PURE1® AND GDPR COMPLIANCE

This brief explains why Pure1 is an effective tool for managing Pure Storage® and Portworx® on-premise and cloud storage products in compliance 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 located in EU member countries. The regulation applies to the processing and storage of data in digital form, regardless of where the processing and storage occur.

THE SCOPE OF THE GDPR

In essence, the GDPR declares that EU residents (called *natural persons* and *data subjects* in the regulation and *individuals* in this brief) own their personal data, and specifies both their rights with regard to it, and the obligations of entities that acquire and process it, particularly in relationship 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 data destroyed when it is no longer required for legitimate processing).

> ***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*

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

Controllers
Entities who determine the purposes and means of processing personal data

or

Processors
Entities that perform processing tasks as instructed by controllers.

A single 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, the regulation 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

As of May 25, 2018, entities that acquire and process the personal data of EU residents are required to comply with the GDPR. Compliance requires that controllers and processors have in place 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]

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

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 is largely concerned with ensuring that computing hardware, software, storage, and communication facilities, when properly managed and maintained, provide high barriers to theft, unauthorized disclosure, alteration, and inadvertent and malicious destruction of EU residents' personal data.

PURE STORAGE AND PORTWORX PRODUCTS AND GDPR COMPLIANCE

As a supplier of both on-premises and cloud-based digital data storage products, Pure is committed to keeping the data stored by its products both available to authorized users and secure against electronic intrusion and physical misappropriation. For example:

Data availability

Data stored by the company's products and in Pure1 databases remains intact and available to authorized users in the face of single-component and infrastructure failures as well as many concurrent failures of multiple components.

Access control

Administrative access to deployed products and Pure1 services is limited to credentialed individuals, each with a specific role. Neither hardware nor cloud-based products have facilities that allow administrators to access or modify customers' data.

Data protection

- The FlashArray™, FlashBlade®, and Cloud Block Store products encrypt all stored data and metadata using the well-known AES-256 algorithm. Encryption cannot be disabled.
- In addition, FlashArray supports removable SmartCards and remote key management (KMIP) servers to protect data in situations where physical security is problematic.
- Portworx products use the encryption facilities of the underlying operating systems' crypto libraries, which are user-controllable.

Data integrity

All products are capable of producing immutable *snapshots* that provide unalterable records of administrator-specified data sets at key points in time.

These properties help data controllers and processors who use Pure Storage products "design GDPR compliance by default" as they implement new processing systems.[2] Technical Briefs

[2] 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."

TB-160201, TB-160202, TB-190701, and TB-160501[3] describe how FlashArray, FlashBlade®, and Pure1™ protect stored data from loss and unauthorized access, even under adverse conditions. Briefs TB-171101 and TB-180202 explain how FlashArray and FlashBlade systems can provide a foundation for an organization's overall GDPR compliance strategy. This brief describes the role of Pure1 in GDPR compliance. When combined with strong network security to protect "data in flight" and robust computer system access and data handling policies on the part of data processors and controllers, Pure Storage products and services can be important components of a GDPR compliance strategy that is both comprehensive and cost-effective.

Pure executes Data Protection Agreements (DPAs) with its vendors who process personal data relating to prospective and existing Pure customers in fulfillment of service contracts with such customers. Pure uses intra-company Standard Contractual Clauses to fulfill requirements for transfer of personal data from the European Economic Area (EEA) to the United States in accordance with the GDPR.

THE ROLE OF PURE1

Pure1 is a virtual private cloud (VPC) suite of applications and databases. It receives information from deployed Pure Storage hardware and cloud-based products. The application filters, analyzes, and stores the information, and in some cases, takes action based on it. Nearly all of the company's deployed systems, (except so-called dark sites barred from external connections by organization policy) utilize Pure1 services, which the company provides to its customers at no additional cost.

The information Pure1 receives includes capacity utilization, product performance, alerts and alert status, and records of administrative actions such as volume and file system creation, resizing, and destruction, host and client connections, etc. It uses this information to provide two primary services:

Pure1 Management Services

A web application accessed both by customers and Pure support engineers via browsers and a mobile application. Pure1 uses information uploaded by products to generate graphical displays of performance, utilization, and alert history for the products.

