a dedicated role and in many cases the function will be performed by a Chief Risk Officer, general counsel or an individual with similar professional qualities. It is also not required that a DPO must be an employee of the firm: many legal and consulting firms will offer DPO-as-a-service propositions.

TECHNOLOGIES THAT CAN HELP IN ACHIEVING COMPLIANCE

A range of technologies will help organizations achieve compliance with GDPR. Some of the more obvious capabilities include data loss prevention (DLP) and data classification. IDC believes that the importance of encryption is substantial, while of the relevance of IAM and network security is underestimated.

Encryption

Many organizations will review of the GDPR and conclude that the safest bet will be to encrypt all of the personal data under their control. The interest in encryption technologies has increased markedly since the initial drafting of GDPR. The main reason for this is that in a case where data is lost outside the organization but it is encrypted this will not constitute a data breach. This is because with properly encrypted data the personal details held within the data are not accessible by unauthorized parties. There would be no obligation to contact the SA and no fine would be incurred.

However, encryption is not as simple as that. Data is typically held across a number of platforms and locations and an "encrypt everything" policy must span these heterogeneous environments. For example, organizations would have to deploy data security encryption across the broadest range of devices and platforms, from iOS and Android mobile devices, cloud data stores, external media, to PCs and Apple Mac laptops.

A policy-based regime of data protection, involving encryption where appropriate, is a more intelligent approach. Such a regime would encompass:

- Encrypted and secure data access across multiple endpoints from a common management platform, for ease of administration
- Automated generation of automatic audit trails that offer proof of end-to-end data security
- Prohibition of unprotected personal data from leaving the organization on USB flash drives or other forms of removable media
- Protection of data from unwarranted access, thus reducing the risk of internal breaches from insider threats

Encryption helps protect both against the likelihood of a security breach arising in the first place and the adverse consequences of the breach, both for the individuals whose data are compromised and also for the business in terms of mitigating its liabilities following the breach.

We suggest that the SA should be notified on an advisory basis of the loss of encrypted data. This is because a security breach (if not a data breach) has occurred, and it is useful to keep the SA informed of such an event. It may also turn out that the encrypted data is not properly or sufficiently encrypted, and so a data breach is likely to follow. Advising the SA early presents a low risk approach, as opposed to finding out much later that a data breach has in fact occurred, and the mandatory breach notification timeline (72 hours) has passed.

Identity and Access Management

Identity and access management (IAM) is an important category of technology in the delivery of GDPR compliance, because through effective IAM an organization is able to show who has or had access to what, why, when, and what they did with that access; it is a core principle of defense of important data. The establishment, control, and governance of valid credentials should be a primary source of protection for all sensitive data. In other words, a firm understanding of who has access to what, who approved that access, and what they have done with that access.

Key components of IAM that must be controlled, audited, and managed include the accounts (or identities) that are the basis for access; the authentication mechanism — such as a password or multifactor token — that grants access based on the identity; and authorization, or collections of rights associated with the identity and invoked by the authentication activity.

A stolen credential or account, a compromised authentication action, or misappropriated rights can all be deemed a violation of the regulation.

IAM can be divided into three main categories, each of which is relevant for the regulation:

1. Access management: The technologies and practices that provide users with appropriate access to resources including applications, networks, and databases. Key technologies that help secure access management include single sign-on, web access management, federation, password management, multifactor authentication, and directory management.

2. Privileged account management: Technologies and practices that control and monitor the use of administrative credentials including those on applications, networks, infrastructure, and servers. Privileged account management technologies eliminate the sharing of credentials, delegate rights based on role and need, and audit activities performed with the credentials.

3. Identity governance: Technologies and practices that provide the attestation/re-certification activities required by regulations and best-practice frameworks. Governance is essentially

ensuring that the right people have the right access to the right resources in the right way and that it can be proven to whomever needs to know that the organization is doing it all correctly.

However, IAM is both a proactive defense – controlling who accesses resources and under what circumstances – and a reactive forensic tool. Through log activity analysis, IAM can determine which user (or which user's stolen credentials) was responsible for a data breach and whether the activity was legitimate (but mistaken) or deliberate and malicious.

This forensics approach is important because in deciding the severity of the breach and the level of fine applied the SA will assess any deficiencies in the compliance regime. Firms that can demonstrate strong access controls (for identities, authentication, and authorization) and an ability to trace the events that led to the breach will be granted leniency.

