DATA PROTECTION BY DESIGN

Preparing for Europe's New Security Regulations

Summary

In 2018, the European Union will begin to enforce the provisions of the General Data Protection Regulation (GDPR), a new law that will fundamentally alter the way businesses and other organizations collect, store, and use personal information. GDPR requirements will apply to any company that does business in the European Union, whether or not the company is based in an EU member country.

In keeping with the law's central concepts of "data protection by design" and "data protection by default," organizations will be required to build stronger data security into their products and services, and to follow strict guidelines as to how personal data may be used. Penalties for failing to comply will be severe, with fines of up to 4% of a company's annual turnover (gross revenue) for violations.

Given the law's broad scope and the heavy penalties for non-compliance, organizations that operate in the EU should evaluate their current policies and data protection measures as soon as possible, and should take steps that will ensure their compliance in 2018 and beyond.

"In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures, which meet in particular the principles of data protection by design and data protection by default."

(Preamble to the General Data Protection Regulation, paragraph 61)

A New Era in Data Protection

The European Parliament formally adopted the General Data Protection Regulation in April 2016, after a lengthy period of negotiation and revision. The regulation will become an enforceable law in all EU countries in May 2018. Organizations that collect, store, and use personal information have until that time to bring their systems and business processes into compliance.

When the new law goes into effect, it will mark the beginning of a new era in data protection. The GDPR creates new rights for individuals, imposes new obligations on businesses and governments, and provides for severe financial penalties in the event of non-compliance.

"EU will now have a single data security law"

Long-awaited updates

The GDPR replaces the Data Protection Directive (DPD), an outdated agreement that gave rise to a confusing patchwork of inconsistent and conflicting rules across the EU. While many of the new law's provisions are similar to those of the DPD, the GDPR includes additional requirements that address concerns related to mobile technology, social media, international data transfers, and other topics.

The new law also differs from the Data Protection Directive in its territorial scope. While the DPD applied stricter standards to companies based in the EU than to companies based elsewhere, the GDPR applies equally to any company that operates in the EU. As a regulation rather than a directive, the GDPR has the force of law immediately, without the need for separate legislation in member countries. This means that the entire EU will now have a single data security law.

Key Provisions of the General Data Protection Regulation

Most of the GDPR's new requirements are directed at data controllers-- businesses that determine how and when personal data is collected, stored, used, or transmitted. The law also provides specific rules for data processors, which are businesses that collect or manage data on behalf of a data controller.

- **Mandate to obtain consent:** Organizations must get clear, unambiguous consent before collecting or processing an individual's personal data.
- **Right to be forgotten:** Data controllers will be required to delete an individual's personal data upon request, unless there is a legitimate need for the organization to retain the data.
- **Notification of data breaches:** Data controllers must notify government authorities (and in some cases affected individuals) within 72 hours if personal data is stolen or compromised. However, this notice is not required if the stolen data is protected by persistent data encryption.
- **Data protection officers:** Companies or government agencies that process sensitive personal information will be required to appoint data protection officers, who will be responsible for monitoring compliance with the law.
- **Severe penalties for violations:** Companies can be fined up to 4% of their annual turnover (gross revenue) for failures to comply with basic data processing or transfer requirements.

Although the GDPR will apply to many government entities as well as businesses, its provisions will not apply to law enforcement agencies. A new Data Protection Directive has been drafted to improve the security of data used by police and other criminal justice organizations.

Is the GDPR an Improvement?

Taken as a whole, the GPDR appears to be a step in the right direction. The law calls for higher standards of data protection and increased rights for individuals, both of which are clearly needed in the wake of recent corporate and government data breaches.

The GDPR's penalties for non-compliance, which could easily run into the millions for large corporations, should provide enough motivation for businesses to implement the required protection. History has shown that privacy laws which lack significant financial penalties (HIPAA in the United States, for example) rarely produce their intended result. Data controllers and processors, while they are subject to several new requirements, should benefit from the simplification of data protection laws across the EU. Companies based in the EU will also benefit from a level playing field, now that overseas businesses must comply with the same set of rules.

Several aspects of the law, however, will likely create difficulties for businesses and government regulators. Compliance with the "right to be forgotten" provisions, in particular, will be very challenging for large organizations that store personal data in multiple systems. Many companies may also face difficulties in identifying qualified data control officers.

Certain details related to implementing and enforcing the provisions of the GDPR are yet to be determined, and it is possible that some elements of the law may change in coming years. The underlying principles will remain the same, however, and businesses and other organizations must be prepared to meet expectations of strong data protection and increased control by individuals.

The Role of Encryption

The GDPR's mandate for "data protection by design" will lead many organizations to rethink their strategies for collecting, storing, and transmitting data. One likely outcome will be a dramatic increase in the use of strong security measures like persistent data encryption.

The growing prevalence of security breaches has brought encryption to the forefront of data protection discussions. In fact, the text of the GDPR was revised several times between 2012 and 2016 to include additional mentions of encryption, along with specific recommendations that organizations use encryption to protect personal information.

Eliminating the Impact of a Data Breach

Most notably, the GDPR provides an exemption for data breach notifications when organizations use persistent encryption to protect their data.

In general, data controllers are required to notify governmental data protection authorities of a data breach within 72 hours. In some cases, controllers must also notify the individuals whose personal information was stolen.

However, the law exempts organizations from these requirements if they have used data protection methods such as encryption to ensure that any stolen data remains unusable to unauthorized individuals. Since encrypted data remains safe even when stolen or misdirected, data controllers can avoid notification requirements and financial penalties under the GDPR , as well as other, potentially catastrophic, consequences of a data breach.

It is important to note that transparent data encryption may not be enough to exempt a data controller from the GDPR requirements. Transparent encryption does not remain in place once data has been read from a database, so it does not meet the criteria as a form of protection which can "render the data unintelligible to any person who is not authorised to access it," as described in the text of the GDPR.

