FLASHBLADE® AND THE GDPR

How Pure Storage® FlashBlade systems help enterprises comply with the data processing and storage provisions of the European Union's General Data Protection Regulation.

EXECUTIVE SUMMARY

The European Union's General Data Protection Regulation (GDPR) went into effect on May 25, 2018. The regulation defines handling, use, and transfer requirements for entities that deal with the personal data of EU residents, as well as those individuals' rights with respect to their data. GDPR applies to all entities that handle the personal data of EU residents, regardless of whether the entities are in an EU member country. The regulation applies to the processing and storage of data in digital form, regardless of where processing and storage occur.

THE SCOPE OF THE GDPR

The GDPR declares that EU residents (called *natural persons* and *data subjects* in the regulation) own their personal data, and specifies both their rights with regard to it, and obligations of entities that acquire and process it, particularly with respect to keeping it secure and available.

Individuals' rights to their personal data include:

- The right to access it
- The right to rectify errors in it
- The right to know how it is being processed and to restrict the types of processing it undergoes (within certain legal limits)
- The often-cited *right to be forgotten* (i.e., to have personal data destroyed when it is no longer required for legitimate purposes).

The regulation classifies entities that deal with individuals' personal data as either:

Controllers

Entities that determine the purposes and means of processing personal data, or

> ***Article 1***
>
> **Subject-matter and objectives**
>
> 1. This Regulation lays down 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.
>
> 2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
>
> 3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.
>
> *Excerpt from GDPR Article 1 defining the regulation's purpose and scope*

Processors
: Entities that perform processing tasks as instructed by controllers.

An entity can fulfill both roles. In the context of the regulation, the term *processing* encompasses both:

Manual operations
: Acquisition, filing, alteration, and disclosure, etc.

Automated operations
: Electronic processing, storage, and transmission of data in digital form.

The GDPR regulates controllers and processors as to the types of personal data they may acquire and the purposes for which they may process it, and specifies protections they must provide against both unauthorized access and loss or destruction during processing, storage, and transfer. Additionally, it obliges processors to disclose what personal data they store and process to its owners, to rectify verifiable errors in it, and to destroy it when it is no longer relevant to its intended purposes. Finally, the GDPR specifies procedural mechanisms for compliance and lays out penalties for non-compliance.

Thus, the GDPR deals with both

Policy
: What data may be collected and for what purposes it may be used, the rights of EU residents with respect to their data, etc.

Technology
: How data in digital form should be secured against unauthorized access and destruction as it is processed, transferred, and stored.

COMPLYING WITH THE GDPR

Since May 25, 2018, entities that acquire and process the personal data of EU residents have been required to comply with the GDPR. Compliance requires that controllers and processors use verifiable procedures to prevent *personal data breaches*, defined in the regulation to be events that lead to "*the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*."[1]

In terms of policy, compliance encompasses organizational structures, data handling procedures, physical security of data repositories and processing facilities, and hiring, training, and auditing operations. From a technology standpoint, compliance consists of ensuring that computing hardware, software, storage, and communication facilities, when properly managed and maintained, provide high barriers to theft, unauthorized disclosure, alteration, and inadvertent or malicious destruction of EU residents' personal data.

[1] Official Journal of the European Union, 4.5.2016, Article 4(12).

A MODEL FOR HANDLING DIGITAL DATA

Figure 1 is a simple model of a lifecycle for personal data in digital form. The numbers in the figure represent points at which personal data must be explicitly secured.

