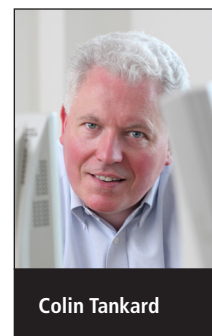


What the GDPR means for businesses

Colin Tankard, Digital Pathways



The long-awaited General Data Protection Regulation (GDPR) of the EU was provisionally agreed in December 2015.¹ The final details are still being ironed out, but publication of the final version of the regulation is expected around July 2016.² There will then be a two-year waiting period until every organisation that does business in, or with, the EU must comply with the regulation. Since it is a regulation, not a directive, compliance is mandatory, without the need for each member state to ratify it into its own legislation.

Previous data protection legislation had become fragmented across the EU as different countries added to the basic principles enshrined in the original directive of 1995. Some countries added clauses to require breach notification and sanctions currently vary widely. Some countries, such as Spain, fine heavily and often; others, such as France, hardly mete out any fines at all. This has resulted in the situation where organisations doing business across the region face a legal minefield of differing interpretations of data protection.

Another reason why new legislation was needed is that the original directive of 1995 was formulated in what now appears to be a different technological era. Back then, just 1% of the world's population was using the Internet, but today it is almost ubiquitous across the EU. Cloud computing and social media were not known then, nor were smartphones or tablets. Today, the vast majority of information is produced and consumed electronically, making it harder to protect.

The major changes

The GDPR expands the scope of data protection so that anyone or any organisation that collects and processes information related to EU citizens must comply with it, no matter where they are based or where the data is stored. Cloud storage is no exception.

The definition of personal data has also been expanded. It states that personal data includes information from which a

person could be identified, either directly or indirectly. Under the new definition, identifiers such as IP addresses and cookies are included as personal information.

Prior to the GDPR, there has been no uniform legislation regarding breach notification, except for electronic communications service providers under the ePrivacy directive. Some countries added provisions to their legislation to cover breach notification, but not all. The GDPR introduces mandatory breach notification unless the breach is unlikely to result in a risk to the rights and freedoms of the data subjects concerned. A particularly onerous demand in the new regulation is that organisations suffering a data breach must notify data protection authorities within 72 hours of its discovery.

"A particularly onerous demand in the new regulation is that organisations suffering a data breach must notify data protection authorities within 72 hours of its discovery"

Sanctions for non-compliance with the regulation have not only been made uniform, but they have been increased considerably. For a minor breach, organisations can be fined up to 2% of their worldwide revenue or 10 million euros, whichever is higher, although a warning can be given for first offences. For more serious violations, fines of up to 4% of worldwide revenues can be imposed or 20 million euros, whichever is higher.

Organisations with substantial data processing activities are required to appoint a data protection officer, who must function independently of the business. However, one such officer can be shared among organisations.

"Under the GDPR, notification is only required in the member state deemed to be the headquarters of the data controller or processor, or where most of the processing takes place. This will reduce the costs and efforts of compliance for organisations"

Data impact assessments will also be required where processing of data is deemed to be high risk for the rights and freedoms of the data subjects involved. Such an assessment must detail the safeguards, security measures and mechanisms that are in place for addressing risk and ensuring compliance. Both of these demands will raise the cost of complying with the regulation for organisations.

Individual rights

Another area that will make compliance harder is that the rights of individual data subjects are being expanded. They must unambiguously give their consent for their data to be processed, which must be informed and voluntary; have the right to access information held on them; and may object to the processing of their data where there are legitimate grounds for doing so. One new requirement, which has been perceived as controversial by some, is that the right to be forgotten has been solidified, requiring data controllers and processors to remove data that is

considered to be inadequate, irrelevant or no longer relevant. This will require that organisations know exactly what information they hold and where it is stored.

However, one thing that will make it easier for data controllers and processors is the introduction of the one-stop-shop concept. Previously, it was necessary to notify the data protection authorities in each EU member state before processing could begin, which was a time-consuming and often costly process. Under the GDPR, notification is only required in the member state deemed to be the headquarters of the data controller or processor, or where most of the processing takes place. This will reduce the costs and efforts of compliance for organisations.

