BlackBerry

Why GDPR Is Important and What You Need to Do to Get to Grips With It

CIO
Strategic Marketing Services

Why GDPR Is Important and What You Need to Do to Get to Grips With It

Preparedness, technology tools, smart thinking and expert counsel will help you meet the tough challenges of incoming rules on data protection

The General Data Protection Regulation (GDPR) will have a dramatic effect on the way that organisations deal with the data of customers, employees and others. Set to come into effect in May 2018, GDPR means every business, government and public sector entity that touches European Union residents' data will need to rethink their data management approaches in order to stay compliant and thereby avoid massive new fines and bad publicity. It also applies to organisations that host in the EU, regardless of the end user or the user's location.

Organisations of all sizes need to start planning now in order to put processes in place. This document is intended as a no-nonsense guide to GDPR, covering its background, key rules, penalties and best practice for dealing with this historic milestone in data protection. It is intended primarily for a non-specialist audience involved in IT, security and C-level roles.

GDPR: an introduction

GDPR needs to be viewed as part of the broader context of data protection regulations. Europe has had laws covering data protection for over four decades and the Data Protection Directive (1995) has helped define rules on information management. But these rules were held in poor regard, have not aged well and they are not fit for purpose in the digital age when our businesses and our processes are primarily electronic.

Previous laws were also limited in their scope, penalties were often weak and individual EU countries went their own ways in interpreting the Directive. GDPR is very different and one of the most important facts to remember is that it harmonises rules across EU member states, rather than leaving each member state to fend for themselves as was previously the case. Also, note that it comes into effect well before the UK is scheduled to exit the EU so the notion that the UK is somehow exempt is redundant. The UK's Information Commissioner's Office has also clarified that 'Brexit' will not affect adoption of the GDPR into UK law.

Another key element is that GDPR demands clear consent: this is, data held on subjects must only be used for the purpose agreed. The definition of that data is very broad and can include not just names, address, emails and telephone numbers, but also social media updates, pictures and IP addresses.

Organisations must ensure that they provide the "right to erasure": that is, the ability to delete information on individuals on demand.

Finally, and perhaps most scarily, GDPR provides much bigger penalties of up to €20m or, if higher, four per cent of annual global turnover for the most recent financial year. That means, in theory at least, fines could run to hundreds of millions or even billions of euros, and this is a very different scale of penalty than has ever been applied previously in Europe. These fines will, of course, also go hand in hand with reputational damage that might effectively outweigh even the fines themselves in value. Companies such as TalkTalk, Target, Sony and Yahoo have all had their brands tarnished by media attention on their data protection failings, and in some cases the financial impact can be significant: Yahoo's email breach, for example, was specifically the reason for a reported $350m discount in its ongoing sale to Verizon.

In order to be compliant with GDPR, organisations will need to appoint Data Protection Officers which can be either an internal or external individual responsible for compliance. They will also have to review processes and create action plans and provisions or else risk the wrath of regulators that now have the ability to impose those massive penalties.

But the good news is that by acting now and putting in place the right tools and processes, GDPR will become manageable and the actions taken to comply will lead to a competitive advantage, enhance reputations for best practices, and will act as a platform for better data insights.

In short:

- GDPR more narrowly defines how EU residents' data must be handled, including in countries outside the Union
- It demands clear consent from residents for data to be collected and clarity as to for what the purposes that data can be used
- It specifies the scope of what constitutes personal data to include social media data, photos, email addresses and even computer IP addresses
- Data must be portable via open and popular file formats
- The 'right to be forgotten' aspect, where an individual's data is permanently deleted or erased on demand, will need to be respected
- Organisations of all sizes will also need to appoint data protection officers answerable to data protection authorities
- Processes and workflows will need to be reworked to build in 'privacy by design'
- GDPR calls for data breach notification within a few days of incidents being detected
- GDPR allows for massive penalties of up €20m or, if higher, as much as four percent of global revenue

The need for data protection

Data has never been so much talked about or as valuable. Some see it as “the new oil”: a gusher of crude material that can be refined to create vast power and wealth, in this case by identifying patterns and trends that lead to opportunities or help to mitigate risks. Data in the web era is used to market to us based on our search histories, transactions, preferences and interests. Organisations can also mine data for defensive purposes, for example to spot behaviour that is indicative of fraud or other criminal behaviour.