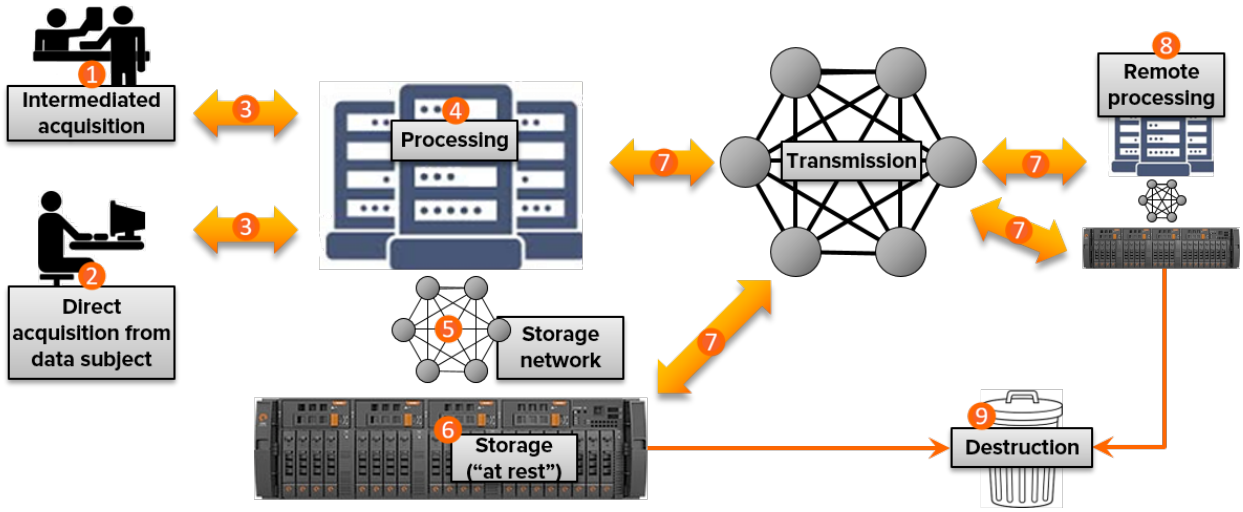

Figure 1: Digital Data Acquisition, Processing, Transmission, and Storage

1. Some digital data originates when a data subject interacts with an intermediary, e. g., a bank teller, salesclerk, or government official. The intermediary interacts with a computer system on the subject's behalf. Privacy and security depend on the trustworthiness of subjects, intermediaries, and processing systems, e.g., via robust vetting and authentication.
2. Increasingly, data subjects digitize their own personal data by interacting with ATMs, governmental and private sector websites, and so forth. Responsibility for securing personal data lies primarily with the networks and computer systems that the subjects use to interact.
3. Some communication links between data subjects, processors' agents, and processing facilities are permanent, and have strong security. But increasingly, data subjects and processors' agents use wireless (e.g., mobile credit card readers) and semi-public Internet access points to interact with processing facilities. These links must be secured against unauthorized access and passive "snooping."
4. Most processing of personal data subject to the GDPR takes place in physically secure data centers. Security of data during processing requires trustworthy, well-managed and maintained hardware and software, comprehensive auditing, and strict control of human access to computer systems.

5 The majority of data processors subject to the GDPR use storage networks to connect their servers to storage. For storage networks contained within a data center, data is secured while in transit by restricting access to facilities and equipment. For networks with external connections (e.g., to servers and storage in separate facilities or to remote replication targets), data must be secured by network-encryption while in transit.

6 Storage systems that hold data "at rest" must protect it not only against unauthorized access and alteration, but also against failure and theft of the systems or their components. Storage systems should encrypt stored data, manage encryption keys securely, closely control human access, and indelibly log all administrative actions.

7 Processors transmit both individual data items (e.g., credit/debit transactions) and bulk data (e.g., for analysis, testing, or archiving). Ideally, private networks would be used, but most processors use common carrier facilities. Typically, they secure transmission over public networks with virtual private networks (VPNs), encryption, or a combination of the two.

8 Sending personal data to a remote system creates a *copy*. The GDPR declares that data subjects have the right to know what copies of their personal data exist and the purposes for which they are used. In addition, they have a "right to be forgotten"—for their personal data to be eradicated once there is no longer a legitimate reason to retain it. To eradicate data, one must know where it is, so data processors are obliged to track copies as they move among their own and their processing partners' facilities.

9 The right to be forgotten requires that processors eradicate personal data upon owner request when it no longer serves a legitimate purpose. For individual items, responsibility for complying with this provision lies with the processor's procedures for dealing with data subjects. For bulk destruction of data sets, such as survey results, some storage systems support fast reliable eradication of large blocks of data.

