BlackBerry

WHAT IS GDPR AND WHY IS IT IMPORTANT?

CIO
Strategic Marketing Services

Is your organization compliant with the GDPR?

Preparedness, technology tools, smart thinking and expert counsel will help you meet the demanding challenges of this regulation.

The General Data Protection Regulation (GDPR) has drastic changes in the way organizations handle personal data, whether it be customer, employee or other sensitive data. Officially in full force as of May 2018, most business, government and public-sector entities that process European Union residents' personal data need to modify their data management approaches to comply with this new regulation – and avoid substantial fines and bad publicity. The GDPR also applies to any organization that is hosting Personally Identifiable Information (PII) in the EU, regardless of the end user's location.

Organizations of all sizes need to define and establish their new processes to be in compliance with the GDPR.

This document offers an overview of the GDPR and its effects, covering its background, key rules, penalties and recommended best practices. Its content is intended primarily for a non-specialist IT, security or C-level audience interested in how to meet the requirements of this historic milestone in data protection.

GDPR: an introduction

Europe has had laws covering data protection for over four decades. The Data Protection Directive 95/46/EC, especially, has helped define rules on information management.

But critics argue that these rules have not aged well: they simply aren't fit for the 21st century, when businesses and processes are primarily digital and data flows across borders. Previous laws were also limited in their scope and resulted in weak penalties. Further, individual EU countries interpreted and applied the DPD differently.

What makes the GDPR different from previous legislation is that it harmonizes rules across EU member states, rather than leaving each member state to fend for itself. It is worth nothing that the Information Commissioner's Office in the UK has clarified that 'Brexit' will not affect the GDPR's adoption into UK law.

Another key differentiator is that the GDPR demands clear consent: data gathered on individuals must only be used for the agreed-upon purpose. 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.

Organizations must ensure that they also support the 'right to erasure' – essentially, the ability to delete information on individuals on demand.

For those organizations that don't comply with the GDPR, the penalties could go up to €20m or four per cent of a company's annual global revenue for the most recent financial year. GDPR penalties have the potential to run much higher than anything that has ever been applied previously in Europe. These fines will, of course, go hand in hand with reputational damage that might effectively outweigh even the fines themselves in value. The financial impact has the potential to be quite significant: Yahoo's email breach, led to a reported $350m discount in its ongoing sale to Verizon.

In order to be compliant with the GDPR, organizations are required to appoint Data Protection Officers which can be either an internal or external individual or team responsible for compliance. The Data Protection Officer's responsibilities include reviewing processes and creating action plans and provisions, or else risk the imposition of substantial penalties by GDPR regulators.

Despite all the challenges that the GDPR brings, the good news is that by putting in place the right tools and processes, the GDPR is manageable. Further, organizations may discover that the actions required to comply with it can lead to a competitive advantage, enhance reputations for following best practices, and serve as a solid foundation for better data insights.

In short, the GDPR:

- Narrowly defines how EU residents' personal data must be handled, including in countries outside the EU
- Demands clear consent from residents for data to be collected and clarity as to the purposes for which the data can be used
- Specifies what constitutes personal data, including social media data, photos, email addresses and even computer IP addresses
- Specifies that data must be portable via open and popular file formats
- Includes the 'right to be forgotten' aspect, where an individual's data must be permanently deleted or erased on demand
- Requires that organizations of all sizes appoint Data Protection Officers answerable to data protection authorities
- Requires that processes and workflows be reworked to build in 'privacy by design'
- Calls for data breach notification within 72 hours of incidents being detected
- Allows for substantial non-compliance penalties of up €20m or, if higher, as much as four percent of global revenue

The need for data protection

Data has never been as valuable. Some see it as “the new oil”: a gusher of crude material that can be refined to create vast power and wealth. Today, data can identify patterns and trends that lead to opportunities or help to mitigate risks.

Data in the web era is used to market to consumers based on their search histories, transactions, preferences and interests. Organizations can also mine data for defensive purposes: for example, to spot behavior that is indicative of fraud or other criminal behavior.

Accumulating and mining data has contributed to the fortunes of web giants such as Google and Facebook, but almost any organization today is accumulating customer, employee and prospect data, along with other PII.

