Whitepaper

SecureDoc™ by WinMagic

The EU GDPR: Assess Your Readiness

How to Ensure You're Prepared for 2018 and Beyond:

We've read it so you dont have to!

Are You Prepared?

According to Gartner,

> By the end of 2018, over 50% of companies affected by GDPR will not be in full compliance with its requirements

WINMAGIC®

SecureDoc™ by WinMagic

The EU GDPR: Assess Your Readiness

How to Ensure You're Prepared for 2018 and Beyond

A New Era of Data Privacy and Protection is Around the Corner.

Data as much as currency, is the lifeblood of the modern world, from financial transactions to medical procedures, it's essential to everything we do. Now that the EU General Data Protection Regulation (GDPR) has been adopted, the future of data movement in the EU and globally has forever changed. After more than 20 years, the new GDPR will replace the former EU Data Protection Directive, effective May 25, 2018. The Regulation expands the scope and enforcement of data privacy, bringing with it uncertainty, challenges and new responsibilities for organizations on a global scale. No one can afford to stand by, as the Regulation delivers serious corrective measures and financial penalties for non-compliance – up to the higher of €20,000,000 or 4% of global revenue.

Evaluate processes across all departments to know what, where and how EU resident data is stored, processed and transferred in and out of the corporate structure.

Adopt data minimization practices and implement appropriate organizational and technical safeguards, including encryption.

Evaluate processes to ensure that consent is voluntary and explicit. Ensure that consent can be withdrawn as easily as it is given.

Consider the rights of data subjects, assess your capabilities to communicate with subjects, and respond to requests from a minimum of 72 hours to a maximum of one month

Here's What You Need to Know:

Expanded Global Reach.

The GDPR will enforce a substantial set of new requirements, not just for those operating in the EU, but also those outside of the EU who process data in connection with the offering of goods and services to, or monitoring the behavior of, EU residents [Article 3 (1)(2)].

What is 'Personal Data'?

It's not just passwords and ID numbers, the GDPR defines personal data as "any information relating to an identified or identifiable natural person" – making reference to names, identification numbers, location data, online identifiers or any data related to physical, physiological, genetic, mental, economic, cultural or social identity [Article 4 (1)].

Consent Re-Defined.

It is now considerably harder for organizations to obtain valid consent from data subjects (EU residents). GDPR defines consent as "a statement or a clear affirmative action" [Article 4 (11)] – a significant change from the former EU Directive stating that the data subject must "signify" consent. Furthermore, data subjects have the right to withdraw consent, while organizations must be able to demonstrate consent [Article 7].

Rights, Rights, and More Rights.

One of the most notable changes from the former EU Directive to the new EU GDPR is an expanded set of data portability and accessibility rights for EU residents, including:

- The Right to Access Data [Article 15]
- The Right to Rectify or Erase Data [Article 16/17]
- The Right to Restrict Data Processing [Article 18]
- The Right to Data Portability [Article 20]
- The Right to Object to Data Processing [Article 21]

Businesses must also respond to any one of these requests by a data subject within one month [Article 12 (2)].

SecureDoc™ by WinMagic

Establish a framework for accountability and determine requirements for a Data Protection Officer and Data Protection Impact Assessment.

Roles and Responsibilities.

In addition to obligations to keep records of processing activities [Article 30], GDPR places onerous responsibilities on organizations to demonstrate compliance. Where an organization's core activities consist of large scale data processing operations, they are required to designate a Data Protection Officer (DPO) to monitor compliance and to act as a point of contact for the Member State's Supervisory Authority. Such organizations are also required to conduct a Data Protection Impact Assessment to determine the impact of data processing operations on the privacy of personal data.

Enforcing compliance within the organization can be the biggest challenge. Reduce the human element wherever possible by applying least-privilege policies and implementing proper technical safeguards, including removal of right, encryption and access controls.

Data Protection by Design.

Businesses are required to implement "appropriate technical and organizational measures" designed to safeguard personal data and minimize data collection, processing, and storage [Article 25 (1)]. The new 'data protection by design' principle encourages the use of techniques including encryption and pseudonymisation, alongside efforts to minimize the processing of data.

Article 32 of GDPR titled "Security of Processing" contains less than 300 words regarding security mechanisms for data processing, making it difficult for businesses to have a clear picture of how to implement appropriate technical safeguards. Compliance is difficult without clear guidance, but as we've seen with regulations on a global scale (eg. HIPAA, PCI DSS, etc.), when a specific mechanism is explicitly mentioned, it should be considered a requirement. Otherwise auditors often determine that your security measures do not meet their interpretation of an "appropriate level of security" [Article 32 (2)]. Encryption is explicitly mentioned as a recommended technique to address the security of processing personal data – a key requirement of the law. By applying encryption and appropriate management tools, organizations can confidently demonstrate compliance with ease.

