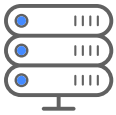
Are you all set for the GDPR?

Businesses of all sizes and industries will be required to implement appropriate technical measures to comply with the GDPR regulations, if they wish to operate in the EU and/or process EU citizens' personal data. As the GDPR imposes strengthened authority and heavier sanctions, and the requirement to notify data breach to both supervisory authorities and data subjects, businesses find themselves in a position to explore and implement technological and organizational measures to ensure compliance with the regulations.

How businesses can achieve technological compliance with the GDPR

As data security industry is providing the businesses with a plethora of technological measures for the GDPR compliance, finding and implementing the measures that fit specific needs may not be the easiest task. Secudrive believes that one solution cannot do it all, and that the businesses must initially consider the key security principles that will translate into the right set of technological measures. By following the life cycle of data, businesses can begin their journey to technological compliance with the GDPR.



Data Storage

- Physical security to prevent intruder breaches
- Encryption to protect hacker or theft threats
- Setting data storage off the internet to prevent access outside the LAN
- Anti-virus vaccines to stop cyber attacks
- Backup to ensure business continuity in case of disruptions

Data Processing

- Least privilege approach to give file access to only authorized users
- Visibility with monitoring and logging of user and file activities
- Persistent data security even out of secure premises

Data Erasure

- Overwriting the existing data with randomized data and algorithms
- Degaussing, or elimination of magnetic fields on disks for complete erasure
- Brute destruction of devices

Secudrive
File Server

Secudrive
USB Drive Solutions

Secudrive
Device Control

Secudrive
Sanitizer

SECUDRIVE
3150 Almaden Exwy, Suite 110, San Jose, California 95118
Web: www.secudrives.com | TEL: 1-408-613-2561 | E-Mail: info@secudrives.com

Secudrive solutions go further than just compliance with the GDPR

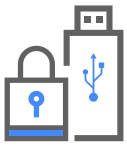
Implementing security solutions for the GDPR could mean obstructing work productivity among employees due to increased number of file/folder access limitations. However, Secudrive solutions do not compensate work productivity for security. Without having to worry about accidental or malicious data breach threats, business owners can still allow employees to perform their tasks.

Secudrive File Server

Office / CAD

File server DLP that stops insider threats leaking your personal and confidential data out of the file servers and blocks external cyberattacks from damaging your IT infrastructure

- Digital Rights Management that can restrict file copy, print, screen-capture, and network-transfer, and enable watermark printing
- Application whitelisting that prevents unauthorized applications and malicious codes from being installed and run on file servers
- Real-time monitoring and logging of user/file activities that provide organization-wide visibility and thorough audit trails
- High compatibility with seamless integration with existing enterprise environment like Active Directory and DFS
- Secure audited copy protocol (SACP) that provides initial file encryption for export prior to transportation on Secudrive USB drives



Secudrive USB Drive Solutions

Basic/Office/CAD, Standalone/Plus

HW-encrypted, remotely manageable USB drives that are specialized in protecting your data from unauthorized leakage and breach even while on the move and while being edited

- HW-encryption with AES-256 crypto-chip provides excellent encryption and TMUSB Security™ 2.1 detects and blocks infected files
- Password protection with complex rules and automatic lock/wipe feature that is enabled after a designated number of wrong entries
- Digital Rights Management that can restrict file copy, print, screen-capture, and network-transfer, and enable watermark printing
- Remote management software helps admins to manage and update USB drive security policies from a centralized location
- Real-time monitoring and logging of user/file activities that provide organization-wide visibility and thorough audit trails

Secudrive Device Control

Basic / Enterprise

Endpoint solution that controls various ports to ensure that unauthorized storage devices do not leak your confidential data and infect your IT infrastructure with malicious codes

- Regulates USB, Wi-Fi, LAN, IEE 1394, and more to prevent confidential data leaks via devices from external environments
- Monitor activities by USB drives, external HDD, and smartphones that are connected to endpoint PCs with permission
- Temporary port permission for a certain period of time, only when approved by the administrator
- Designated port and device permission to maintain work productivity only among the employees with security clearance

Secudrive Sanitizer

Portable / Enterprise

Cost-effective disk erasure solution that helps businesses to completely erase stored data on multiple disks simultaneously and remotely from a centralized location

- AD GPO implementation and MSI file installation allow multiple PC wipes while unattended and remotely from a centralized location
- Effortless disk erasure with only a few clicks, even while operating systems are running
- Real-time monitoring and logging of disk erasure process that provide organization-wide visibility and thorough audit trails
- Internationally certified deletion algorithms and compatibility with various disk types

SECUDRIVE
3150 Almaden Exwy, Suite 110, San Jose, California 95118
Web: www.secudrives.com | TEL: 1-408-613-2561 | E-Mail: info@secudrives.com