Users of Pure1 management services can initiate and manage support tickets, and employ built-in tools for analytics that include constructing "what if" scenarios, for example to evaluate the impact of adding workloads to a system, moving workloads between systems, and so forth.

Authorized Pure Storage and partner representatives can view information about any system that provides information to Pure1. Customers and partners can only view information about and perform operations related to their own organizations' products.

[3] Available from the knowledge base or from Pure Storage representatives. Appendix B contains a list of the URLs for related briefs. Some briefs require non-disclosure agreements.

Pure1 Support Services

The primary tool of the Pure Storage Support organization (Pure Support) for:

- Analyzing uploaded information to identify actual and potential issues with deployed products and initiate remediation. In a typical period, the support organization itself creates well over half of all support tickets.
- Continuously comparing deployed products' configurations and status to "fingerprints" of known product and environmental issues to identify and avert potential issues before they occur in deployed systems.
- Communicating with deployed products via the *RemoteAssist* capability that enables secure direct interaction between support engineers and deployed products that require software upgrades or other hands-on support services.

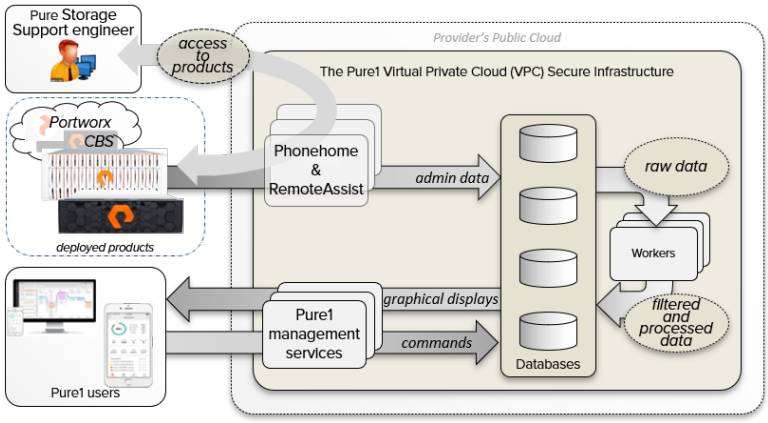

Figure 1: Pure1 Information Flows

Pure1 management services do not include mechanisms for accessing customers' stored data; all the information it collects and stores is administrative. Among that information is a limited amount of potentially personal data such as administrator userids (but not other credentials, which are stored only in the managed products), administrator and alert watcher contact information. Pure Support uses this information to assist with managing and upgrading the products and correcting faults when necessary, as specified in support contracts. Pure1 also stores technical information that identifies an organization's arrays, storage volumes, file systems, connected host and client computers by name, as well as capacity, utilization, and performance data. It is therefore imperative that communications with Pure1 and the data it stores be reliably available and protected against access by unauthorized parties.

This brief describes the mechanisms that Pure1 uses to secure communications between Pure Storage products and to protect the administrative data it stores and illustrates how those mechanisms can help organizations comply with the provisions of the GDPR.

PURE1 DATA SECURITY

Figure 1 illustrates the information flows between the Pure1 VPC, products that connect to it, users of Pure1 management services, and Pure Support engineers. Products upload administrative data to Pure1 via authenticated and encrypted channels called *Phonehome* that are dynamically established for each interaction.

Pure1 stores the information it receives within its VPC, both in raw form as objects and filtered and reformatted in databases for rapid response to users. Support engineers use the raw data for troubleshooting.

Phonehome is also the channel through which support engineers authenticate themselves and connect directly to deployed products for *RemoteAssist* sessions to deal with issues that require "hands-on" access. All RemoteAssist activity is controlled by administrators of the products, who can terminate sessions at any time.

User interactions with Pure1 management services take place over connections encrypted by HTTPS. To gain access, users who represent customer organizations authenticate themselves via the organization's own identity provider or, for organizations who choose not to use an identity provider, by a recognized provider with whom Pure has a standing relationship (at the time of publication, Salesforce.com). In both cases, Pure1 executes the authentication procedure specified by the customer. The customer is responsible for policies such as password strength, multi-factor authentication, and timely and secure authorization and deauthorization of users.