As data has soared in value, we have seen a parallel rise in attacks and threats designed to steal it.

Organizations today are storing data and PII not just on mobile devices, desktop computers and data center 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 small feat, 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

According to estimates from January 2016, 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, which is interpreted across Europe by various data protection authorities, including: the UK's Information Commissioner's Office (ICO); France's Commission Nationale de l'Information et des Libertés (CNIL); Germany's federal states and so on. Past regulations have varied in scope and outlook, but one consistent theme is that the fines have usually been capped in the hundreds of thousands of euros range, even for major data breaches that attracted headlines, such as the 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 organizations."

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

Under the GDPR, EU members could fine non-compliant organizations up to €20m or, if higher, four per cent of a company's annual global revenues for the most recent financial year. The penalties have the potential to run much higher than any applied previously in Europe. This is just one of the many reasons that the GDPR has caused a wave of concern among organizations. It should also be noted that the GDPR applies to any organization collecting personal data under the EU's jurisdiction.

Large fines will also attract large amounts of damaging publicity, leading some IT and risk professionals to suggest that a massive penalty could cause irreversible damage at some organizations.

Organizations need to prepare thoroughly to be compliant with the GDPR. Some organizations would, in the past, have set aside a budget for paying fines (and consider it a cost of doing business), but now that the GDPR has come into effect, fines could turn an annual profit into an annual loss.

Clear consent

The GDPR makes the concept of consent very clear, specific and unambiguous, and states that organizations cannot use data without clear consent and only for pre-defined purposes. For example, an App that caters content to future parents cannot sell customer data to a company that markets children's products and services such as a cord blood bank, a private school, a nanny agency or a clothing store, without the clear consent from the future parents.

The right to be forgotten

The 'right to be forgotten' has entered the English language as an expression 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 the GDPR allows individuals to demand that personal data be erased, or that data processing stops (in certain situations).

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

The right to erasure is highlighted under the 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. The right to erasure can be applied or requested in the following cases:

- 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.

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 becoming aware of it. The authority will then advise as to what the organization needs to disclose publicly and to customers.

Already effective in various forms across US states, the 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 other organizations.

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 the breach is being dealt with. (Some aspects might come in phases rather than all at once.)

To be optimally effective, organizations 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 sign of laxness in detecting breaches is likely to increase penalties.

Data Protection Officers

The GDPR requires that organizations retain Data Protection Officers (DPOs) who are answerable to the authorities. In larger companies, the DPO will often be a dedicated role, with a supporting team attached. In smaller organizations, it might fall under the remit of an individual working in another department: staff working within legal departments, for example, or in IT (because some technical proficiency will be necessary to protect and oversee data).

Germany is already advanced in this area because DPOs have, for decades, held roles in organizations; for other countries, this will be a novelty. Dedicated DPOs will be required in cases where core activities center on data processing (e.g., list brokers or credit agencies) or where data is sensitive (e.g. in patient medical care histories and social services cases, or where criminal records are held).

The DPO could also be a third party contracted on behalf of the data controller, but he or she will need to be able to access IT systems and have a strong knowledge of data laws.

Going beyond adequacy: cross-border transfers

The GDPR allows for personal data transfers to other countries that are subject to conditions that the EU sees as having "adequate" personal data protection. Even without that adequacy judgement, compliance with Binding Corporate Rules, implementation of the EU Model Clauses, or certification to the EU-US Privacy Shield will suffice.

The 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?

The GDPR brings irresponsible and reckless use of personal data into the public spotlight and increases our awareness of how data is used (and, sometimes, misused and abused).

The GDPR might also be a catalyst for change within organizations, as the act of putting new data management structures in place and revising workflows creates efficiencies and a solid foundation for data-driven insights.

The 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 from it, 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 the GDPR will be a quick fix, but with new processes and more robust data collection and storage structures in place, organizations will be better able to mine their data. Some forward-looking organizations will work on the GDPR alongside wider digital transformation projects across websites and apps that can help reinvent the organization, its brand and ways of doing business.