PURE'S ROLE IN GDPR COMPLIANCE

As a supplier of data storage systems, Pure's key contributions to GDPR compliance are:

- Protecting data both "at rest" in its storage systems and in transit during replication between them (points 6 and 7)
- Keeping data available and secure as it moves between application servers and storage (points 5 and 8) over storage networks with connections outside the data center. This typically requires coordination with storage network and/or server facilities.
- Ensuring to the extent possible that no personal data is exposed in the logs that systems transmit to the company's Pure1 Virtual Private Cloud for analysis and troubleshooting. Technical Brief TB-210301[2] describes the role of Pure1 in GDPR compliance.

The remainder of this brief illustrates how FlashBlade storage can be a key component of an organization's comprehensive GDPR compliance strategy.

[2] https://support.purestorage.com/Pure1/Pure1_Security/Pure1_Security_Reference/Pure1_and_GDPR_Compliance

FLASHBLADE AND GDPR COMPLIANCE

As a supplier of digital data storage systems, Pure Storage makes every effort to keep the data stored in its systems both available to authorized users and secure against electronic intrusion and physical misappropriation. Availability and security measures provided by FlashBlade systems include:

Data Availability
Systems keep data intact and accessible during all single-component failures and many concurrent failures of multiple components

Access Control
Systems restrict administrative access to credentialed individuals, each with a defined role that permits specific actions. They provide no mechanism for administrators to access or modify stored data

Data Protection
Systems use a hardware implementation of the well-accepted AES-256 algorithm to encrypt *all* data and metadata stored in flash and staged in NVRAM. Encryption cannot be disabled. Both per-blade and system-wide encryption keys are managed autonomously and partitioned so that data on a misappropriated blade cannot be decrypted.

Data Integrity
Immutable snapshots provide unalterable records of data set contents at user-specified key points in time.

These properties help data controllers and processors "design GDPR compliance by default" as they implement new processing systems.[3] Pure Storage Technical Brief TB-190701,[4] *FlashBlade Security* describes how FlashBlade systems protect stored data from loss and unauthorized access under adverse conditions and attacks. When combined with strong network security to protect data while it is "in flight," and robust data processor and controller system access and data handling policies, FlashBlade systems can be an important component of an overall GDPR compliance strategy that is both comprehensive and cost-effective.

[3] Excerpt from GDPR Article 25 (Data protection by design and by default): "…the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

[4] https://support.purestorage.com/FlashBlade/FlashBlade_Security/FlashBlade_Security_Reference/FlashBlade_Data_Security_TB-190701

FLASHBLADE AND COMPLIANCE: KEEPING DIGITAL DATA AVAILABLE

FlashBlade systems provide robust facilities for keeping file and object data intact and accessible. The systems are designed to continue operating in the presence of hardware component failures, up to and including concurrent failure of two blades. RAID-HA protection makes data recoverable from all single and concurrent double read failures, as well as in many failures that affect more than two blades. Intra-device checksums detect *latent* read errors, both those that deliver corrupt data or data from the wrong locations.

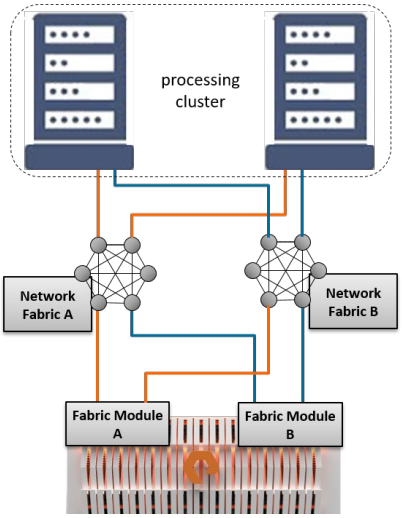

Figure 2: Redundant Client-to-FlashBlade Connections

Systems protect against administrative errors by imposing an automatic 24-hour delay when file systems and object buckets are destroyed. During the delay, file systems and objects destroyed in error can be recovered.

FlashBlade systems provide these protections together with data compression that conserves physical storage with virtually no impact on performance.

Pure Storage Technical Brief TB-160701[5] describes the FlashBlade architecture, including the techniques employed to protect stored data against loss and unintended destruction.