Data transfers are still prohibited to jurisdictions deemed to have inadequate levels of security, unless authorised by a supervisory authority. This requires the negotiation of contracts for the data transfer. Binding corporate rules, standard data protection clauses adopted by the European Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority may all be used for enabling the international transfer of data. Of these, binding corporate rules are considered to be the gold standard for data transfer. EU model clauses remain valid.

“According to Ovum, 52% of organisations believe that the GDPR will result in fines for their business and 68% feel that it will dramatically increase the costs of doing business in Europe”

However, the Safe Harbour Agreement that was negotiated with the US has been deemed invalid and may no longer be used owing to fears that it was enabling bulk surveillance by authorities. A new agreement has now been reached in the form of a Privacy Shield Agreement, which creates multiple enforcement mechanisms for data protection authorities, as well as multiple paths for remedies for EU citizens. Although not all the details are yet known, it is expected that requirements for consent, as well as for securing data, will be higher.

Time to get your house in order

Many are worried about the impact of the GDPR. According to Ovum, 52% of organisations believe that the GDPR will result in fines for their business and 68% feel that it will dramatically increase the costs of doing business in Europe, with some believing that their budgets will need to increase by some 10% to deal with its ramifications over the next two years.

Two years may seem a fair amount of time to prepare, but it will pass quickly. The time to start preparing is now. Polls conducted during a recent webinar sponsored by Vormetric found that 48% of attendees are already preparing for the GDPR, but 30% did not know whether they were or not. This is despite 91% stating that they were at the very least worried about non-compliance.

What is required for compliance

As with the 1995 directive – and, indeed, many directives and regulations – the GDPR is not prescriptive in the technologies that should be used to achieve compliance. This is nothing out of the ordinary, since any legislation that is too prescriptive runs the risk of quickly becoming obsolete, especially given the rapid pace of technological change in today’s world.

Rather, the GDPR states that organisations need to implement appropriate tech-

nological and operational safeguards for securing data, including putting in place strong privacy controls. It states that organisations should adopt internal measures that meet the principles of data protection by design and default. What this means in practice is that data protection and privacy must be considered right from the beginning of the security planning process.

“Organisations should adopt internal measures that meet the principles of data protection. Data protection and privacy must be considered right from the beginning of the security planning process”

There is, however, one exception to the regulation being non-prescriptive in terms of technologies. Encryption is specifically called out, along with pseudonymisation, as an appropriate safeguard for securing data. If they encrypt data, organisations that suffer a data breach are not obligated to notify data subjects as the data is considered to be adequately protected, as long as the encryption was properly implemented.

Keeping pseudonymous data separate

Where pseudonymisation is used, in which data is processed in such a way that it cannot be attributed to a specific individual, pseudonymised data must be held separately from any additional information stored in clear form to ensure

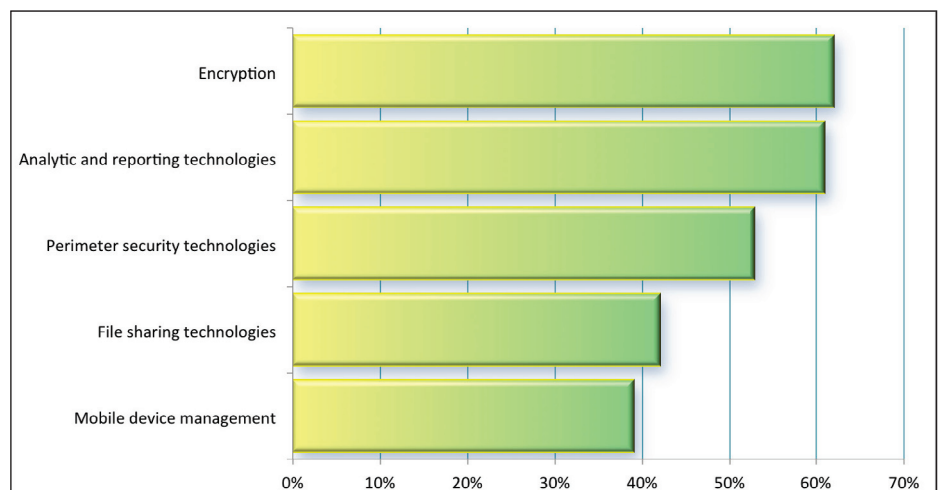


Figure 1: Technology investments for achieving data protection regulation compliance.