Accumulating data and querying it has made the fortunes of web giants such as Google and Facebook but almost any organisation today will be sitting on customer data, employee data, data on prospects and other personally identifiable information (PII). And the challenge is that as data has soared in value we have seen a parallel rise in attacks and threats designed to steal data.

Organisations today will store that data not just on mobile devices, desktop computers and datacentre servers but also on third-party web-based services and the public cloud. Getting visibility into the personal data they hold and ensuring compliance with GDPR will be no trivial task, especially for larger enterprises that typically maintain multiple databases, customer relationship management systems, spreadsheets and other software running across versions, operating systems and hardware platforms.

The EU and data protection

In January 2016, it was calculated that over 510 million people live in countries governed by the European Union – more than one-and-a-half times the population of the United States.

Over the years many regulations have been passed, most notably the Data Protection Directive that is interpreted across Europe by different data protection authorities such as the UK's Information Commissioner's Office (ICO), in France by the Commission Nationale de l'Information et des Libertés (CNIL), in Germany by its federal states and so on. They vary in scope and outlook but one consistent theme is that the fines these watchdogs have dealt out have been relatively weak, usually capped in the hundreds of thousands of euros range even for cases of data breach that attracted headlines such as Talk Talk (2015) and Sony PlayStation Network (2011) cases.

As lawyers at Pinsent Masons have noted, "None of CNIL, the Hamburg Commissioner [responsible for Google in Germany] or the ICO has made full use of all the powers before it against organisations."

CNIL imposed a €100,000 fine on Google for unauthorised collection of data relating to data collected for its Street View service while the Hamburg authority gave the search giant a €145,000 penalty. As many critics have queued up to point out, these are tiny sums for a company that has tens of billions of dollars of annual revenue.

Under GDPR, EU members could in theory fine companies hundreds of millions, or even billions, of euros in penalties. Little wonder that with penalties of that magnitude GDPR has caused a wave of concern among companies.

It should also be noted that GDPR does not just apply to EU members but to any company collecting data under its jurisdiction. Large fines will also attract large amounts of damaging publicity of course, leading some to suggest that a massive penalty could cause the collapse of an organisation.

More prosaically, companies will need to prepare thoroughly in order to avoid being on the wrong end of GDPR penalties. Whereas some would in the past have effectively set aside budget for paying fines and account for it as a risk of doing business that will not be an option in the GDPR world where a fine could turn an annual profit into an annual loss.

Clear consent

GDPR addresses a grey area in the ways in which organisations can use personally identifiable information and whereas the previous Directive was in some ways an 'opt out' environment for individuals, GDPR makes it very much an 'opt in'. It makes the concept of consent very clear, specific and unambiguous, and states that organisations cannot use data without clear consent and only for named purposes.

So, for example, a healthcare provider that provides a liposuction procedure cannot pass patient data on to a gym that wants to attract that person to become a member and sees a correlation between a person wanting that liposuction procedure and seeking to get fit.

That is a huge change. Personal data today is the currency of the web. With 'free' services such as web search or cloud email or social networks we effectively 'pay' for services by giving away information. GDPR effectively kerbs that free flow of personal data information by clamping down on how data is collected, used and shared.

The right to be forgotten

The "right to be forgotten" has entered the English language as a phrase that resonates in an age where we are all subjected to having our details stored online whether we want them to be or not, and regardless of whether we have a broadband connection, computer or telephone.

Sometimes also known, perhaps more accurately, as "the right to erasure", Article 17 of GDPR allows individuals to demand personal data be erased, and for processing to stop in certain situations.

There are some exceptions where the right to erasure can be refused, mostly to do with freedom of expression, legal claims and research in the public interest, but GDPR generally mandates that data controllers must comply with the right to erasure and make best efforts to share notification of erasure processes with

The right to erasure is highlighted under GDPR in a way that it was not under the previous Data Protection Directive. This is an important, and very visible, plank in the overall legislation.

- Data is no longer being used for its original purpose
- Consent is withdrawn and there is no legitimate reason for processing to continue
- The subject is not an adult
- Data was unlawfully processed in the first place
- There is a legal obligation

Data controllers and data processors

A data controller is a person who, acting alone or as part of a team, specifies the purposes for which personal data will be used and how data will be processed.