Not only do FlashBlade systems protect data against faults, they keep it available to application servers ("clients") via multiple storage network ports on separate *fabric modules* (in-chassis interfaces to the external environment). When FlashBlade systems are cross-connected to clustered clients through two independent IP network fabrics (Figure 2) data remains accessible for processing if either a network path, a client, or a fabric module should fail.[6]

Similarly, processors can configure connections between FlashBlade systems redundantly so that replication survives network and fabric module outages (Figure 3).

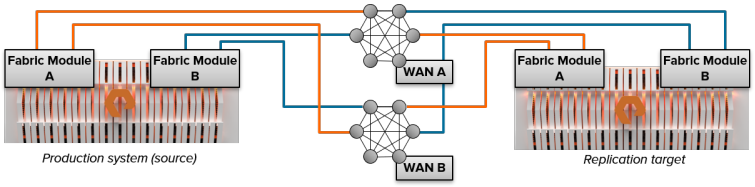

Figure 3: Redundant Replication Network Paths

[5] https://support.purestorage.com/FlashBlade/Purity_FB/FlashBlade_Technical_Reports/FlashBlade%3A_Scale-Out_Storage_Built_for_Big_Data_TR-160701

[6] Multi-chassis FlashBlade systems connect to their external environments via *external fabric modules* (XFMs), whose role is identical to that of the on-chassis fabric modules in single-chassis systems.

FLASHBLADE AND COMPLIANCE: KEEPING DIGITAL DATA SECURE

Digital data storage does not exist in a vacuum. Its inherent purpose is to create a durable record of manipulations of information by data processors or by data subjects. Storage is integral to the digital data lifecycle represented in Figure 1, particularly while data is "at rest" and while it is "in transit" between processing systems and arrays.

For example, the storage networks that connect application servers to storage (point 4 in Figure 1) carry personal data. For "air gapped" storage networks entirely within a data center, this data is typically protected by data processor policies that limit access to storage networks and to the servers and storage systems connected to them. Processors should restrict system access to specific trusted individuals, and specify administrative roles narrowly, with disjoint responsibilities. Different individuals should manage storage, servers, networks, and security.

Data on storage networks that have connections outside the data center should be protected by combinations of VPNs and encrypting network switches.

Systems should log all administrator actions. To comply with the GDPR, data processors must use IT products that implement policies to protect personal data and enforce those policies.

FlashBlade systems contribute to GDPR compliance by securing stored data against theft, either electronic (e.g., unauthorized access by an administrator or host computer), or physical (e.g., misappropriation of blades or entire systems). But in addition to this, security in other IT components as well as processors' policies are necessary for full compliance.

The key FlashBlade features that raise barriers to unauthorized data access are:

No administrator access to stored data

While authenticated administrators can delete[7] file systems and object buckets, no administrative interface (command line, graphical, or REST) includes any facility that would allow an administrator to retrieve or alter stored data.

Controlled administrative access

Each administrative login requires an account name and a password or public-private key pairs. Systems communicate with LDAP servers to validate administrative account credentials.[8] Each account is associated with a role that only permits specific actions. Every REST call must contain a unique *API Token*, generated by the system for each administrative account for which REST access is enabled.

[7] The term "delete" is commonly used in information technology contexts to mean either "make inaccessible," "obliterate," or a combination of the two. For example, a deleted file system on a file server becomes invisible to clients immediately, but unless it is *securely* deleted (physically erased), its data may remain on media until the space it occupies is reclaimed and overwritten. Pure's command line interfaces use the term "destroy" to mean "make invisible to clients," and "eradicate" to mean "obliterate contents." Destroyed FlashBlade data objects are invisible to clients but remain intact for 24 hours unless explicitly eradicated.

[8] Each FlashBlade system manages its built-in pureuser administrative account locally.

Secure administrative communications

CLI interactions between administrators and FlashBlade systems take place within encrypted secure shell (SSH) sessions. Browser communication uses HTTPS, both during authentication and for information exchanges. Systems use HTTPS with TLS encryption to transmit logs to the Pure1® Cloud.