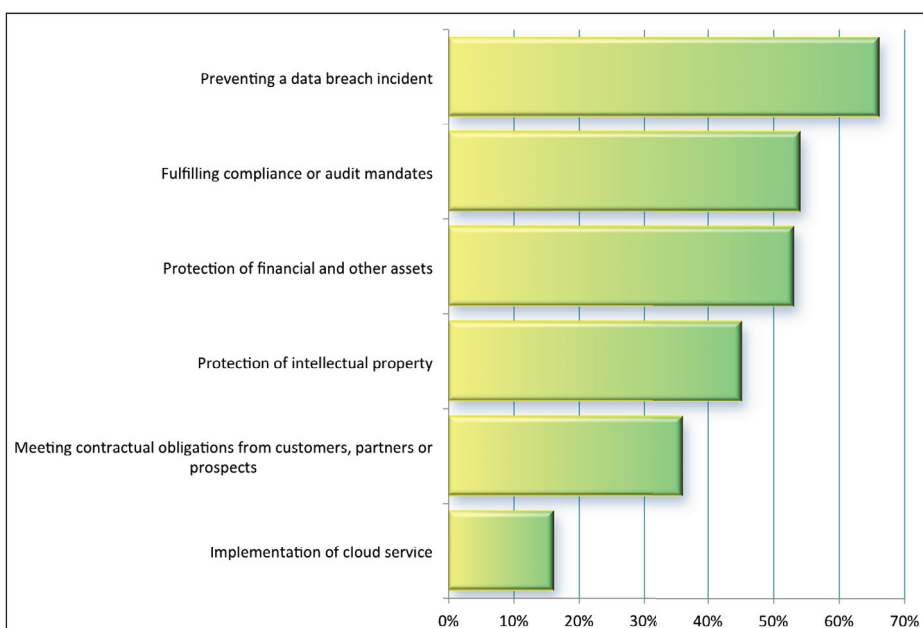


Figure 2: Primary drivers for encrypting data.

that it cannot be attributed to a specific individual. As Figure 1 shows, encryption is considered to be the top technology control for data protection.

A separate survey looked to gauge what the primary drivers for encrypting data are, as shown in Figure 2.

Law firm Baker & McKenzie states that there are five initial steps to make before considering measures to take to achieve compliance. These are:

- Assess whether or not you will fall within the scope of the GDPR.
- Understand the new compliance obligations, decide how to comply with them and assess their operational impact.
- Identify new responsibilities and risks and consider how to address those risks.
- Understand the market, in particular what data controllers will require from processors moving forward and what your competitors will be willing/not willing to agree to vis-à-vis data controllers.
- Devise a strategy for negotiating processing agreements.

Technology controls

As stated above, encryption is specifically called out in the GDPR and should be the default option for protecting all data, both when data is being transmitted and is in storage. This includes both structured and unstructured data stored in databases, or included in spreadsheets,

word documents, presentations, emails and archives. Even when data is stored in the cloud or on endpoints, cryptographic keys should be kept with the organisation responsible for collecting or processing the data to prevent the opportunity for inappropriate access by third parties, which could lead to charges that the encryption was not adequately implemented. Strong security controls should also be applied within the organisation to ensure that only those entitled to can access keys.

“Should data be put to uses other than those to which the data subject gave his or her consent, the data subject may seek redress in the form of compensation”

Even though data is being encrypted, it is still good practice to minimise the amount of data collected. This will not only help to reduce the burden of protecting massive datasets, but will also mean that the organisation is less likely to fall foul of requirements in the GDPR that data only be used for purposes for which it was collected, and no other. Should data be put to uses other than those to which the data subject gave his or her consent, the data subject may seek redress in the form of compensation.

While encryption is an extremely good tool for data protection, it is not sufficient

by itself. Organisations should ensure that they have adequate access controls in place to prevent unauthorised access when the data is decrypted and to control what users can do with the data according to their role. For example, a systems administrator needs to be able to perform management tasks such as back ups but should not be able to read the content of the data – eg, in an HR system the server operation team need to be able to take care of the system and know that data is there but should not be able to read the contracts of employment. This applies, in exactly the same way, for applications accessing data, which should have access controls applied to them.