PURE1 AND THE GDPR

The information that Pure1 receives, processes, and stores is entirely about product operations and status. Pure1 has no access to *customer data*—data that users of the products store or process. Information flow is inbound; Pure1 stores and processes information received from the products. With the exception of support engineer RemoteAssist interactions, the application does not "push" information or commands to products.

The graphical displays of historical performance and utilization data that Pure1 management services produce for authorized users are based entirely on information received from the products and stored in databases in its VPC. There is no direct interaction between Pure1 management services analytics and the products.

INFORMATION IN PURE1 RELATED TO GDPR COMPLIANCE

The only data subjects for whom Pure1 processes and stores any potentially personal information are customer representatives who administer Pure Storage products that connect to the application. The information consists of (a) the identities by which administrators access products to perform their duties and (b) records of their interactions with the products. Products send both types of information to Pure1 in logs transmitted via the secure Phonehome channel.

In addition to this potentially personal information, logs sent to Pure1 identify products and their environments, such as volume and file system properties, host connections, network addresses, and so forth. These are not personal information per se, but if exposed to unauthorized parties, they could possibly abet attacks against products and data stored by them.

To guard against exposing this information to unauthorized parties:

- Products identify themselves uniquely to Pure1 before interacting with the system.
- Pure1 requires strong authentication of Pure1 Management services users and Pure Support engineers.
- All communications between products, Pure1, users, and support engineers are encrypted.

Identifying Products Uniquely

Each Pure Storage hardware product ships with pre-installed private keys. Manufacturing stores the corresponding public keys in the Pure1 VPC prior to shipment. During installation, products use this key pair and a pre-installed generic certificate to register with Pure1 and obtain a signed certificate that identifies them uniquely. Portworx products obtain their signed certificates during installation. Thereafter, every interaction between a product and Pure1 is authenticated by the *mutual TLS* (mTLS) protocol.

Securing Incoming Information

Pure1 uses TLS mutual authentication to ensure that all incoming connection requests emanate from registered products, and uses HTTPS to encrypt all information in transit. This minimizes the possibility of false information being injected into its databases.

Encrypting data in 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, connect products to unauthorized “rogue” servers, and so forth. Thus, any end-to-end encryption of data must be accompanied by policies that include interlocking safeguards against misappropriation and misuse by the data processor’s personnel.

User Access to Pure1 Management Services

A Pure1 database contains two objects for each Pure customer:

- An *organization object* that identifies the customer uniquely
- A *Pure1 administrative client* (**Pure1admin**) account for the customer.

The **Pure1admin** account is managed by the customer. It can be used to create, modify, and delete additional administrative accounts for the organization. During each product installation, Pure1 creates a database record linked to the product owner’s organization. It uses these records to determine the scope of each account’s access. Account users have access to Pure1 management services *on behalf of their organizations’ Pure Storage products only*

All user communications with Pure1 management services are encrypted by HTTPS.

Identity provider procedures executed by Pure1 management services ensure that only authorized users can access its services, and only for their organization's products. However, customers are responsible for managing their representatives' access:

- For ensuring that only individuals whose job functions require access are authorized to use the application
- For creating and deleting user accounts promptly as situations change
- For ensuring adherence to the organization's rules governing credentials
- For ensuring that individuals use the application for legitimate purposes.

Moreover, customers are responsible for the integrity of personal information stored by their identity management providers. The company does not make information stored by its provider available to any customer or partner.

Partner Access

The company extends Pure1 access to its Authorized Service Providers (ASPs). ASPs have access to Pure1 *for their customers' systems only*. Organizations that acquire products through non-ASP partners can create accounts to provide partner access to their products' information. Pure's partner and legal organizations vet all potential partners before granting status.

RemoteAssist Access

RemoteAssist sessions enable Pure Support engineers to access the administrative interfaces of deployed products directly for diagnosis, remediation, software installation, and other types of customer assistance. RemoteAssist is completely controlled by the customer. For an engineer to gain access, an administrator must enable the feature. The administrator can terminate a session at any time, and moreover, unless explicitly renewed, sessions terminate automatically after 48 hours.

Pure1 Information Retention

The potentially personal data that Pure1 collects and stores consists of product administrator account names (userids) and contact information (electronic mail addresses) for administrators and *alert watchers*—individuals designated to receive alerts from the products when exceptional conditions occur. Products record and upload all administrative actions along with the account names under which they were performed. Pure1 stores uploaded information, including records of administrative actions, for the legitimate business purposes of:

- Troubleshooting by support engineers
- Generating displays and analytics for users of Pure1 management services.