> *In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks, such as encryption. (Preamble, paragraph 66)*

> *The communication to the data subject referred to in paragraph 1 shall not be required if: (a) the controller has implemented appropriate technical and organisational protection measures, and that those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption. (Chapter IV, Section 2, Article 32)*

Implications for the UK

When the GDPR takes effect in 2018, it will replace the current data security laws in every EU member country, including the Data Protection Act 1998 (DPA) in the UK. Companies that do business in the UK, even if they are in compliance with the DPA today, will need to update their data protection practices in order to avoid penalties under the GDPR.

Among the many differences between the DPA 1998 and the GDPR, four key areas will likely create the greatest need for change among data controllers in the UK:

- **Consent Requirements:** The GDPR's requirements for obtaining consent are much more strict than DPA 1998 requirements. Today, organizations can rely on passive consent in many cases, meaning that they have permission to process personal data as long as an individual fails to take a specific action (checking an opt-out box, for example).

  Beginning in 2018, organizations will be required to get consent "by a statement or by a clear affirmative action," before collecting or processing someone's personal data. The new law also raises the minimum age for consent to 16; however, the UK has stated that it will maintain its current threshold age of 13, as permitted by a special provision in the GDPR.

- **Data Access Rights:** Under the DPA 1998, individuals have the right to request a copy of their personal data from a data controller, but the data controller can charge a £10 fee for the request and has 40 days in which to provide the data.

  When the GDPR takes effect, organizations will no longer be allowed to charge individuals who request copies of their data. Furthermore, under the GDPR data controllers must provide data within one month, and they must provide it in a portable format which can be given by the individual to another data controller (for example, when someone switches account between service providers).

- **Data Breaches:** Under the DPA 1998, the maximum fine allowable for a data breach or other violation is £500,000. The GDPR's penalties of up to 4% of annual turnover will represent a significantly higher risk for many large corporations.

  Just as importantly, the GDPR does away with the condition that a data breach must cause measurable harm to a data subject before a data processor can be penalized. Beginning in 2018, individuals will no longer need to demonstrate that they have suffered a financial loss or other adverse effect as a result of a data breach.

- **Definition of Personal Data:** The GDPR will expand the definition of personal data to include more types of information than are covered by the DPA 1998. This will create a larger burden for data controllers and processors, who will need to develop strategies for protecting a larger percentage of the data they collect. The new law also adds new categories of "sensitive" personal data, such as genetic and biometric data, which will require special processing and protection.

It is important to note that the UK's planned exit from the EU is not expected to exempt UK businesses from the GDPA, as the UK will still be a member of the EU when the GDPR takes effect. Furthermore, officials have stated that the UK's post-Brexit data privacy laws will remain consistent with the GDPR, rather than reverting back to DPA 1998 provisions.

Possible Complications

Like any law that brings about a significant change in the ways that businesses and governments operate, the GDPR raises several significant questions:

- How will the GDPR's rules regarding international data transfers be affected by a new US-EU agreement for data sharing, if another agreement is reached?
- Can companies simultaneously comply with the GDPR while sharing information with the NSA or other US agencies under the Cybersecurity Information Sharing Act (CISA)?
- Will data controllers need to obtain new consent from individuals whose data is already in use, or will previously-obtained consent still be considered valid?
- Under what circumstances can a data controller retain an individual's data despite the individual's request that the data be deleted?

Given the high level of public interest in the GDPR, the EU pushed forward with the approval process without addressing every possible area of concern in the text of the law. The answers to these and other questions, most likely, will be answered in court over the next several years.

Recommendations

Although the GDPR will not go into effect until 2018, organizations that do business in the EU should begin to prepare for the new law as soon as possible. The steps listed below should provide a starting point for companies and other organizations who need to comply with the new law.

- Evaluate current systems and business processes to identify potential compliance gaps. Specifically, organizations should determine what types of personal information they are collecting, storing, and processing today, and whether the information will require stronger protection under the GDPR. In addition, data controllers should look at the forms of consent they are currently obtaining from data subjects and whether additional consent will be necessary in order to collect similar information in the future.
- Determine the organization's financial exposure in the event of a data breach or other violation. Understanding the impact of a potential GDPR penalty will assist with cost/benefit analysis related to new business processes and security protocols.
- Look for opportunities to build data security measures into new products and services, in order to demonstrate compliance with the mandate for data protection by design. Organizations will likely be required to provide detailed documentation of the steps they have taken to ensure compliance.
- Begin discussions with vendors and other partner organizations, especially those that provide data processing or storage services, to confirm that they are aware of the new requirements and will be in compliance beginning in 2018.

As the law's effective date draws nearer, organizations should stay informed about possible changes or clarifications in the law, and should stay up to date on the guidance released by the EU's data protection authorities.

About

PKWARE is a trusted leader in global business data protection. For three decades PKWARE has focused on data. Building on our compression expertise with the latest encryption technology, PKWARE protects data for over 35,000 customers, including government agencies and global corporations. Our software-defined solutions provide cost-effective and easy-to-implement protection that is transparent to end users and simple for IT to administer and control.

PKWARE®
www.pkware.com

CORPORATE HEADQUARTERS
201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204

+ 1 866 583 1795

EMEA HEADQUARTERS
79 College Road
Suite 221
Harrow HA1 1BD

+ 44 (0) 203 367 2249

PKWARE is a trusted leader in global business data protection. For three decades PKWARE has focused on data. Building on our compression expertise with the latest encryption technology, PKWARE protects data for over 35,000 customers, including government agencies and global corporations. Our software-defined solutions provide cost-effective and easy-to-implement protection that is transparent to end users and simple for IT to administer and control.