Network Security

It is tempting to think that traditional perimeter protection is no longer necessary, or at least has become marginalized. However, it still remains the case that attacks are more likely to be conducted across the network, and so perimeter protection remains the first line of defense.

Today's cybercriminals employ several complex techniques to avoid detection as they sneak silently into corporate networks. Their threats are often encoded using multifarious complicated algorithms to evade detection by intrusion prevention systems or traditional firewalls. Also. the growing use of cloud and mobile computing, SSL-encrypted web traffic, bring your own device (BYOD) policies – and the rise of shadow IT – has added new levels of risk, complexity and cost to securing an organization's data and intellectual property. Organizations of every size must now combat a wide range of increasingly sophisticated threats, including advanced persistent threats (APTs), cybercriminal activity, spam and malware; so perimeter protection remains the first line of defense to protect and secure companies' data.

To combat growing security challenges, organizations are migrating away from traditional firewalls that focus only on stateful packet inspection (SPI) to next-generation firewalls (NGFWs). NGFWs have transformed network security by providing much more robust protection against emerging threats, featuring deep packet inspection (DPI), real-time decryption and inspection of SSL sessions, and full control and visualization of application. NGFW logs are useful in the forensics activity following a suspected breach. It is important to be able to trace activity on the network, including user or device credentials, network traffic origination and destination, and contents of transmitted packets of information.

Millions of workers today use corporate and personal laptops, smartphones, tablets and other mobile devices not only for business, but also for private purposes. With so many mobile devices accessing enterprise networks, mobile data security has become one of the top challenges for IT security professionals: corporate data can (and does) go anywhere, and if organizations can neither manage it nor track it, then it becomes difficult to protect it.

So when it comes to data loss and data theft with mobile workers, there are four points of vulnerability:

- Data at rest on backend systems
- Data in transit between the mobile user and the backend services or system
- Data on the mobile device itself
- Data to apps and into the cloud

All of the above data-security considerations can be addressed by many by different products and solutions. The right approach will ultimately be the solution (or a combination of solutions) that fosters the secure flow of corporate data while supporting IT and enabling employees to use the devices and applications they need to optimize productivity, like secure mobile access platforms.

Email remains the most widely used vehicle for distributing business data. Yet this communication poses a considerable risk for organizations of all sizes, as they must protect their intellectual property and sensitive information from inappropriate distribution while also ensuring compliance with new laws and regulations governing the protection of confidential information.

Adding email compliance and encryption services to the email security solution enables organizations to meet both regulatory and corporate requirements. The joint solution enables organizations to identify email for compliance policy enforcement; apply multiple email governance policies; monitor and report on email traffic; and ensure the secure exchange of sensitive and confidential data.

KEY INITIAL STEPS TOWARDS GDPR COMPLIANCE

There are 91 articles in the GDPR and though they do not all relate to an individual organization's compliance obligations there remains a substantial amount of effort in reaching, maintaining, and proving compliance. Clearly, some organizations are in a better place to start with than others. But there are certain prerequisites that all organizations can start with in order to set a course in the right direction.

Find the Data

Many organizations fall at the first hurdle with GDPR, in that they do not have full knowledge of the type and location of personal data they control or process. Data is easy to copy, often for good reasons such as for reporting or analytics. But this leads to duplication, which is hard to control. An additional challenge that many organizations have is that they underestimate the types of data that fall within the GDPR. According to GDPR, personal data is "any information relating to an identified or identifiable person". Identity can be revealed through a number of identifiers and include physical, physiological, genetic, economic and social attributes. It would, for example, include a specific IP address tied to a computer used by an identifiable person.

Assess the Risk

Not all data carries the same risk. We advise companies to apply a simple 3Rs assessment to the data that they control:

- What data will make a company **Rich**, through competitive advantage, operational excellence, or some other means?
- What data will **Ruin** the company if they have it leaked, stolen or copied?
- What data must a company keep for **Regulatory** purposes?

This third category speaks directly to compliance with GDPR. But we strongly urge companies not to limit their data protection activities to reaching compliance. The scope of GDPR relates only to personal data. Other forms of sensitive data, such as intellectual property, are outside the scope of GDPR. Techniques used in the protection of personal data may be wisely extended to other types of important data. There is more to data protection than compliance with GDPR, and the importance of data extends beyond that of the personal type.

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-insights-community.com
www.idc.com