Prepare a breach notification procedure and apply comprehensive encryption to prevent data breaches and subject notification.

Data Breach Notification.

Unlike the EU Directive, which left data breaches untouched, the EU GDPR sets out strict requirements in the event of a personal data breach. Notification of a breach to personal data must be made "without undue delay and, where feasible, not later than 72 hours after having become aware of it." [Article 33]. Furthermore, when a personal data breach contains highly sensitive information, the responsible organization must notify all affected individuals [Article 34].

However companies that encrypt personal data gain the advantage of not having to notify data subjects in the case of a breach, a damaging and costly process [Article 34 (3)(a)]. We have seen numerous examples around the world that when companies report a breach to customers, their stock prices and profits take a hit, senior executives lose their jobs and brand reputation plummets. Encryption is the simplest and most cost-effective method to avoid subject notification and the evident consequences.

Develop a response plan in the case of an audit or investigation as a result of a breach. Keep a record of all measures taken to protect the privacy of personal data.

Investigations, Audits and Penalties.

Each Member State of the EU – 28 in total – must provide one or more independent public authorities responsible for monitoring and enforcing EU GDPR [Article 51]. These Supervisory Authorities (SAs) are provided with some serious powers, including the ability to:

- Conduct Investigations and On-Site Audits [Article 58 (1)]
- Order Compliance within a Specified Period [Article 58 (2)(d)]
- Order Breach Notification to Data Subjects [Article 58 (2)(e)]
- Impose a Temporary or Definitive Ban on Processing [Article 58 (2)(f)]
- Impose Serious Fines [Article 58 (2)(j)]

The GDPR also introduces a tiered approach to fines. Less serious violations will result in either a fine €10,000,000 or 2% of global revenue whichever is greater. However, for more serious violations, such as a breach of an individual's rights or a breach as a result of an international transfer, fines are doubled – €20,000,000 or 4% of global revenue [Article 83]. Regardless of the violation or magnitude of breach, serious consequences follow.

SecureDoc by WinMagic

Lessons from a Global Perspective.

Big Data and Cloud Computing is changing the way we view data privacy and protection. Regulations are rapidly evolving – now on a global scale – introducing a new approach to data protection. Privacy and security are increasingly engrained in business strategies, no longer viewed as a hindrance to, but rather a necessity for success. When it comes to the GDPR, the stakes are high, emphasizing the need for businesses, organizations and governments alike to adopt comprehensive data protection practices across all levels and departments.

The alternative approach – as we've seen with breaches worldwide – is no longer a viable option. In the United States for example, the 2009 Health Information Technology for Economic and Clinical Health Act (HITECH) introduced dramatic changes to enforcement of the Health Insurance Portability and Accountability Act (HIPAA), increasing penalties up to $1.5 million. Soon afterwards, fines and settlements increased year over year, reaching record levels in 2016. Supervisory Authorities may similarly look to make an example and set precedence within their Member State by issuing serious fines and/or corrective measures following the compliance deadline in May 2018.

Nevertheless, many organizations will not be compliant by 2018, in part due to budget cycles. For an IT project of this magnitude – provided two years notice for GDPR compliance – this is a very short timeframe. Furthermore, budget cycles occur typically once a year, which means that unless the past two budget cycles included provisions for GDPR compliance, businesses will be forced to implement compliance measures in a matter of months or even weeks.

Where to Begin with Security? Start with the Foundation.

Navigating the GDPR minefield is an onerous task for IT leaders and their teams. However, a risk-based approach to data privacy – known as data protection-by-design – can significantly reduce the potential of non-compliance violations, or worse yet, a breach. If companies compare the potential costs of non-compliance with the cost of implementing technical safeguards, like encryption – when it comes to the GDPR – encryption will win in virtually every scenario.

What About Encryption?

Encryption is a recommended solution throughout the EU GDPR:

Article 6 – Lawfulness of Processing

- **Consider appropriate safeguards, including encryption (4)(e)**

Article 32 – Security of Processing

- **Implement encryption to ensure a level of security appropriate to risk (1)(a)**

Article 34 – Communication of a Personal Data Breach to the Data Subject

- **Avoid subject notification with encryption (3)(a)**

Businesses must be smart about implementing cost-effective and efficient ways of addressing the level of risk across their IT environment. Encryption is a recommended practice throughout the GDPR legislation, referenced in sections addressing the lawfulness, security, and breach notification of personal data. At WinMagic, we believe that encryption for data-at-rest across physical, virtual, and cloud environments is foundational to data protection by design.

Endpoint Encryption: Foundational to Data Protection by Design.

