SecurityFirst™
Data-Centric Cyber Solutions

Avoiding Costly GDPR Reporting

Third Certainty of Life

Any adult can name the first two. “Death and taxes” apply to all of us, but for anyone involved in IT security, a third is upon us and getting stronger—reporting. The ability of cybercriminals to breach our traditional perimeter defenses and steal our precious data has motivated governments and industries to define a new code of conduct. Henceforth, all organizations using networked computer technology must comply.

Likely to be recognized as a global watershed event, the European Union (EU) has presented the new General Data Protection Regulation (GDPR), which will become fully enforceable in May, 2018 for both EU member countries and all the rest of us who’ve ever done business with an EU resident. Proper IT policies, procedures and technologies must then be operational or compliance failures could doom your organization. The loss of any significant ‘private’ data will ensure the payment of fines, but the reputational damage of having incurred them and the potential to be listed as non-compliant could easily dwarf these one-time expenses.

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 information security practice. Few and far between will be the unaffected.

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
- 28,000 new Data Protection Officers required in Europe

Why is this so Critical?

GDPR is the largest regulation that specifically focuses on personal data privacy for individuals. 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 for individuals. It further refines and focuses data security to mitigate and where possible reduce the negative impact of private data exposure to people.

In the event your organization loses private data associated with EU citizens, you must report this loss to a relevant supervisory authority. 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 the cybercriminals. Protected data losses are exempted from supervisory authority reporting because there's no EU citizen private data exposure. What the hackers got was unreadable.

DataKeep™ – The Solution

DataKeep technology is designed to encrypt data on Windows and Linux, physical and virtual data servers. Better than a meets minimum solution, it helps assure data privacy and protects against brute force attacks. The SPxCore™ technology combines AES-256 certified encryption and internal key management certified by the National Institute of Standards and Technology (NIST) to be FIPS 140-2 compliant. DataKeep takes full advantage of the AES-NI hardware acceleration available in most current processors for optimal performance. For your added protection, no "backdoor" exists, even for intelligence or law enforcement agencies.

For deployment flexibility, DataKeep works at both the storage volume and individual file levels. A single console is used to administer all data access policies, permissions and provisions lightweight agents across on-premises and cloud assets. It supports a separation of duties between security and product admins meaning no individual has complete system control. Transparent, built-in key management capabilities enable creation, rotation, and revocation/shred activities and support local key storage preventing cloud service providers from seeing unencrypted data.

All event logging (permits and denies) occurs in real time and is recorded for review or can be forwarded to a security information event monitoring (SIEM) application. DataKeep will help you meet regulatory requirements for DFAR, NIST, HIPAA, HITECH, FISMA, Sarbanes-Oxley, GBLA, PCI and more including most local, state and global requirements.

EU Citizens live Everywhere

As a CISO or the person in-charge of your organization's IT security, you should be aiming for GDPR-like compliance with all transactions involving your current and future customers, formally declared as EU citizens or not. Why? Because trying to identify your organization's relevant exposure will eventually become an intolerable burden. Agree or disagree, GDPR is generally a good idea for preserving whatever's left of your customer's personal privacy regardless of their passport origin.

And the nature of what data needs protection is multiplying with every effort you're making to better serve the customer's interest. 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, social media relationships and more. Better to provide the pound of protection now and avoid future loss notifications and identity protection service offerings.

About Security First Corp.

SecurityFirst™ specializes in data-centric security solutions – providing cryptographic splitting across a range of security options for robust security and policy defined access controls – all intended to meet the growing mandate for data privacy. Our mission is to provide innovative and affordable software solutions that protect one of the world's most valuable assets – digital data. DataKeep software protects any data from being exposed in the event of a breach – making it useless to hackers, and allowing you to control access to your data and help track unauthorized activity regardless of the data location.

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

16-20673-000 Rev. A0