Hewlett Packard Enterprise

Business white paper

How LTO Ultrium tape can support a GDPR compliant data processing system

Disclaimer

The purpose of this document is to explain how **HPE StoreEver tape storage** solutions offer a number of benefits for businesses considering their GDPR compliance strategy. The information contained in this document is not intended and may not be used as legal advice about the content, interpretation, or application of laws, regulations, and regulatory guidelines.

What is the GDPR and what are its aims?

The General Data Protection Regulation (GDPR) is legislation developed to strengthen and unify data privacy protection for natural persons within the European Union. It can impact any business, regardless of location, that processes European individual personal data. Non-compliance could mean fines of up to the greater of €20 million Euros or 4% of the company's annual worldwide turnover for a corporate group.

The primary objective of the GDPR is provide rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. This objective comes at a time of unprecedented creation of digital information with more and more of this personal data is being processed than ever before.

The key principles of GDPR relating to the processing of personal data are lawfulness, fairness, transparency, purpose and storage limited, data minimized, accuracy, integrity, confidentiality and accountability. The definition of what constitutes personal data has also been considerably widened in the GDPR to include IP addresses, genetic, health and biometric data, as well as data types such as Global Positioning System (GPS), media access control (MAC) addresses, unique mobile device identifiers (UDID), and International Mobile Equipment IDs (IMEI).

In essence, the GDPR means that safeguards for personal data will have to be designed into the very fabric of how personal data is captured, managed, used and stored during its lifecycle. While this might appear challenging, for many organizations GDPR is actually an opportunity to gain better insight into where personal data is gathered, used, and stored in order to assess the robustness of how it is protected.

Technology Neutral

Before looking in more detail at how tape can assist with GDPR projects, it is worth re-iterating that GDPR is explicitly "technology neutral"[1] so that the protection of individuals' rights in respect of their personal data is not dependent on the techniques used. In other words, the GDPR does not recommend any single storage technology as a means of compliance. It is up to organizations to determine that the technology they use to process and store personal data complies with the GDPR.

In its paper on GDPR transformation, available from **hpe.com**[2], the consultancy group PWC created a technology framework with 5 domains and 16 technical capabilities to identify the functional requirements demanded by the GDPR across the spectrum of both structured and unstructured personal data. Reviewing this matrix, it is clear that there is no "one size fits all" storage platform or technique that will enable companies to simply tick a box marked "GDPR compliance." Some storage technologies fit certain aspects of GDPR better than others. And no two businesses are alike. Enterprises will probably need to evaluate their options and use a mix of solutions depending on which aspect of compliance they are trying to address.

The benefits of encrypting personal data using LTO Ultrium tape

Encryption—a key feature of LTO technology—is one of only a few techniques specifically mentioned by the GDPR in the context of data protection and security.[3] And when it comes to encryption, tape is a highly efficient and effective data protection solution for several reasons.

- Firstly, HPE LTO drives use the 256-bit Advanced Encryption Standard with Galois/Counter Mode of Operation (or AES256-GCM for short). AES256-GCM confirms to specific US and international standards published by a number of standards bodies, including: National Institute of Standards and Technology (NIST), International Standards Organization (ISO), and Institute of Electronic and Electronic Engineers (IEEE).

[1] Recital 15—**gdpr-info.eu/recitals/no-15/**

[2] **hpe.com/pt/en/resources/solutions/gdpr-data-protection.html**

[3] Recital 83—**gdpr-info.eu/recitals/no-83/** "**In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption.**"

- Secondly, the encryption technology is built into the HPE tape drive so there is no requirement for additional hardware and expenditure other than the HPE Encryption Kit (a pair of USB key server tokens). For more sophisticated environments, encryption key management is possible through HPE's Enterprise Secure Key Manager appliance or by license to other KMIP[4] compliant key manager solutions. But the main point is that the tape drive or tape library itself is doing the major task of encrypting terabytes, or even petabytes, of data "on the fly" instead of data being passed through an expensive secondary appliance.
- Thirdly, because the tape device manages the encryption process, there is no performance degradation for compression or encryption,[5] which offers massive benefits in terms of data throughput. Software-based encryption encrypts the data before it leaves the server and this approach places a very high load on the server as the software performs many mathematical operations using host processing power. In comparison, an LTO MSL6480 tape library with ten drives installed can write a petabyte of encrypted data in just 36 hours. This makes LTO encryption an extremely fast as well as a highly scalable process.

How tape encryption can mitigate the impact of a data breach as defined by GDPR

Tape encryption may also help customers minimize risk and make it easier to comply with critical GDPR requirements, such as data security.

Article 34[6] of the GDPR states that in the event of a personal data breach, controllers are obliged to communicate the incident to the data subject "without delay." But Article 34 also says that this communication will **not** be required if the personal data has been rendered unintelligible through the use of encryption. The ability of LTO Ultrium tape devices to encrypt large amounts of data quickly and easily may help reduce administrative workloads and mitigate the risk of GDPR non-compliance for enterprises processing personal data at scale.

