ADVERTORIAL

Data protection through technical design

RDX removable disk technology meets GDPR requirements

Despite the GDPR not being the main task for IT managers, it does cause headaches, particularly for small and medium-sized companies. Data protection and data backup are of course a must, especially in view of other regulatory requirements such as the data protection recommendations made by government bodies or due to the risk of cyber-attacks. Removable disk systems such as RDX are suitable to better deal with these issues

The GDPR with its 99 articles in eleven chapters is intended to secure the protection of privacy and the processing of personal data. The good news: Many areas of data protection have not been not newly regulated by the GDPR, but they are now more critical as a result of possible penalties and/or the fear of waves of formal warnings. At the very least, the regulation will also make small and medium-sized enterprises (SMEs) put their data management to the test: What is stored, saved, and archived where? How long is data retained?

Article 25 (1) of the GDPR requires companies and organisations to take “appropriate technical and organisational measures” (TOM) designed to protect privacy and guarantee data protection principles.

This is also about “data protection by design,” and this is ultimately the IT department’s responsibility as it forms part of the GDPR.

Data retention and technology selection

This is about finding ways to secure, store and, if necessary, delete data. It must be possible to access data, regardless of whether it is located in online storage, a back-up, or an archive. Since this usually has to be guaranteed for ten years or longer, the choice of suitable storage technology is a critical decision. Ultimately, however, a data backup strategy using removable media remains necessary and transferring data to secure, resistant and removable media is a must.

The robust RDX media by Overland-Tandberg is optimised for this task. It combines the portability and reliability of tape drives with the speed of a hard disk. Files can be accessed quickly and directly in the file system; RDX is easy to use and compatible with common backup software including on-board tools such as WindowsBackup or Apple Time Machine. RDX media are extremely robust, designed to last more than ten years, fully backwards and forwards compatible and can therefore always be used in an RDX drive without any technological migration effort. RDX offers a data throughput of up to 1.2 TByte/h and storage capacities of up to five TByte per removable medium with ability to span multiple removeable cartridges for additional capacity.

Access control and encryption

According to the GDPR, personal data must be protected against “unauthorised disclosure” and unauthorised access. This ultimately concerns the possibility of subjecting data carriers to policy-based access control. The controller and processor must take steps to ensure that any natural persons under their authority who have access to personal data do not process it unless instructed to do so by the controller. Another point raised is the need for “pseudonymisation and encryption” of personal data and the “ability to ensure the confidentiality, integrity, availability, and resilience of systems and services in connection with processing in the long term.” This is a decisive criterion, particularly for data transfer and exchange.

RDX technology addresses these technical aspects through a series of recent developments. First, RDX systems are based on conventional hard disk technology, which most users, especially SMEs, are probably more familiar with than magnetic tape or cloud solutions. The media is fully compatible across all product generations, which is an enormous advantage when restoring archived data.

A free software application is also available in the form of the RDXCartridgeEncryptor Software (RCE) It allows encryption of all RDX secured data. The software is designed for easy and efficient use, based on the AES-256 encryption industry standard, which also provides NISP Secure Erase for complete elimination of data programmes, as well as a cryptographic key deletion functionality. The RDX encryption software thus offers SMEs a free solution for securely storing data.

Hardware encryption meets the highest standards

RDX PowerEncrypt also provides hardware-based encryption on the basis of the 256 AES-XTS standard for removable disk technology. Hardware-based encryption technology is easier to use than software, does not reduce processor performance and nor cause conflicts with operating systems and other software versions. The fastest super-computer available today is theoretically capable of generating 10^{14} keys per second and would take 3.31 x 10^{56} years to crack conventional 256 AES encryption. With RDX Power Encrypt, key entry is limited to one key per second, and is so robust the software can even resist hacker parallel cracking techniques used to reduce cracking time. RDX PowerEncrypt management via the RDX Manager supports up to eight users with different rights profiles and access hierarchies, an optional automatic drive identification as well as the analysis of password security on installation.

From FIPS to KPMG – certified solutions provide security

RDX PowerEncrypt currently supports internal RDX-SATA-III drives and media using Windows. It will also be FIPS 140-2 validated in this configuration in 2018. FIPS 140-2 (Federal Information Processing Standard) is a U.S. government standard and describes the encryption and related security requirements that IT products must meet for confidential use. The standard ensures that a product employs sound security practices such as approved, strong encryption algorithms and procedures. It also specifies automated procedures to be followed by individuals or processes when using the product and how modules or components must be developed for safe interaction with other systems. The FIPS 140-2 validation level stands for security and quality and certifies to all buyers that the requirements for security products are met. WORM technology (Write Once Read Many) is suitable for archiving according to regulatory requirements.

The rdxLOCK software has recently been certified by the auditing company KPMG, thereby approving the use of the integrated WORM function for a large number of national and international standards in accounting, bookkeeping and taxation.

This WORM function thus meets all requirements of current and future compliance regulations such as the European General Data Protection Regulation (EU GDPR).

In the debate surrounding the implementation of the GDPR, ”appropriate technical and organisational measures,” sec. 25 (1), remain requisites, which must be implemented in hardware, software, and suitable processes. RDX technology with removable disks, single drives or appliances and the corresponding software can provide valuable support in addition to other storage technologies: data protection through technology design!