Preparing for the General Data Protection Regulation (GDPR)

Technology Paper

Tough European Union Standards Are Set to Impact Cyber Security and Compliance Worldwide

As an early adopter and leader in the development of drive-level encryption technologies, Seagate understands that the most valuable asset in any storage system is the data itself. And while encryption is only a small part of any true security strategy, it can help with privacy compliance.

Recent high profile mass data breaches, such as Equifax and Yahoo, have brought cyber security issues to the mainstream. The GDPR means tough European Union (EU) standards on security and compliance will also become the norm in the US and worldwide. There is now greater emphasis on accountability, and drive-level encryption technologies are one method by which organizations can demonstrate this.

Changes to the GDPR

The GDPR is the most significant change in the world of data protection in a generation. It updates the law to recognize the significant advancements in technology during the last 20 years, and to address those technologies that will likely emerge in the future. The goal is twofold: 1) balance an individual's right to protection and 2) allow a data-based economy to thrive without stifling innovation.

Key changes at a glance:

Scope. The GDPR applies to organizations based in the EU, and any organization anywhere in the world which offers goods or services or monitors the behavior of people located in the EU. Citizenship or residency status is not pertinent. The GDPR also contains direct obligations on service providers (known as processors) for the first time. Furthermore, the European concept of personal information is broader than the US concept of personally identifiable information (PII), and includes online identifiers such as IP addresses.

Accountability. This is a critical thread running throughout the GDPR. Accountability leads to a number of obligations for organizations responsible for personal information (known as controllers). It will not be sufficient for organizations to simply comply, they must demonstrate their compliance. Organizations will have to keep records, record and justify their decisions, record an individual's consent, and may have to prove this to a European regulator.

Security. The GDPR requires that organizations put "appropriate technical and organizational measures" in place to protect personal information. Technical measures include drive-based encryption, passwords, access controls, two-factor authentication, etc. Organizational measures include information management policies, staff training, and having an information governance structure in place. What defines appropriate depends on the circumstances: the type of data being processed, how sensitive it is, the volume, and the overall risk of data breaches.

Breach notifications. Data breaches are any inadvertent loss or sharing of personal information. This can be due to hacking incidents, loss of an unencrypted hard drive or failing to dispose of old records securely. Controller organizations must report these to the regulator within 72 hours and may have to respond to the affected individuals. Processor organizations have to inform their customer as soon as possible.

Fines. One of the aims of the GDPR is to push data protection/security to a board level issue. As a result, the fines are significantly increased by up to 4% of global annual gross turnover or €20 million, whichever is greater. EU regulators also have significantly broader powers to investigate and put sanctions in place—including ordering an organization to cease processing data.

Pseudonymization. Any form of reversible encryption is known as pseudonymization in the GDPR. It refers to masking the data using some process, and keeping the key required to undo the process separate. Encryption and pseudonymization are greatly encouraged throughout the GDPR as they are considered methods of significantly lowering the risks to individuals.

Principles. The GDPR is principles-based legislation, based on the same basic and relevant data protection principles that have been around since the 1980s. They include: acting within the law; informing individuals how their data will be used; only using data for a specific purpose; collecting the minimum data necessary; not keeping data longer than necessary, etc.

Privacy by design and by default. These GDPR concepts state that privacy/security considerations should be baked into all data processing. Organizations should consider protection principles when designing all new products/services. Parameters should be set to collect the minimum amount of personal data necessary.

Individuals' rights. Under GDPR, individuals will have new and expanded rights. These include the right to ask any organization handling their information for a copy of it, to have it corrected if inaccurate, or deleted if no longer necessary. There are also rights to object to certain processing or have one's information moved to another organization. These rights are not absolute, so organizations must understand how they should apply.

Data processing agreements. The GDPR contains specific terms that must be in place between controllers (i.e., customers) and processors (i.e., vendors). Organizations will need to put these terms, which cover items such as security obligations, in place by May 2018.

Transfers. As with the current law, transfers of personal information outside the EU are prohibited, unless one of a limited number of safeguards are in place. For US organizations the most relevant are the EU/US Privacy Shield, the EU Model Clauses or– for larger organizations – Binding Corporate Rules.