This is significant because one of the fundamental changes brought in by GDPR compared to previous data privacy law is the scale of the penalties for non-compliance. As mentioned above, failure to comply with the GDPR may lead to hefty fines for organizations—up to a maximum of 4% of annual worldwide turnover of a corporate group or €20 million Euros, whichever is greater). A technology such as HPE StoreEver LTO tape, with its powerful AES256-GCM encryption features, could mitigate the risk of heavier fines if encryption has been used.

In the worst-case scenario of personal data being lost or stolen, which would constitute a data breach under Article 4 (12), if the data was encrypted, then Article 83 says that due regard shall be given to "the degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them pursuant to Articles 25 and 32."

- Article 25 places an obligation on data controllers to adopt "appropriate technical and organizational measures" to protect the rights of data subjects by design and default.
- Article 32 obliges controllers to "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk."

Encryption is specifically mentioned as one of the technologies that may mitigate the risk of data breach (e.g., "taking into account technical measures.....implemented by them") and by association, the consequential penalties. With its powerful encryption capabilities, and ability to scale to high levels of data throughput, HPE LTO Ultrium StoreEver tape solutions are worthy of strong consideration for any enterprise or business considering how to encrypt and secure large quantities of personal data to assist with an organizations compliance with GDPR.

How offline tape storage enhances the security of processing under GDPR

Another core benefit of tape technology relevant to security of processing considerations is the fact that tape is essentially an offline storage medium. Once removed from a tape drive or library host, cartridges can be placed in a controlled and secure facility to reduce the risk of data loss or disruption caused by cyberattack, malware or other hostile intent.

[4] KMIP—Key Management Interoperability Protocol is an industry-standard protocol for communications between a key management server and an encryption system. The KMIP specification is developed by the KMIP technical committee of the OASIS standards body (Organization for the Advancement of Structured Information Standards).

[5] A HPE LTO Encryption Technology White Paper is available **here**

[6] Article 34—**gdpr-info.eu/art-34-gdpr/**

"In the world of technology just about anything and everything is possible. It's simply a question of having enough time and money. In the real world however, both are limited resources, and is why we view the only realistic way to address the GDPR's requirements is through a risk-based approach, where the highest risk areas are addressed first and most comprehensively. Accordingly, enterprises should use the findings of their gap analysis, a cost/benefit analysis and scenario testing to identify and plan their priorities."[7]

This core feature of HPE StoreEver tape technology may be useful for companies facing up to the challenges of Article 32, in particular:

1. "The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;"
2. "The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;"

Should the primary production environment be locked down through cyberattack, or unavailable due to a natural disaster, personal data stored on encrypted tape can be recovered from a secure location and used to help systems return to operation.

Encrypted tape, because of its inherent offline nature has an advantage if a cyberattack occurs. It would be very difficult for a malicious individual to both gain authenticated system access and thence to the tape library or vault.

Deployment of tape, therefore, may greatly increase the resilience of an organization to recover personal data in the event of a physical or technical incident and lessen the potential risk of GDPR non-compliance.

The TCO benefit of tape

PWC points out (in their white paper "Technology's role in data protection—the missing link in GDPR transformation" mentioned above) that there is likely to be a cost/benefit aspect to any assessment of the risks of GDPR non-compliance.

Since tape has phenomenally low TCO compared to disk and cloud, it can help companies manage their risk more cost effectively. Business can protect large quantities of personal data securely and relatively inexpensively, which might help mitigate storage costs and accelerate progress towards GDPR compliance by freeing resources to be deployed elsewhere.

In their white paper comparing the cost of ownership for different storage technologies,[8] analysts ESG reported that "dramatic savings in hardware, media, staff, and maintenance costs can be achieved by leveraging tape over disk." ESG went on to conclude that "for IT organizations looking to increase their efficiency in the realm of capital expenditure, while boosting their ability to be an exceptional service bureau for the organization by freeing up highly skilled administrators to focus on other endeavors, LTO tape solutions warrant close consideration."

Finally, it's important to remember that the GDPR relates to personal data. The archive datasphere—which IDC forecast will be 2.25 ZB (2.25 trillion GB) by 2025—will contain vast quantities of commercially valuable, **non-personal** data for which tape undoubtedly remains the pre-eminent platform for long term retention because of the advantages of low cost, security and scalability.

Conclusion

There may not be a better business case for organizations to fortify their cybersecurity and risk management portfolios than the GDPR. The need to meet the higher data protection standards of the GDPR will offer organizations the opportunity to streamline IT, enhance server infrastructure security, and improve data management.

As the security of personal data becomes ever more central to economic growth and for society at large, the organizational costs of losing or misusing it are increasing and can be devastating from reputational and financial perspectives.

Hewlett Packard Enterprise is focused on the new world of threats and how to best protect against them. **HPE StoreEver tape storage solutions** can assist your organization with its GDPR compliance.

Learn more at
hpe.com/us/en/what-is/gdpr.html

[7] **hpe.com/pt/en/resources/solutions/gdpr-data-protection.html**

[8] **lto.org/2016/04/esg-study-reveals-astounding-storage-cost-conclusions/**

Sign up for updates

a00058058ENW, October 2018