A data processor is a third-party person, not employed by the data controller, who organises, adapts, retrieves, discloses or shares the data on behalf of the data controller

There are some exceptions where the right to erasure can be refused, mostly to do with freedom of expression, legal claims and research in the public interest, but GDPR generally mandates that data controllers must comply with the right to erasure and make best efforts to share notification of erasure processes with relevant third-parties.

The right to erasure is highlighted under GDPR in a way that it was not under the previous Data Protection Directive. This is an important, and very visible, plank in the overall legislation.

Breach notification

Another highly significant aspect of GDPR is what is known as breach notification. Under the new rules, data controllers, upon receiving information from data processors, must advise their data protection authority of a breach within 72 hours of their becoming aware of it. The authority will then advise as to what the organisation needs to disclose publicly and to customers.

Already effective in various forms across US states, breach notification often leads to public and media attention, but advocates of the system say it brings transparency and the opportunity to spot trends, for example, similar attacks on organisations.

A notification to the authority must at minimum describe the personal data breach, the scale of the issue, the data protection officer's contact details, likely consequences of the breach, and how this is being dealt with. (Some aspects might come in phases rather than all at once.)

To be optimally effective, organisations will need to update and reconfigure services so they can identify security breaches quicker and have a plan of action in place.

The scale of the challenge is daunting. Over half of companies polled believed they would be hit by successful cyber attacks within a year, according to one report. The median number of days when attackers are dormant on networks before detection is about 200, according to another report. Although breach notification dates from when the breach is detected, any signs of laxness in detecting those breaches are likely to increase penalties

Data Protection Officers

GDPR requires Data Protection Officers (DPOs) to be retained to be answerable to the authorities. This could become a booming role as in larger companies the DPO will often be a dedicated job with a supporting team attached. Among smaller companies it might fall into the remit of an individual working in another department: staff working within legal departments at organisations will be an obvious possibility but the IT department is another that is well suited to the task because some technical proficiency will be necessary to protect and oversee data.

Germany is already well advanced here because DPOs have for decades held roles in organisations, but for other countries this will be a big switch. Dedicated DPOs will be required in cases where core activities centre on data processing (list brokers or credit agencies, for example) or where data is sensitive, for example with patient medical care histories, social services cases, or where criminal records are held.

The DPO could act as third-party contracting on behalf of the data controller but s/he will need to be able to access IT systems and have a strong knowledge of data laws.

Going beyond adequacy: cross-border transfers

GDPR allows for personal data transfers to other countries that are subject to conditions that the EC sees as having "adequate" personal data protection. Even without that adequacy judgement, compliance with Binding Corporate Rules will suffice.

GDPR also clarifies that it is not lawful for personal data to be transferred out of the EU to answer a third country's legal requirement.

From hygiene factor to enabler?

Is there an upside to GDPR? Arguably, yes. GDPR will bring irresponsible and reckless use of personal data into the full glare of the public spotlight and grow our awareness of how data is used (and, sometimes, misused and abused).

But GDPR might also be a catalyst for change within organisations as the act of putting new data management structures in place and revising workflows creates efficiencies and a platform for data-driven insights. GDPR might appear a purely defensive measure but it could also act as a stimulus for broader change and could create business opportunities.

Marketing departments might benefit, for example. With explicit consent gained, CMOs could be better positioned to target customers who are more relaxed in what they are content to disclose because they know precisely how it will be used.

Nobody is suggesting that GDPR will be a quick fix but with new processes in place and more robust data platforms, organisations will be better able to mine their data and decades of experience. Some forward-looking organisations will work on GDPR alongside wider digital transformation projects across websites and apps that reinvent the company, its brand, ways of doing business, and transacting.

What to do now

Don't panic but if you haven't already begun planning your GDPR compliance, now is the time to start. GDPR takes effect in May 2018 so service level agreements being made now need to factor in these new measures.

An obvious starting point is to conduct a full data audit with a gap analysis and review of processes and workflows, under what is termed a Data Protection Impact Assessment (DPIA).

Many companies today are guilty of 'storage landfill' with redundant, outdated and irrelevant data that is kept on a 'just in case' basis and because storage is relatively cheap and /or admins can't assess what value needs to be stored and what can be deleted. Data minimisation, with routines to delete or move archived data away from core processes, will help clarify what data you hold and how it overlaps and is replicated.