Controlled access by client computers

Systems only execute I/O commands from clients that have been explicitly authorized to access specific file systems or object store accounts by a system administrator.

Logging of events and administrative actions

Systems log all administrative actions locally, and in addition, when connected to the Internet (as most are), regularly transmit logs to the Pure1 Cloud,[9] where they can be viewed by Pure Storage Technical Support Engineers (TSEs) or by agents of the system owner through the Pure1 Cloud *Manage* feature. Comprehensive logging of system events and administrator actions enables auditors to analyze all actions performed on a system.

Encryption of all stored data all the time

Systems encrypt all stored data and metadata using custom hardware in each storage unit that implements the AES-256 algorithm, widely accepted as the "gold standard" for digital data encryption.[10] Each storage unit on a blade uses a unique *device key* to encrypt incoming data before storing it in flash or staging it in NVRAM, and to decrypt stored data for delivery to clients. Storage units hold their device keys in encrypted form in special-purpose flash, using a system-wide *key encrypting key* (KEK) to encrypt them. Device keys are never exposed outside storage units.

Systems partition their KEKs mathematically and store each partition on a separate blade. More than half the partitions are required to reconstruct a KEK. At system startup, fabric modules request KEK partitions from all blades and use them to reconstruct the full KEK, which they send back to the blades. Blades relay the KEK to their storage units, which use it to decrypt the device keys that encrypt incoming data and decrypt stored data.

Immutable snapshots

Data in FlashBlade snapshots cannot be altered. Thus, they protect against inadvertent destruction of data, and provide point in time records that can be used to detect unauthorized alterations or thwart ransomware or other malware attacks.

From a policy standpoint, data processors should limit administrative access to computing, network, and storage systems to specific trusted individuals. They should specify administrative roles narrowly, with non-intersecting responsibilities (for example, different individuals should manage storage, servers, networks, and security servers), and automatically log all administrative

[9] https://support.purestorage.com/Pure1/Pure1_Security/Pure1_Security_Reference/Pure1_and_GDPR_Compliance_-_TB-210301 describes the role of Pure1 in GDPR compliance.

[10] The United States Federal Government certifies that the arrays comply with the FIPS 197 and FIPS 140-2 Level 1 data security standards. See https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3345.

actions unalterably. Processors should only employ IT products that provide facilities for safeguarding personal data and implement policies that utilize those facilities.

FLASHBLADE SYSTEMS AND THE "RIGHT TO BE FORGOTTEN"

Several articles of the GDPR relate to a data subject's "right to be forgotten"—the right to request that data controllers and processors destroy personal data that no longer serves a valid purpose (within limits imposed by member states' laws). Individuals' rights to be forgotten must be considered in two contexts:

Destruction of a single subject's data

Deleting a single subject's data requires knowledge of the structure of the files or databases that contain it. Complying with an individual's right to be forgotten therefore lies with applications that process data and their users, as well as with the processor's data set management policies. It must be possible to identify all instances of a subject's data (e.g., in snapshots, copies, backups, and other transformations of data sets) so it can be removed from derived data sets as well. Thus, data processor policies for tracking and managing digital data sets play an important role in compliance with this requirement.

"Deletion" at the application-level typically makes records inaccessible but does not immediately obliterate them physically. Data processors must physically destroy all copies of data subjects' obsolete personal records within an acceptable time after "deletion."

Destruction of data about groups of subjects

Record-by-record destruction of large data sets (e.g., obsolete polling results or no-longer required database tables) is usually too onerous to be practical. FlashBlade systems can *destroy* an entire file system at a single administrator command to expedite destruction of appropriately organized data sets. Destroyed file systems can be recovered by administrators for 24 hours (to protect against administrative errors), after which systems permanently *eradicate* them and reclaim and the storage they occupy.[11] A FlashBlade system can eradicate an entire file system, but data processor management policies must identify all copies of obsolete data sets and ensure that they are destroyed.