What to do now

If you haven't already begun planning how your organization will meet the requirements of the GDPR, now is the time to start. The GDPR came into effect May 2018; therefore, any service-level agreements being made now should 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 create 'storage landfills' with redundant, outdated and irrelevant data that is kept 'just-in-case' (and because storage is relatively cheap and/or admins can't determine what needs to be stored and what can be deleted). Data minimization, with routines to delete or move archived data away from core processes, will help clarify what data to hold.

After this, the next step is to conduct a compare-and-contrast assessment of the way your organization handles data today, and the ways that the GDPR will mandate those processes to 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 program, media alerting and employee awareness messaging.

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

BlackBerry: Your Partner providing a single end-to-end offering to help fulfill GDPR requirements

Achieving GDPR compliance can be complex and costly, especially if it's not done right the first time. You can't simply buy a piece of software or hire consulting services. Instead, you must undergo an organizational transformation in the way that you manage personal data. That transformation requires the right combination of consulting services and software in one single offering. BlackBerry delivers this offering as your trusted security partner.

Now that the May 2018 deadline for the GDPR has passed, there is no time for trial and error in choosing the right partner. The time to act is now, because any errors or delays could result in extremely costly fines, as well as damage to your organization's reputation and brand.

Here are just a few of the broad benefits of the BlackBerry end-to-end offering for GDPR compliance:

A single partner for consulting services and software
With BlackBerry, you can eliminate the complexity and risk of working with multiple partners and service providers to fulfill the requirements of the GDPR.

Aligned with your IT processes & context, as well as your business objectives
With the BlackBerry end-to-end approach, your organization can secure its data without compromising productivity.

Business value beyond GDPR compliance
We can show your organization how to use GDPR compliance to regain control of your data and convert the value from stored information into analytical and/or marketing insights and revenues.

Founded on deep security expertise
BlackBerry is trusted by some of the world's most security-conscious organizations, as well as by state and federal governments, to protect critical data and operations.

Services: BlackBerry Cybersecurity Consulting

BlackBerry Cybersecurity Consulting provides a strategic, practical and actionable approach to GDPR compliance. We assess where your organization stands regarding the GDPR, and take a risk-based approach to secure information agnostically across any mobile device or computer – and beyond the borders of your networks. We offer the capacity to monitor and control PII wherever it resides.

Our end-to-end offering covers:

- Gap analysis
- Remediation of your policies and processes
- Remediation of your software
- Breach drills
- GDPR training and awareness courses

BlackBerry Cybersecurity Consulting also provides Data Protection Officer (DPO) services. The International Association for Privacy Professionals (IAPP) estimates over 27,000 DPOs will be needed to address this single requirement of the GDPR, creating fierce competition for these experts. BlackBerry offers your organization the assurance of our proven leadership and expertise in data protection should you lack the capacity, expertise, or business focus for an internal DPO.

BlackBerry Cybersecurity Consulting guides your organization through the process of understanding the PII in use by your company, its value and the associated risks. We then help you define where, when and how to apply controls proportionally – when needed.

Tools: BlackBerry Enterprise Mobility Suite

The BlackBerry Enterprise Mobility Suite delivers security and productivity while helping to support compliance with the GDPR. With on-premises and cloud-based software to secure data, flag threats, audit assets and assess incidents, it offers the ability to add more capabilities as your organization's needs evolve.

BlackBerry software provides encryption within every offering, delivering data protection across networks, on devices, around apps and within files. Particularly relevant for GDPR, BlackBerry provides encryption in transit 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.

The following tools in the BlackBerry Enterprise Mobility Suite support GDPR compliance:

1. BlackBerry Unified Endpoint Management (UEM) enables visibility of all endpoints connecting to data potentially affected by the GDPR

2. BlackBerry Work allows secure collaboration involving PII

3. BlackBerry Workspaces provides comprehensive file-level Digital Rights Management

4. BlackBerry 2FA & BlackBerry Enterprise Identity provide an identity management system to authenticate all network users

BlackBerry provides end-to-end offerings to help you address all your GDPR challenges – with software and services for every device, a secure network, and the expertise to prepare your people and IT infrastructure. We take your organization through the practical, step-by-step process of understanding how the GDPR applies to your organization, and how to achieve a competitive compliance posture without compromising productivity.

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).

BlackBerry