Conduct a compare-and-contrast assessment of the way you handle data today, and ways that GDPR will mandate those processes change.

Security processes must be thoroughly reviewed and followed up with regular tests and assessments. But don't forget softer issues such as planning for what you need to do in the event of a breach, including your communications programme, media alerting and employee awareness messaging.

With interpretation and precedent yet to be established, organisations should adhere to the strictest interpretations of a worst-case scenario.

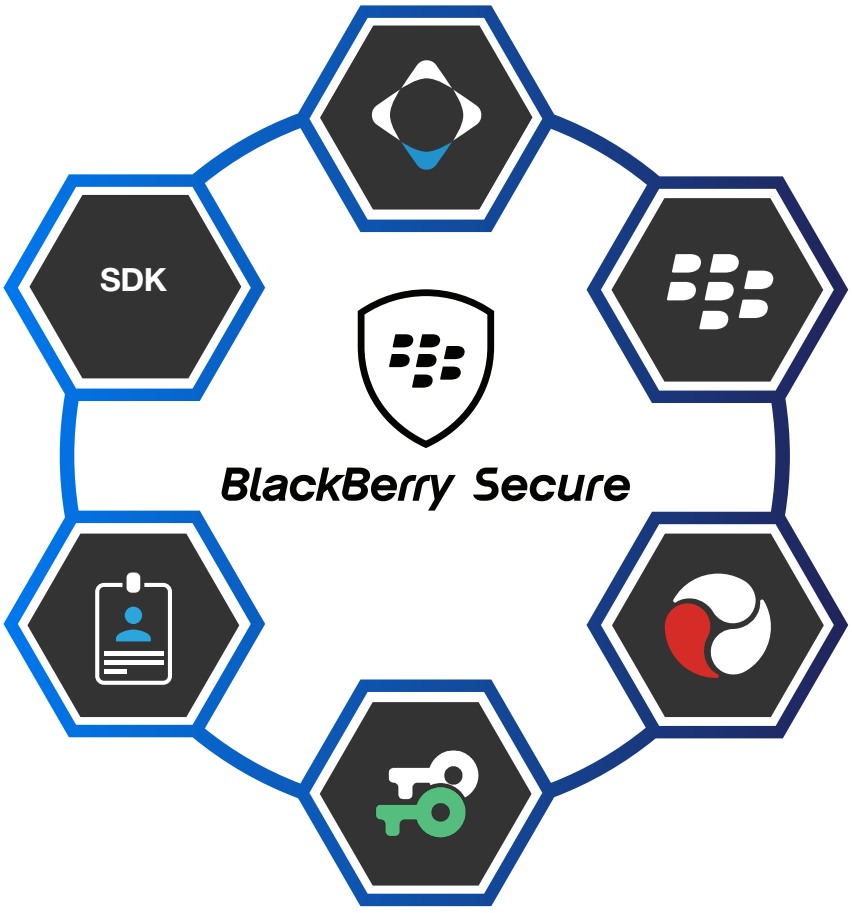
How BlackBerry can help you

As we have outlined, GDPR is a major departure for data protection in Europe but it is also manageable.
Appointing a DPO and re-engineering processes will be needed but technology will also be an aid. BlackBerry provides a comprehensive set of tools to secure data, flag threats, audit assets and assess incidents.
At a minimum, organisations need to consider:

- Visibility of all endpoints connecting to data that is potentially affected by GDPR
- A strong analytics capability to understand data use
- A secure network environment
- Encryption of data in motion, in use and at rest on an endpoint device
- An identity management system that authenticates all network users
- Comprehensive digital rights management
- The ability to secure endpoints at the device, applications and data layers across platforms and device types via a single, integrated platform
- Protection for contractors as well as permanent employees
- The support of an organisation with practical expertise in all of the above

BlackBerry has a portfolio of tools and services that can help organisations manage their way through GDPR compliance.

BlackBerry **Enterprise Mobility Suite** provides a flexible approach to services that offer security and productivity while helping maintain compliance with GDPR. As an organisation's needs evolve the Enterprise Mobility Suite provides the ability to add more capabilities as needed.