FlashBlade systems present data to clients in the form of files in file systems or objects in an object store service account. The systems have no awareness of file or object internal structures. Thus, while a FlashBlade administrator can destroy an entire file system, it is not possible to eradicate or alter data *within* a file system or object store service account without a command from a client computer. Bulk erasing of large quantities of data by destroying a file system is therefore feasible only when the items to be erased are the sole occupants of the file system.

[11] During the 24-hour period, an administrator with the appropriate role can eradicate a file system immediately.

THE DATA ENCRYPTION DILEMMA

The GDPR does not specifically mandate encryption of stored digital data. Within the data processor community, however, it is generally accepted that encryption of personal data throughout its digital lifecycle will ultimately be a practical necessity for compliance. As Figure 1 suggests, "end to end" encryption must occur in multiple stages. For example, data should be encrypted on the path between origin and processor (3 in Figure 1), but it must be decrypted for processing (4), and re-encrypted for transmission to and storage by storage systems (5 and 6).

For storage networks completely contained within the data center, protecting data in transit between servers and storage rests primarily with data processor policies and practices. But some storage networks, for example those that use iSCSI over Ethernet, cannot be isolated. This complicates end-to-end data encryption. One solution recommended by some GDPR consultants and IT equipment vendors is to encrypt data at the application server before sending it to storage, thus eliminating transmission and storage "in the clear." Data thus encrypted is protected—in primary storage, when sent to other servers, and when backed up. However, encrypting data at the server requires (a) managing encryption key distribution so that copies of data can only be decrypted for legitimate purposes, and (b) implementing policies to ensure that only authorized individuals have access to keys and data, and only for authorized purposes.

Setting key management aside, data encryption at the server covers many GDPR compliance requirements for digital data, but it carries a high cost. *Data reduction*—the elimination of redundancy in data prior to storing it—has become a universal expectation of data processors as they evaluate storage alternatives. Increasingly, processors budget for and acquire storage based not on raw capacity requirements, but on expectations of their data's reducibility. Reducibility varies widely, but typically falls in the range of 1.5:1—5:1. Because so much personal data is textual, it typically falls in the middle of the range or higher. Put another way, with reduction, processors can store a given amount of data in 20-67% of the physical capacity its unreduced size would suggest. Moreover, when data is reduced, storage cost, space requirements, and power consumption, are all proportionally lower.

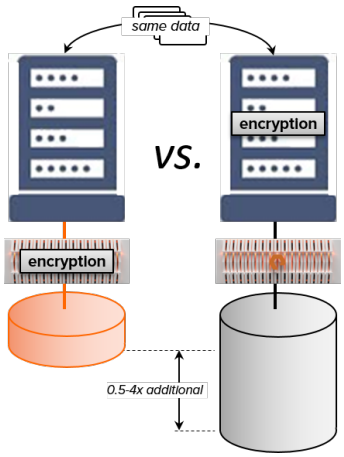

Figure 4: The Cost of Encryption at the Application Server

FlashBlade systems remove redundancy from data by *compression*—replacing sequences of bytes that occur multiple times within a block with descriptors that point to a single occurrence of each sequence.

But encrypting data inherently produces quasi-random bit patterns that essentially eliminate the possibility of

compression. Thus, even ignoring any computational impact of encryption on application servers, encrypting data at the server virtually eliminates the data reduction advantages that processors depend on.

Encrypting data at the server prior to transferring and storing it is only the tip of the storage cost iceberg. Each time data is copied—for analytics, for development testing, for backup, for archiving, or for disaster protection—0.5-4 times as much additional storage and network bandwidth are consumed compared to data reduced and encrypted by the storage system.

Moreover, server-side encryption keys are an inherent security weakness. For example, the key that encrypts a production data set must be available to systems that analyze copies of it, that use copies for development testing, and that restore backups. Every use of a data set widens the circle of systems and individuals with access to its contents. Worse, when production data sets are re-encrypted with new keys and then copied, the new keys must be available to all users of copies so they can correctly decrypt each instance of the data set they process.

Server-level encryption of sets of personal data is a "brute force" solution to the digital data security component of GDPR compliance—it does the job (provided that keys can be managed) but at significant cost to the processor, and ultimately, to the data subject. It sacrifices data reduction—arguably one of the most important storage technology advances of the past decade.

