USING SMARTCRYPT TDE FOR GDPR COMPLIANCE

Smartcrypt Transparent Data Encryption helps companies meet the demands of Europe's General Data Protection Regulation.

About The Law

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)

Uncertain Times For Companies Doing Business In The UK

By 2018, the General Data Protection Regulation (GDPR) will require any company that does business in the European Union to more securely collect, store, and use personal information. The task will be all the more challenging with the October 2015 nullification of a "Safe Harbor" agreement between the European Union and United States.

"Severe penalties for violations"

The Safe Harbor rule allowed firms to transfer massive amounts of data to their servers in the U.S. and streamlined the complicated process companies had to go through in order to comply with European regulations. Thousands of global companies used it, including Google, Amazon, Twitter and Facebook.

The European Court of Justice jettisoned Safe Harbor in October 2015 out of concern that U.S. authorities would use the personal data stores for mass indiscriminate surveillance. The decision was in response to revelations made by former National Security Agency contractor, Edward Snowden. Its elimination will have to be considered carefully as companies work to meet GDPR compliance.

GDPR's Tough Requirements

GDPR requires that organizations build stronger data security into their products and services and follow strict guidelines on how personal data may be used.

The law provides specific rules for data processors -- businesses that collect or manage data on behalf of a data controller:

Mandate to obtain consent: Organisations 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 organisation 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.

Best Practices

Although GDPR does not take effect until 2018, organizations should start preparing as soon as possible. The following steps provide a starting point:

1. 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.

2. 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.

3. Build stronger data security into products and services to better control how personal data may be used. Organizations will likely be required to provide detailed documentation of the steps they have taken to ensure compliance.

4. Begin discussions with vendors and other partner organizations, especially those that provide data processing or storage services, to confirm the scope and impact of the new requirements and create a plan for compliance beginning in 2018.

As the law's effective date draws nearer, organizations need to stay informed about changes in the law and clarifications and guidance released by the EU's data protection authorities. This is especially important as it's still unclear what effect the UK's decision to leave the EU (Brexit) will have on existing laws.

DPA To GDPR: 4 Key Differences

GDPR will replace current data security laws throughout the European Union, most notably the UK's Data Protection Act of 1998 (DPA). Companies that are DPA-compliant today won't necessarily be GDPR-compliant in 2018.

A side-by-side comparison of the two laws reveal four key differences:

1. **Consent Requirements:** Under DPA, organizations can rely on passive consent, meaning they have permission to process personal data as long as someone fails to check an opt-out box. GDPR requires that companies receive consent "by a statement or by a clear affirmative action," before collecting or processing personal data.

2. **Data Access Rights:** DPA allows individuals to request a copy of their personal data from a data controller, but the data controller is allowed to charge a £10 fee and has 40 days to meet the request. Under GDPR, data controllers can't charge a fee and must fulfill requests within a month. Furthermore, they will be required to provide data in a portable format that can be transferred to another data controller when, for example, an individual switches accounts between service providers.

3. **Data Breaches:** Under the DPA, fines for data breaches and other violations go as high as £500,000. GDPR makes the allowed penalty much higher -- up to 4% of a company's gross revenue. Furthermore, GDPR won't require that a data breach cause measurable harm before a data processor can be fined. Individuals will no longer need to demonstrate that their personal finances or reputation suffered as a result of a data breach in order for an organization to be penalized.

4. **Definition of Personal Data:** The GDPR definition of personal data is far broader than that of DPA. Data controllers and processors will be under greater pressure to protect a larger percentage of the data they collect. New categories of "sensitive" personal information under GDPR will include genetic and biometric data, which will require special processing, protection and IP addresses.

Source: Information Law Group, UK Society for Computers, Privacy Law Blog

Smartcrypt TDE Solution

Based on GDPR's requirements, Smartcrypt Transparent Data Encryption (TDE) protects sensitive information at rest on enterprise servers and ensure compliance with a wide range of regulatory requirements and customer privacy mandates. It eliminates the effects of theft or accidental sharing of customer information, employee records and intellectual property.

One challenge companies have with compliance is that upgrading systems can lead to configuration issues and end user confusion. Smartcrypt TDE is designed to minimize those problems.

Smartcrypt TDE is installed on application, file and database servers containing sensitive information. Data is encrypted at the block level by a file system driver, between the operating system and the file system. Agents perform automatic encrypt/decrypt operations as data is read/written across the network.

As GDPR develops in the wake of the Safe Harbor collapse and the still-unknown implications of the Brexit vote, the most responsible approach for organizations to take is to deploy an encryption solution that ensures compliance with the least amount of disruption.

Smartcrypt TDE is the answer.

GDPR Questions To Consider

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

About PKWARE

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.

SRC Secure Solutions

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.