The company makes records of administrative actions on an organization's products available to the organization on request, for example for auditing.

Pure1 retains uploaded logs for approximately a year, after which it automatically deletes them. There is no other mechanism for deleting them, so records of actions taken by product administrators remain on file for about a year because they are required for the legitimate business purposes of producing security audit logs and fulfilling support contracts between Pure and its customers.

Administrative account names are ***potentially*** personal data because the extent to which they identify individuals is determined by customer organizations' policies rather than by Pure. For example, an administrator account name or email address of the form "first-name.last-name" would identify an individual as a product administrator or alert watcher and make it possible to track actions the individual took on the product, whereas a *pseudonymised*[4] account name or email alias like "portworx-admin-1" would provide a record of actions taken by an individual without identifying the individual. Securing the association of such pseudonymised names with individuals would be a customer responsibility. Pure does not require personally identifiable information from customers who use its identity provider.

[4] GDPR documentation uses the term *pseudonymisation* to mean the encoding of information that might identify an individual in such a way that the individual's identity is not discoverable from it.

THE BOTTOM LINE

- Since May 2018, for all practical purposes compliance with the European Union's General Data Protection Regulation is necessary for organizations that do business in the EU.
- The GDPR contains organizational, procedural, and digital data handling provisions. Pure Storage products and services, including Pure1, implement extensive features for keeping the data they store and process available to users and secure from unauthorized parties.
- Pure1 stores and processes administrative data about product utilization and performance; the application has no mechanisms for accessing users' data.
- The potentially personal data stored and processed by Pure1 consists of product administrator account names and email addresses of administrators and alert watchers. Administrator account names are associated with log records of actions taken on the products. According to customer policy, these may identify individuals (e.g., first-name.last-name), or they may be pseudonymised (e.g., admin01).
- The highly available Pure1 VPC helps satisfy GDPR requirements for keeping data available.
- All communication between products and Pure1, as well as RemoteAssist sessions between support engineers and the products uses the *Phonehome channel*—a dynamically established, mutually authenticated, and encrypted connection to prevent "snooping" and "man-in-the-middle" attacks.
- Each Pure customer has a **Pure1Admin** account through which they control their representatives' access to Pure1 management services. Pure1 uses either a customer's identity management provider or salesforce.com to authenticate users. Users only have access to information related to their organization's products.

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 for handling and protecting data while it is in digital form.

APPENDIX A: PURE1 AND GDPR COMPLIANCE

Table 1 lists excerpts from GDPR articles that relate to digital processing, storage, and transmission of personal data and describes the Pure1 capabilities that help users comply with them.

Table 1: GDPR Text Relationship to Pure1 Properties and Capabilities

Article	Excerpt from GDPR Text	Relationship to Pure1
3.1 3.3	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. 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.	Pure1 is implemented within a Virtual Private Cloud using the facilities of a recognized public cloud provider that operates worldwide, including in the European Union. Availability, data security, and access controls are the same regardless of the location of products that interact with Pure1. Thus, wherever a product is deployed, how its interactions with Pure1 help with GDPR compliance is as described in the body of this brief.
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;	Pure1 performs the highlighted operations on the data it collects (described in the body of this brief). Logs uploaded to the application by deployed products are retained for approximately a year and then destroyed.
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 Pure1 VPC implementation, including redundant virtual servers and databases provides state-of-the-art protection against accidental loss, destruction, or damage of data stored by the system.

Article	Excerpt from GDPR Text	Relationship to Pure1
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').	The body of this brief describes how end-to-end encryption of all interactions between deployed products and Pure1, as well as RemoteAssist sessions minimizes the possibility of data breaches. Authentication by recognized identity providers and audit logging minimize the possibility of data misappropriation.
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*.[5]	All log data stored by Pure1 is encrypted. The data is necessary for fulfilling support contracts with customers, which is compatible with the purpose for which the data is collected. Administrator account names and email addresses stored by Pure1 may constitute personal information in cases where customer policies do not require pseudonymisation. Logs of administrative actions that include actors' account names are viewable by product administrators and authorized users of Pure1 Manage.
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.	Customers may submit erasure requests via the Pure Privacy Statement portal. Pure1 does not publish any of the aforementioned administrative account information (which may identify individuals if customer policies do not prohibit it). Logs of administrative actions that include actors' account names are viewable by customer representatives, subject to non-disclosure agreements.