“All security systems should be continuously monitored, taking into account all the risks associated with data processing and storage, including inadvertent loss or destruction”

For this reason, the controls should be tied to back-end databases such as Active Directory, which will help in defining granular entitlements and ensuring that they are kept up to date as things change, such as a person being promoted or moved to another role.

Where organisations find the management of Active Directory very complex there are tools available, such as those from 8Man, that enable a business to have a graphical view of user rights and easily remove or add controls to ease the burden of user management. Furthermore, linking the authentication of users or applications to the encryption enhances the controls available within Active Directory and provides a fine grain audit trail of user access to data that further benefits the ability to monitor and track the ‘insider threat’ that faces many organisations.

Entitlement to data

The use of strong authentication will help to ensure that the people accessing data are who they say they are so that a user with entitlements to access data cannot pass those entitlements on to someone else.

In order to test, assess and evaluate that

controls are effective and to ensure that they are working at all times, all security systems should be continuously monitored, taking into account all the risks associated with data processing and storage, including inadvertent loss or destruction. Integration with security information and event management systems will provide visibility over events occurring over the network, which can be analysed to ensure that security and compliance objectives are being met. This will also provide the audit trail that is required to prove that controls are working properly.

Industry standards and best practice frameworks

The use of industry standards and best practice frameworks can help organisations to manage the risks that they face while adding greater efficiency and sustainability to their operations. They enable best practices to be embedded into an organisation.

The CIS critical security controls, which are listed in Table 1, can be considered to be a checklist of the controls that organisations should have in place to ensure that their security posture is up to the task of managing risk. These controls are a recommended set of actions that will provide organisations with specific and actionable ways to boost their cyber-security capabilities, allowing organisations to prioritise actions should an attack occur in order to achieve the best results with the least effort.

“The time and effort required to achieve compliance will vary greatly from one organisation to another, but it is well worth the effort”

Security standards such as ISO 27001 and ISO 27002 will help organisations to ensure that they have in place effective information security programmes. ISO 27001 was originally created with the intention of helping to manage the security of government services and citizen data in

the hands of service providers. The use of ISO 27001 will help to ensure the principle enshrined in the GDPR that appropriate technological and organisational measures are in place to protect information. It will help organisations to define responsibilities, such as who is responsible for certain information assets and who can authorise access to data. ISO 27001 provides independent accreditation for information security management systems, while ISO 27002 is a code of practice that is not accredited by external parties. The use of either will help to show that an organisation has put in place strong controls should that organisation ever need to address issues related to negligence.

Conclusions

After years of wrangling, the GDPR is now a fact and compliance deadlines are looming. The time to start preparing is now. In fact, Digital Pathways has been promoting technologies that link access control to encryption for over 20 years. Organisations need to ensure that they are not caught out and face sanctions for non-compliance. With the right precautions in place, organisations should have little to fear. The time and effort required to achieve compliance will vary greatly from one organisation to another, but it is well worth the effort.

About the author

Colin Tankard is managing director of data security company Digital Pathways, which specialises in the design, implementation and management of systems that ensure the security of all data, whether at rest within the network, in a mobile device, in storage or in transit across public or private networks.

Resources

1. ‘General Data Protection Regulation’. Wikipedia. Accessed May 2016. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation.
2. ‘Regulation (EU) 2016/679 of the European Parliament and of the Council’. Europa. Accessed May 2016. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

Control	Description
CSC 1	Inventory of authorised and unauthorised devices
CSC 2	Inventory of authorised and unauthorised software
CSC 3	Secure configurations for hardware and software on mobile devices, laptops, workstations and servers
CSC 4	Continuous vulnerability assessment and remediation
CSC 5	Controlled use of administrative privileges
CSC 6	Maintenance, monitoring and analysis of audit logs
CSC 7	Email and web browser protections
CSC 8	Malware defences
CSC 9	Limitation and control of network ports, protocols and services
CSC 10	Data recovery capability
CSC 11	Secure configurations for network devices such as firewalls, routers and switches
CSC 12	Boundary defence
CSC 13	Data protection
CSC 14	Controlled access based on the need to know
CSC 15	Wireless access control
CSC 16	Account monitoring and control
CSC 17	Security skills assessment and appropriate training to fill gaps
CSC 18	Application security software
CSC 19	Incident response and management
CSC 20	Penetration test and red team exercises

Table 1: SANS CIS critical security controls.