PKWARE | SMARTCRYPT

MEET GDPR REQUIREMENTS WITH SMARTCRYPT

WHAT IS GDPR?

The General Data Protection Regulation (GDPR) is the European Union's unified data privacy and security law. The law introduces new rights for EU citizens, along with new obligations for companies that collect, use, or process the personal information of EU citizens. The GDPR replaces the EU's outdated Data Protection Directive and is intended to address new privacy and security concerns while standardizing cybersecurity rules across Europe.

The GDPR is being enforced by supervisory authorities in each EU member country, who have the power to impose heavy sanctions on businesses that fail to comply. Organizations that do business in more than one EU country are accountable to the supervisory authority in the country in which their primary operations take place.

HOW DOES GDPR AFFECT MY ORGANIZATION?

Unlike previous European data protection laws, the GDPR applies to any company that collects or processes the personal information of EU citizens, even if the company is headquartered outside the EU. It applies in the UK despite the Brexit referendum, because the UK is still be a member of the EU. British authorities have also stated that the country's post-Brexit regulations will remain aligned with the GDPR.

The GDPR includes a variety of new mandates for data controllers (companies that collect personal information on EU citizens) and data processors (companies that store, transmit, or process data on behalf of data controllers):

- Companies must obtain active consent before collecting or processing personal data
- Individuals can request that their personal information be deleted from a company's records, and can request copies of their data in a portable format
- Companies must notify authorities and affected individuals within 72 hours of a data breach, unless the compromised data is protected by encryption or similar measures
- Each company must appoint a Data Protection Officer to oversee GDPR compliance
- Companies must build data protection into their products and services "by design and by default"

Penalties for non-compliance may be severe. Supervisory authorities have the power to fine organizations as much as 4% of their annual top-line revenue for infractions, and may impose heavier auditing and reporting obligations after a violation.

HOW DOES SMARTCRYPT HELP MEET GDPR REQUIREMENTS?

PKWARE's Smartcrypt combines data discovery, classification, and protection to enable enterprise-wide control over sensitive data. Smartcrypt helps organizations meet their GDPR obligations while keeping data protected from internal and external cyber threats.

GDPR REQUIREMENT	SMARTCRYPT SOLUTION
SECURITY OF DATA PROCESSING (ARTICLE 32): Organizations must be able to demonstrate they have taken "appropriate technical and organisational measures to ensure a level of security appropriate to the risk," including encryption of personal data.	Smartcrypt applies strong encryption that remains with data even when it is shared or stored outside the organization's network. This ensures that data remains inaccessible to unauthorized users, even if stolen or mishandled.
DATA BREACH NOTIFICATIONS (ARTICLE 34): Organizations must notify supervisory authorities and affected individuals within 72 hours of a data breach. However, organizations are exempt from the requirement to notify individuals if the stolen data is protected with encryption.	Whether a breach occurs due to a misplaced device, network intrusion, or other cause, if the organization is using Smartcrypt, it can avoid the necessity of informing individuals that their data has been compromised, as well as the PR damage and lawsuits that typically follow a data breach.
RIGHT TO BE FORGOTTEN (ARTICLE 17): Individuals can demand that data controllers delete all records containing their personal information.	After receiving a deletion request, administrators can use Smartcrypt to detect and delete an individual's data on servers and user devices across the entire organization.
DATA PROTECTION BY DESIGN AND BY DEFAULT (ARTICLE 25): Organizations must "adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default." These principles should be considered when "developing, designing, selecting and using applications, services and products"	Smartcrypt's integrated workflow allows organizations to find, classify, and protect sensitive data as soon as it is created or stored on company assets. Additionally, Smartcrypt Application Encryption lets organizations incorporate strong encryption into applications with only a few additional lines of code, in keeping with the concept of data protection by design.

PKWARE®

www.PKWARE.com

PKWARE provides a data-centric audit and protection platform that automates policy-driven discovery, classification, and encryption wherever sensitive data is used, shared, or stored.

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