[5] GDPR documentation uses the term *pseudonymisation* to mean the encoding of information that might identify an individual in such a way that the individual's identity is not discoverable from it.

Article	Excerpt from GDPR Text	Relationship to Pure1
24.1 24.2	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. 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.	All log data stored by Pure1 is encrypted. The data is necessary for fulfilling support contracts with customers, which is compatible with the purpose for which the data is collected. The Pure1 VPC's high availability, administrative access control and auditing features provide tools to assist Pure customers acting as controllers and/or processors in complying with the data availability, security, and access control provisions of the regulation. Pure1 engineering implements all security-related best practices recommended by the vendor that hosts the Pure1 VPC. But a comprehensive program of GDPR compliance requires both protection of digital data and administrative procedures and workflows that regulate human access to and handling of data in all forms.

Article	Excerpt from GDPR Text	Relationship to Pure1
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.	Pure1's data security, high availability, control over administrative access, and auditing features mean that processors automatically "design in" protection for stored and processed digital data as they develop new applications. As processors implement new applications that utilize Pure Storage products and Pure1, their interactions with the latter automatically comply with the high availability, security, and access control provisions of the GDPR for digital data.
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.	Users of Pure Storage products administer their products, including managing administrative accounts and alert watcher email addresses. Similarly, each of the company's customers has a Pure1Admin account used to manage access to Pure1 management services. Pure1 does not have access to customer data stored on the company's products. Ensuring that customer representatives use the company's products and services properly is therefore the customer's responsibility.

Article	Excerpt from GDPR Text	Relationship to Pure1
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...*	The product logs sent to Pure1 record all administrative actions on the products, including volume and file system creation, resizing, and destruction, host connection and disconnection, and snapshot and replication schedule creation. On request, Pure will provide records of administrative actions on its products to customers, thereby assisting them in complying 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.	The Pure1 VPC's high availability, administrative access control and auditing features help customers who act as controllers and/or processors comply with the data availability, security, and access control provisions of the regulation. Pure1 does not publish any of the aforementioned administrative account data (which may identify individuals if customer policies do not preclude it). Pure will make logs of administrative actions on deployed products, including actors' account names, available to customers on request. The company regularly engages outside firms to perform penetration testing on both its products and the Pure1 VPC.

Article	Excerpt from GDPR Text	Relationship to Pure1
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." Pure regards the aforementioned encryption and access control features of Pure1 as "appropriate technical protection measures." As noted above, whether the administrative account information uploaded to and stored by Pure1 identifies individuals is determined by the customer's pseudonymisation policies for digital data.
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 field 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, as well as policies governing the manual acquisition and processing of personal data.

APPENDIX B: RELATED MATERIAL

Technical Brief TB-160201: Securing FlashArray® "Data At Rest"

https://support.purestorage.com/FlashArray/FlashArray_Security/FlashArray_Security_Reference/The_FlashArray_Data_Security_Model_TB-160201

Technical Brief TB-160202: FlashArray® Access Security

https://support.purestorage.com/FlashArray/FlashArray_Security/FlashArray_Security_Reference/Pure_Storage_FlashArray_Access_Security_TB-160202

Technical Brief TB-190701: FlashBlade® Security

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

Technical Brief TB-160501: Security in Pure1®

https://support.purestorage.com/Pure1/Pure1_Security/Pure1_Security_Reference/Pure1_Security%3A_Technical_Report_TB-160501

Technical Brief TB-171101: FlashArrays and GDPR Compliance

https://support.purestorage.com/FlashArray/PurityFA/FlashArray_Technical_Reports/FlashArray_Technical_Papers/FlashArrays_and_GDPR_Compliance_TB-171101

Technical Brief TB-180202: FlashBlade and GDPR Compliance

https://support.purestorage.com/FlashBlade/FlashBlade_Security/FlashBlade_Certifications_and_Compliance/FlashBlade_and_GDPR_Compliance_TB-180202