Ransomware and phishing attacks may grab the headlines, but one of the leading causes of data breaches across all industries is simple and often forgotten – lost or stolen devices. It's important that organizations protect networks and users from malware, ransomware and other such attacks. However, it is critical that devices and the data that resides on them are locked down and protected from unauthorized access or disclosure – whether malicious or unintentional.

Servers, desktops, laptops, tablets and even removable media – whether residing in or outside of the EU – serve as potential outlets of sensitive data if they are not properly protected. Full Disk Encryption (or FDE) provides comprehensive, foundational protection to prevent against the "destruction, loss, alteration or unauthorized disclosure of, or access to personal data…" stored on devices across the enterprise [Article 32 (2)]. It's also critical that organizations follow least-privilege practices – providing access only to information and resources necessary for specific processes, users or programs. Key management combined with encryption can help organizations to enforce access controls to personal data and maintain active security intelligence across your IT environment.

SecureDoc Endpoint Encryption

WinMagic's SecureDoc Enterprise can help confidently demonstrate compliance and gain the advantages of protecting data with industry-leading full disk encryption and intelligent key management across virtually any device, platform and operating system.

SecureDoc by WinMagic

Cloud IaaS Encryption: Data Governance and Enterprise Control.

Infrastructure as a Service (IaaS), offering on-demand and scalable compute, storage and networking hosted by a provider, is being adopted at a magnitude never seen before. More and more businesses are migrating data, applications and other business activities from onsite data centers to the Cloud. However, Cloud Service Providers (CSPs) share liability with their users when it comes to the privacy and protection of data, ultimately leaving users responsible for the security of their assets in the Cloud.

Microsoft Azure – Shared Responsibility

Microsoft Chief Privacy Officer (CPO) Brendon Lynch announced in February 2017 that Microsoft – with 100+ data centers and more than 200 cloud services – is committed to GDPR compliance by 2018 across all cloud offerings. However, Lynch was quick to mention that "it is important to recognize that compliance is a shared responsibility," reinforcing the understanding that migrating assets and operations to the Cloud does not mean migrating risk to your Cloud Service Provider.

When selecting a cloud provider or a partner, where you physically store your data won't necessarily be at the forefront of your mind. However, it should be, because exporting data to foreign countries can result in severe penalties. In fact, EU GDPR will hold both cloud service users (data controllers) and their providers (data processors) jointly responsible for appropriate protection measures and breaches to data privacy [Article 26]. Although Cloud Service Providers have stepped up their data protection game following the announcement of EU GDPR, it's the cloud users that ultimately retain control of, and responsibility for, security of their content.

Safe Harbor No More: EU-US Privacy Shield

The EU-US Safe Harbor Framework was negotiated in 2009, serving as the primary mechanism under which thousands of businesses legally transferred data across the Atlantic. In October 2015, the EU Court of Justice declared the agreement invalid, based on the notion that the EU Commission had not evaluated equivalent protections in the US. In July 2016, the EU-US Privacy Shield took effect, bringing in stricter obligation for protection and reporting, increased surveillance, and more options for citizens to file complaints and claims.

Data is increasingly distributed across hybrid IT environments – residing on endpoints, stored in corporate data centers and across public clouds. Given this reality, there are three key concerns when it comes to protecting data stored with Cloud Service Providers:

- The threat of attackers compromising a cloud service to access data stored in the Cloud
- The threat of an "insider" stealing a physical drive or server that contains customer data
- The threat that a government issues a subpoena or warrant to gain access to customer data without their given consent or knowledge

Fortunately, these threats across the public cloud landscape can be addressed simply and effectively with volume and full-disk encryption for Cloud IaaS instances, Virtual Machines and Storage. Furthermore, enterprise-controlled, on-premises key management ensures proper access controls and data governance, all without being locked in with any one Cloud Service Provider. Enforcing compliance can be especially difficult in the Cloud. GDPR-specific controls such as geo-fencing, time-based rules, and cloning restrictions will help reduce the risk of external threats, and more importantly, internal misuse by ensuring sensitive data remains unusable outside of approved policies.

WinMagic's SecureDoc Enterprise helps businesses, organizations and governments alike tackle the challenges associated with securing data across endpoints, virtualized and cloud deployments, offering the kind of state-of-the-art data protection, access management, monitoring and reporting that EU GDPR mandates.

Find out how WinMagic can help you on your journey to GDPR compliance

info@winmagic.com | www.winmagic.com

WINMAGIC®

US & Canada +1 888 879 5879 | United Kingdom +44 0148 334 3020 | Germany +49 69 175 370 530 | Japan +03 5403 6950 | India +91 124 4696800 | APAC-Singapore +65 9634 5197