SecurityFirst™
Protecting Critical Data

Avoiding Costly GDPR Reporting

New Standard of Care for Personal Data

The European Union's General Data Protection Regulation (GDPR) is now in force helping to protect EU data subjects against the collection and use of their personal data without explicit consent. But for organizations outside EU borders, how can you be sure GDPR applies?

The question of global applicability for GDPR enforcement is covered by multiple articles and the words "citizen" and "privacy" never occur once in the Regulation. The potential global applicability of the GDPR is not always clear and is tied the location of the Data Controller and Processor rather than the subject.

GDPR is the most far-reaching regulation that specifically focuses on personal data privacy for individuals and has the steepest fines for non-compliance. Previous regulations and mandates have been industry specific (e.g. PCI-DSS and HIPAA), dedicated to data protection at the enterprise. The distinction is critical; previous regulations were imposed to ensure enterprises, businesses and agencies put adequate controls in place. GDPR acknowledges that adequate controls are no longer good enough, and mandates that effective data stewardship, control and security must be provided and accessible by data subjects. It further refines and focuses data security to mitigate and where possible reduce the negative impact of personal data exposures.

EU Data Subjects Can Live Anywhere

Data subjects now have the right to request Controllers and Processors delete their data, amend their data, provide a record of all the data held about them, and even require a copy of their data in a machine-readable format so they can move to another provider, even a competitor.

Any Controller or Processor organization with a presence in the EU must comply, despite where the actual processing may take place. Therefore, even companies housed outside of the EU, if they process an EU data subject's personal data, must comply with the regulation.

The GDPR Difference

Unlike many checkbox-driven compliance programs, GDPR is a risk-based framework. Because it covers personal data, it's focused on having the right governance structure, policies and operational practices, as well as monitoring, detection and response capabilities. For these reasons, there are important implications for every organization with even a modest EU presence.

Significant Components of GDPR:

- Requirements for privacy by design and default, data portability and the right to erasure
- 72 hours to report a breach to the regulator after discovery
- Fines as high as 4% of global annual revenue, or €20 million, whichever is greater
- Appointment of a Data Protection Officer for most public authorities

Why is this so Critical?

In the event your organization loses personal data associated with EU data subjects, you must report this loss to a relevant supervisory authority, and a ransomware attack qualifies as a personal data loss under the GDPR definition including: the accidental or unlawful destruction, loss or alteration of personal data. The act of reporting will consume precious IT security staff time, and if done poorly, might induce several follow-on remediation activities to avoid being stigmatized as an EU non-compliant supplier of goods or services. Such a black mark might exclude your organization from participating in future contracts and bids.

The exception to this rule concerns when the lost data was in a protected state and therefore useless to cybercriminals. Protected data losses are exempted from supervisory authority reporting because there's no personally identifiable data exposure. What the hackers stole or encrypted was unreadable.

Security by Design and Default

As a CISO or the person in-charge of an organization's IT security, you should be aiming for GDPR-like compliance with all transactions

involving current and future customers, formally declared as EU data subjects or not, because trying to identify your organization's relevant exposure will eventually become an intolerable burden.

And the nature of what data needs protection is multiplying with every effort made or app written to better serve a customer's interests. We all understand the core data like birthdates, addresses, payment methods, social medicine numbers, etc., but consider the growing data points regarding URL visits, shopping habits, smartphone pictures, social media relationships and more. Better to provide the pound of protection now and avoid future loss notifications and identity protection service offerings.

DataKeep – The Solution

The security offered by DataKeep can address the data-centric Articles of GDPR including:

- Article 17 - Right to erasure (Right to be 'forgotten')
- Article 19 - Notification obligation regarding erasure of personal data
- Article 25 - Data protection by design and by default
- Article 32 - Security of processing
- Article 33 - Notification of a personal data breach to the supervisory authority
- Article 34 - Communication of a personal data breach to the data subject

File level encryption offers a ready means of destroying any personal data. When no longer required, administrators can revoke the encryption key from the system, leaving the data encrypted wherever it is stored, absent a decryption key, and log when a key was deleted for audit purposes.

DataKeep will encrypt any data-at-rest and protect it from the moment of creation or collection through and while stored on a server asset. Confidentiality, data privacy and protection against brute force attacks is assured by SPxCore™ technology supporting AES-256 encryption and internal key management certified by the National Institute of Standards and Technology (NIST) to be FIPS 140-2 compliant. The solution easily drops into existing security infrastructures, whether as a separate single-pane-of-glass or integrated into automation via RESTful API.

DataKeep supports on-premises or cloud-based object storage with client-side encryption key and access control. The Object Store Agent leverages cryptographic splitting to send shares of encrypted data to multiple object store locations or multiple Cloud Service Providers for added resiliency. A native backup and restore capability copies encrypted data to an off-site storage environment providing rapid recovery from ransomware attacks thus avoiding reporting requirements.

In most cases, any notifications of a personal data breach to an EU supervisor or data subject are unlikely given advanced access permissions that protect the data in the event of a breach, and real-time logging—with forwarding to a SIEM analytic engine—for awareness of potential infiltration risk and alerts. DataKeep meets the requirement to provide appropriate technical and organizational protection measures for personal data affected by a breach, rendering it unintelligible to any person not authorized to access it.

SecurityFirst™ delivers data-centric solutions that address the high-profile cyber threats facing organizations today, such as data breaches, ransomware and cloud security. We emphasize protection of the data itself to serve as your last line of defense. Data is always protected no matter where it resides and recoverable in the event of an unexpected failure or malicious attack. As organizations and governments mandate stricter requirements for data privacy, SecurityFirst helps protect data from compromise and exposure.

DataKeep™, by SecurityFirst, secures critical data at its core to deliver unrivaled protection, control and resiliency. Customer-defined access policies, strong encryption and event logging combine with native secure backup/restore capabilities to address your data privacy, compliance and recovery needs. Organizations can utilize the backup and restore capabilities with object storage for secure cloud backup and archiving to improve resiliency and enable prompt recovery of archived data in the event of a ransomware attack. Leading OEMs and integrators have selected DataKeep to safeguard enterprise and multi-cloud environments.

SecurityFirst™
Protecting Critical Data

For a product demonstration
or more information call
1-888-884-7152
securityfirstcorp.com