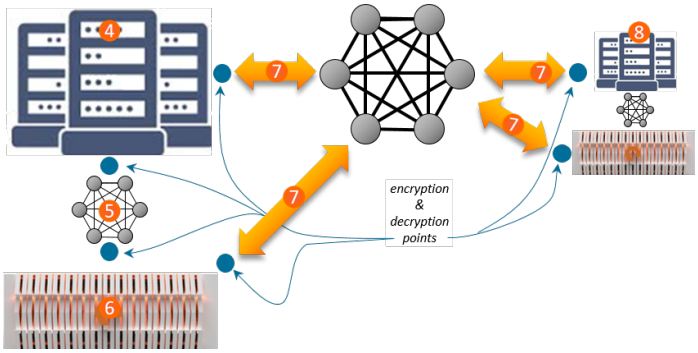

Figure 5: Encrypting Data in Transit

The alternative—encrypting at the storage level as FlashBlade systems do—preserves the data reduction cost advantage and mitigates the key management problem, but it exposes data as it moves unencrypted between servers and storage systems.

For storage networks contained within secure data centers, data in transit is protected by processor policies and practices.

But these measures do not protect data that is transferred over connections to remote servers and storage systems. Data processors may find it more robust and cost-effective to use network tools to encrypt data while it is being transferred between servers and storage systems, as well as between replicating storage systems (7 in Figure 4) and rely on storage system encryption (6 in Figure 4) to protect it "at rest" (stored). Compliance with GDPR digital data security provisions may require IT architecture redesign in some cases, but it is possible to provide robust protection throughout data's digital lifetime and still enjoy the cost benefit of data reduction.

Encrypting personal data during transit provides reasonable protection against "snooping" and "man-in the middle" attacks, but data remains susceptible to *threats from within*—administrators that divulge keys indiscriminately, authorize file system and object store service account access

by unauthorized “rogue” servers, and so forth. Thus, whatever the end-to-end data encryption architecture, it must be accompanied by policies that include interlocking safeguards against misappropriation and use by the data processor’s own personnel.

A COMPROMISE: SELECTIVE PSEUDONYMIZATION[12]

Application servers can encrypt data at different levels of granularity. They may encrypt every block they send to a storage system, data that they write to specific file systems or databases, or even specific files or database columns (for example names or other identifying characteristics). Because the GDPR is specific about the types of personal data that are subject to protection, some data processors may provide server-side encryption (or other types of pseudonymization) for sensitive items, and transfer non-sensitive items “in the clear.” Such strategies may enable them to comply with the GDPR’s digital data protection provisions while retaining at least *some* of the cost benefit of reduction. Selective encryption is likely to lessen the degree to which storage systems can reduce data, but where the percentage of non-sensitive data is significant, some benefit should still accrue. Moreover, selective pseudonymization is likely to consume less application processing power than encrypting all data that a server processes and writes.

[12] The term pseudonymization is used in the text of the GDPR regulation.

THE BOTTOM LINE

- From May 2018, compliance with the European Union's General Data Protection Regulation is effectively a condition of doing business in the EU.
- The GDPR contains both organizational, procedural, and digital data handling provisions. Digital data handling includes keeping personal data available and protecting it from misappropriation and misuse.
- The GDPR does not specifically require encryption of data in digital form, but end-to-end encryption simplifies compliance to the point where data controllers are likely to require it, and data processors are likely to adopt it as a standard practice.
- Encryption at the application or database server protects data throughout its digital life, but at a substantial cost in incremental storage due to the near impossibility of reducing it. Storage cost is multiplied each time data encrypted at the point of origin is copied for analytics, backup, testing, and so forth.
- Server-level encryption increases key management complexity and introduces inherent security risks due to the need to manage wide distribution of keys to every user of any copy of a data set.
- For systems such as FlashBlade, that reduce and encrypt data before storing it, end-to-end encryption can be achieved in combination with network encryption hardware and/or software.
- FlashBlade systems control administrator access, log every administrator interaction, and encrypt all stored and staged data and metadata *all the time*—encryption cannot be disabled, inadvertently or otherwise.
- The FlashBlade highly available architecture helps satisfy GDPR requirements for keeping subjects' data available for processing. In conjunction with redundant storage networks and clustered application servers, it can provide a secure, highly available environment for personal data in digital form as part of an overall GDPR compliance strategy.

