The European Union’s General Data Protection Regulation (GDPR) is unlike any previous cybersecurity law, requiring extensive changes in the way businesses and other organizations collect, store, and use personal information. 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 revenue for violations.

Data encryption, the strongest form of data protection, has become even more important in the era of the GDPR. Encryption renders sensitive information unreadable by unauthorized users or applications, providing reliable protection against internal and external cyber threats. Its use is specifically recommended in several sections of the GDPR as a safeguard for personal data.

PKWARE’s Smartcrypt provides transparent data encryption (TDE) capabilities that can secure sensitive data without the need for additional infrastructure and without disrupting existing workflows. Smartcrypt TDE is an easy-to-implement solution that lays a strong foundation for GDPR compliance and helps organizations build a foundation of trust with consumers in Europe and beyond.
A New Era in Data Protection

The General Data Protection Regulation (GDPR) takes effect in May 2018, introducing new protections for individuals and new obligations for companies that collect, use, or process EU citizens’ personal information.

Given the heavy fines that can result from violations, GDPR compliance should be a top priority for every organization that does business in Europe.

The law includes significant 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, with stricter consent requirements for highly sensitive information such as health care data.

• Individuals can request that their personal information be deleted from a company’s database, 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.”

Supervisory authorities in each EU member country will be responsible for enforcing the GDPR. Organizations that do business in more than one EU country will report primarily to a “lead” supervisory authority in one country.

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

GLOBAL IMPLICATIONS

The GDPR replaces Europe’s patchwork of outdated, often contradictory data protection laws and establishes a consistent set of requirements for the EU as a whole.

Unlike previous European data protection laws, the GDPR applies equally to any company that collects or processes the personal information of EU citizens, even if the company is headquartered outside the EU.

This means that organizations based in the Americas, Asia, and elsewhere must be prepared to comply with GDPR requirements if they intend to continue to do business in Europe.

GDPR IN THE UK

The UK’s planned exit from the EU is not expected to exempt UK businesses from the GDPR, 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.
Smartcrypt TDE: Secure and Easy to Manage

Smartcrypt Transparent Data Encryption (TDE) protects sensitive information at rest on enterprise servers, ensuring compliance with a wide range of regulatory requirements and customer privacy mandates.

Smartcrypt TDE secures files and structured data without application changes, additional infrastructure, or professional services. No endpoint software is required, and the user experience is unaffected.

Effective Protection, Easy Implementation

Smartcrypt TDE is a software-defined solution that can be installed quickly and easily on enterprise servers in as little as one hour. Smartcrypt’s streamlined implementation makes it a popular choice for organizations who need to meet compliance objectives on short timelines.

Once a location is protected by Smartcrypt TDE, only users and applications that have been granted access are able to decrypt the data in that location. Sensitive data at rest is secured against a wide range of internal and external threats, while remaining available for authorized use.

Centralized Control

Administrators use the Smartcrypt Enterprise Manager, a web-based control panel, to define policies that determine which applications and users are able to decrypt and access protected information.

The Smartcrypt Enterprise Manager provides a user-friendly interface for the tasks needed to manage transparent data encryption across the organization:

- Deploying TDE agents on servers
- Identifying volumes or paths to be protected by TDE
- Generating, rotating, and deleting encryption keys
- Granting and revoking access for users, applications, and processes
- Reporting on encryption and decryption activity in protected locations

Smartpoints are designated locations on a file system that contain sensitive application data and files.

Policy driven TDE agents manage encryption keys and rotation schedules for each Smartpoint.

Policies support whitelists and blacklists, which allow only authorized users and applications to access and decrypt/encrypt data.

TDE file system drivers manage access to specified directories and perform encryption and decryption during read and write operations.
Meeting GDPR Requirements with TDE

Smartcrypt TDE is an easy and effective way for organizations to demonstrate compliance with GDPR requirements while maintaining existing workflows and business processes. Smartcrypt TDE also lays a strong foundation for other data protection initiatives that may become necessary as EU authorities issue more guidance regarding GDPR compliance.

GDPR mandates that TDE can address

**Security of data processing**

According to Article 32 of the GDPR, organizations must be able to demonstrate that they have taken “appropriate technical and organisational measures to ensure a level of security appropriate to the risk,” including encryption of personal data.

Encrypting data at rest is a widely-accepted method of securing sensitive information and is highly effective at preventing access by unauthorized employees or applications. By implementing Smartcrypt TDE and creating Smartpoints in locations where personal information is stored, organizations can demonstrate to EU authorities that they have taken appropriate action as called for by the GDPR.

**Data protection by design and by default**

Article 25 of the GDPR states that organizations must “adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.”

Smartcrypt’s policy-based approach to data protection enables organizations to implement consistent data protection practices across the entire enterprise, keeping data safe while gaining the ability to audit and report on policy changes and other encryption activity.

ABOUT PKWARE

PKWARE is a trusted leader in enterprise data protection.

For more than thirty years, PKWARE has provided solutions for corporations and government entities around the world.

We provide more data protection solutions on more operating systems than any other company, and continue to develop new technologies to help organizations meet new challenges and achieve new goals.

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.