The following tools are included in the Enterprise Mobility Suite:

Unified Endpoint Management (UEM) helps to address one of the challenges of securing today's enterprises: the sheer proliferation of device types, from smartphones to desktops via laptops, tablets, e-readers and smart wearables and connected endpoints. BlackBerry UEM supports the latest container technologies – Android Enterprise, Samsung Knox, and BlackBerry Dynamics, is hugely scalable and can be configured with business continuity and disaster recovery options. The software can be deployed on premises or in the Microsoft Azure cloud in the region of choice.

BlackBerry software provides encryption within every offering, providing data protection across networks, on devices, around apps, and within files. Particularly relevant for GDPR, BlackBerry provides **encryption in transit, in use, and at rest,** roles-based controls and remote access tools so that in the event of devices being lost or stolen, data can be wiped or recovered.

BlackBerry Work builds on the company's name for secure communications with deep data protection on email and collaboration. This all-in-one productivity app provides a seamless experience to multitask between work apps while at the same time providing a secure container that prevents data loss.

BlackBerry Workspaces offers a file secure file synchronization and sharing services with digital rights management (DRM) support across any device. Workspaces allows organisations to track how files are shared – key for GDPR – and even change who can access those files after they have been sent.

BlackBerry Dynamics extends the security used in BlackBerry's own apps to protect key custom and third-party applications from being tampered with, and allows for secure sharing of data between apps and users.

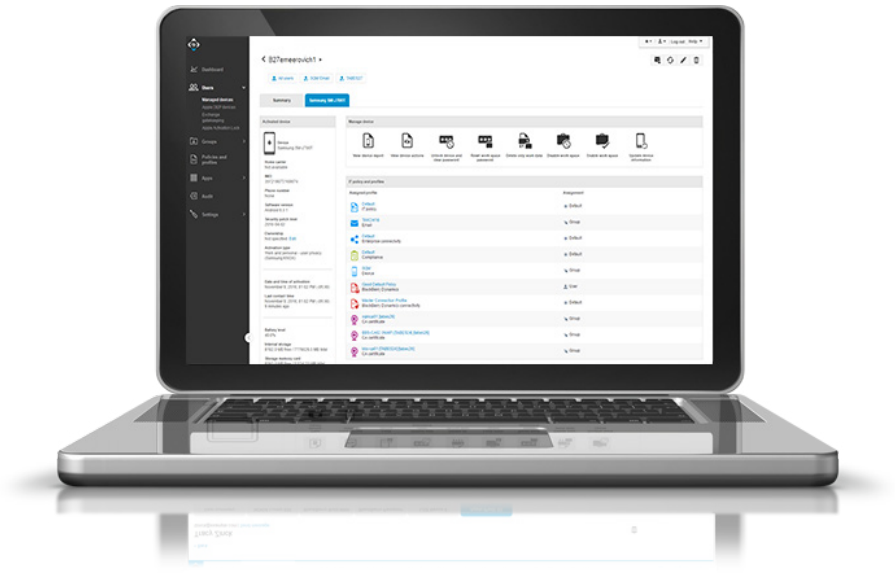
BlackBerry Enterprise Identity allows single sign-on to services from any device, providing security with quicker access to secured apps.

BlackBerry 2FA lets IT departments provide two-factor authentication for secure access, and protects access to VPN infrastructure, thereby protecting key data.

For organisations that don't have the time to set up dedicated operations, third-party consulting services provide a way to stay compliant and implement best practices without taking your eye off everyday business. BlackBerry provides a full range of cyber-security consulting services and can help you plan, deploy and manage your GDPR project.

Further reading

The Top 10 operational impacts of the GDPR is an excellent, easy-to-read guide published by the International Association of Privacy Professionals (IAPP).



Our Vision:
To be the leading point of communications between UK based business technology leaders.

Our Mission:
To provide focused peer led information, networking opportunities and knowledge sharing to help UK based business technology leaders be more effective
CIO is the leading information brand for today's busy chief information officer.
CIO addresses issues vital to the success of chief information officers worldwide. CIO provides technology and business leaders with analysis and insight on information technology trends and a keen understanding of IT's role in achieving business goals.

About the author:
Martin Veitch is Editorial Director of IDG Connect. He has written about business and technology for over 25 years and has held senior editorial positions at ZDNet, IT Week and CIO.

Content: 05/17