Compliance with the digital provisions of GDPR is necessarily an integration of application, server, network, and storage data protection facilities, together with data processor policies and procedures for handling and protecting data while it is in digital form.

APPENDIX
FLASHBLADE AND GDPR COMPLIANCE

Table 1 lists excerpts from GDPR articles that relate to digital processing, storage, and transmission of personal data and describes the FlashBlade capabilities that help users comply with them.

Table 1: Relationship of GDPR Provisions to FlashBlade Properties and Capabilities

Article	Provision Excerpt	Relationship to FlashBlade Systems
3.1	This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.	FlashBlade systems have virtually no optional features. The systems' high availability, data security, and access controls are the same throughout the product line. Thus, no matter what model or where it is deployed, a FlashBlade system's role in GDPR compliance is as described in the body of this brief.
3.3	This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.	
4(2)	'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;	FlashBlade systems perform or participate in the operations highlighted in green.
4(12)	'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;	The body of this brief describes how FlashBlade's always-on data and metadata encryption, in conjunction with network encryption facilities for data in transit minimizes the possibility of data breaches. In addition, credential-based administrative access, together with rigorous logging of events and administrative actions minimizes the possibility that unauthorized processing or misappropriation will occur or go undetected. Finally, the systems' built-in resiliency against single and double component failures represent state of the art protection against accidental loss, destruction, or damage of personal data.
5.1(f)	processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').	
6.4(e)	...the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: ... the existence of appropriate safeguards, which may include encryption or pseudonymisation.	
17.2	Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	From a storage system standpoint, this provision primarily applies to bulk erasure of entire data sets. FlashBlade system administrators can destroy and eradicate entire file systems at a stroke. It is incumbent upon applications to direct the systems to delete individual files and objects.

Article	Provision Excerpt	Relationship to FlashBlade Systems
24.1	Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.	FlashBlade encryption uses the widely-accepted AES-256 algorithm (implemented in custom storage unit hardware) to keep stored data secure. The systems' high availability, administrative access control, and logging features all help processors comply with the GDPR data availability, security, and access control provisions.
24.2	Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.	
25.1	Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.	FlashBlade systems use the widely-accepted AES-256 algorithm to encrypt stored data. All data security, high availability, administrative access control`, and logging features are integral to every system. Taken together, they help data processors "design in" protections for personal data in digital form that comply with the GDPR's high availability, security, and access control provisions as they implement new processing systems.
29	The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.	
30.1	Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. *...several processing activities called out...*	FlashBlade systems log all administrative actions, including: • file system creations, resizings, protocol changes, and destructions, and recoveries • snapshot creations and destructions • client connections and disconnections. As such, they provide the raw information required to comply with this article.
32.1	Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	FlashBlade data encryption, high availability, administrative access control, and logging features all help processors comply with GDPR data availability, security, and access control provisions. However, full compliance also entails network encryption of data in transit, application trustworthiness (e.g., with regard to pseudonymisation), and rigorous policies for data and IT equipment access and handling by agents of the data processor.

Article	Provision Excerpt	Relationship to FlashBlade Systems
34.3(a)	The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;	Paragraph 1 of this provision defines the data controller's obligation to notify data subjects of personal data breaches "without undue delay." FlashBlade encryption and access control are regarded as "appropriate technical protection measures," so this provision is expected to apply where FlashBlade systems are used for data storage.
35.1	Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.	Through its system engineering organization, Pure Storage makes available a series of technical reports and briefs that controllers can use to help assess the impact of proposed operations on personal data protection. A complete assessment, however, would take into account all facets of a proposed operation, including data acquisition, processing, storage, transmission, and eventual destruction.

Users are advised to seek appropriate legal advice on GDPR compliance. Pure Storage customers are solely responsible for obtaining legal advice from competent counsel in appropriate jurisdictions on any actions they may need to take to be in compliance with any relevant laws and regulations.