Data Security/Encryption as a Compliance Tool

Seagate's Self-Encrypting Drives (SEDs) encrypt all data as it enters the drive using an encryption key stored securely on the drive itself. The drive is encrypted at rest by default. To retire or repurpose the drive, the drive owner sends a command to the SED to perform an Instant Secure Erase (ISE). The ISE uses the SED's cryptographic erase capability to change the data encryption key. The data becomes unreadable and cannot be recovered.

Encryption and pseudonymization are encouraged throughout the GDPR and, in fact, are mentioned 20 times in the text. While not specifically required, they are powerful tools and organizations that use them will benefit from lower compliance obligations. In particular, encryption can help in the following areas:

Security. While the GDPR leaves it to organizations to determine what appropriate security is, encryption is one of just four measures that are specifically suggested. When deciding which measures are appropriate, organizations must take into account the state of the art, costs of implementation, the type of processing and the risks to individuals. This is an obligation for both controllers and processors.

Encryption is one simple step organizations can take to lower risk, and is always something that is taken into account by regulators in determining whether to levy a fine, and if so, the amount.

Fines. The GDPR sets out the factors a regulator will take into account in determining the level of a fine to impose on an infringing organization. One factor is the technical and organizational measures that were taken to adhere to Privacy by design/default and Security. Encrypting hard drives, removable drives and laptops are a simple way of demonstrating compliance with these obligations, thereby reducing the amount of any fine.

The regulator will also consider the negligence of the organization. Most regulators would consider encryption of data-at-rest and in transit to be a basic measure, particularly if the data is sensitive. Regulators have little patience for organizations that don't put such obvious measures in place and so without SEDs an organization increases its risk of a much larger fine under GDPR.

Breach notification. An organization must notify the regulator about a data breach unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Where data has been securely encrypted, e.g., after ISE, then the data would be largely useless to any hacker or identity thief. The risk to individuals is lowered and so it may not be necessary to notify the regulator, thus avoiding negative press for the organization. If the organization decides to notify the regulator in any case, it will need to describe measures taken to mitigate the breach, which will include its strong encryption.

The test of whether or not to notify the individuals affected is whether the breach results in a high risk to their rights and freedoms. The GDPR specifically states that such notification is not required where the data has been encrypted.

Principles. The problems of secure data deletion have led some organizations to securely store data rather than delete it. Not only is this expensive and increases the risk of data breaches but it breaches the principle of data minimization. Seagate SEDs allow organizations to repurpose defunct drives, confident that the data has been sanitized.

Further, there is an exception to the principle against using data for a further purpose if certain criteria are fulfilled. One criterion is whether the data has been pseudonymized.

Data protection by design. The GDPR lists pseudonymization as an example of a measure which implements data protection principles in their products/services. Data on Seagate SEDs is always encrypted at rest.

Data processing agreements. The GDPR requires that a controller and processor have terms in place to cover, among other things, security and data deletion. The customer must help to ensure that the vendor has appropriate security measures in place, and the vendor must agree to return or delete the customer's data at the end of the contract. While the data is not technically deleted, it is sanitized to an extent that it is not feasible for it to be recovered, which will be sufficient for most customer's needs. Seagate's data sanitization technology has been recognized as compliant with ISO 27001 and National Institute of Standards and Technology.

Individuals' rights. Individuals have the right to have their data deleted but only when the controller can identify that individual. With ISE, it will be impossible for an organization to link data to a specific individual and means that organization is not obliged to respond to the request, greatly reducing its administrative burden.

Conclusion

GDPR readiness is a major project for most organizations, and compliance will be an ongoing process following the May 2018 implementation. Organizations that have not yet considered how they will adapt to the changes list above need to formulate a strategy and take action immediately.

GDPR is broader than just data security. However, putting secure storage and encryption in place is one straightforward technical step organizations can take to demonstrate they have become compliant, especially for the accountability principle. And certainly Seagate SEDs can be an important tool in the overall compliance armory.

AMERICAS Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, United States, 408-658-1000
ASIA/PACIFIC Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888
EUROPE, MIDDLE EAST AND AFRICA Seagate Technology SAS 16–18, rue du Dôme, 92100 Boulogne-Billancourt, France, 33 1-4186 10 00