Pure Storage Technical and Security Measures Relating to Processing of Personal Data within Pure Support Systems

Pure Storage, Inc. and its subsidiaries (collectively “Pure”) are committed to protecting our customers’ personal data and providing a positive experience when using our products and services.

Pure have implemented a number of technical and security measures to ensure that the customer data in our support and maintenance systems is protected in accordance with industry standards and regulatory requirements.

This document details why Pure processes customer personal data and the technical and security measures that have been implemented.

For what purposes does Pure process customer personal data in its Support and Maintenance systems?

Pure maintains a Record of Processing Activities (ROPA) for all of the customer personal data it processes in its Support and Maintenance systems. The following summarizes the business purposes for processing the personal data:

Business Purpose	Description
Create customer contact	Either during customer onboarding, or during case work, Pure support agent may create or modify contact records in Support System, for the purpose of customer support. Includes adding new contacts to customer accounts upon request of account team and/or customer, Includes updating existing contacts with support-specific information (cc on all case, Main Support Contact, product responsibility, etc).
Pure1 Registration	Customers can register to the Pure1® cloud system, where they are granted access to Pure1 Knowledge and Pure1 Community (customer forums).
Pure1 Manage user account registration / enablement / modification	Customers who own a Pure array and want to be able to monitor and manage it via Pure1 may request access to Pure1 Manage.
Ongoing Pure1 Manage, Pure1 Knowledge, Pure1 Community Permission assignments	User permission assignments are modified as applicable. Includes granting additional access/permissions, removing access/permissions, troubleshooting user account issues if reported. As new roles/permissions are created in Knowledge and Community (e.g. a

	special section of KBs for a specific product, or a special forum for a particular customer type), existing customers are processed and updated with new permission sets. Users may also be deactivated, or have lesser permissions assigned as applicable (end of POC, customer request)
Support Case work	Contacts may be automatically or manually associated ('added') to cases based on the customer's request and per customer's support contract. This is true for all support case types, including both pro-active and customer-initiated cases
Incoming / Outgoing support calls	Customer calls support to open a ticket, check on an existing ticket OR Support calls customer upon request as per support contract with customer
Customer Contact Maintenance	Contacts that should no longer be associated with a particular customer account in Support System can be removed upon request
Customer signs up for training or access to specialized array administration information	Pure Service Support Training team will be informed and each user is enrolled in a course administered by Training Team
Field Engineer registration / training	Pure maintains a list of all Field Engineers qualified to deliver parts/services during RMA process. FEs are registered by their company directly via file upload. This data is loaded into Support System via SFTP file upload directly from the Partner. If an FE leaves the company or becomes inactive, the FE company is responsible for removing them from the FE list.
RMA / Parts Dispatch	Customer system component(s) needing replacement are dispatched to install site, addressed to site contact. 3rd party field engineer (contractors/partners), or employees may deliver and/or install replacement parts. All people are collected and listed or associated on the dispatch record.
Dispatch Process - Outbound Information	Dispatch communication including Customer & FE Name, Email, Phone, is shared with customers and the FE delivering parts (if applicable)

What Technical and Security Measures have Pure implemented in the Support and Maintenance Systems?

Pure have implemented a number of technical and security measures to protect customer personal data in accordance with industry standards:

Measure	**Description**
Physical Access Control	• *Controls implemented to stop unauthorized access to data processing systems* • *Surveillance systems employed to monitor access to data processing systems - Biometric access system in place at data center facilities* • *Policies defined regarding physical access control*
Logical Access Control	• *Data processing systems are accessed by means of authorization and authentication* • *Single-sign-on (SSO) employed* • *User ID and strong password policy assigned to authorized persons* • *Role-based access applied to authorized persons* • *Encryption of data storage devices applied whilst in transit* • *Firewall / antivirus software used and updated* • *Policies defined regarding logical access control*
Application Access Control	• *System-wide authentication of all users / devices* • *Role-based access implemented* • *Principle of least privilege to systems employed* • *Clear desk policy in place* • *Encryption of data storage devices applied whilst in transit* • *Firewall / antivirus software used and updated* • *Regular review of privileged accounts implemented*
Separation Control	• *Systems are multi-tenant capable* • *Systems are only accessed by authorized persons from secure network*
Encryption	• *Encryption implemented on all devices accessing the systems* • *TLS encryption implemented for data transfer* • *Platform level encryption used for Support system*
Transmission Control	• *Use TLS certificates for websites to transfer data within forms* • *Mobile device policy implemented* • *Disposal process for storage devices implemented in accordance with data protection regulations* • *Clear desk policy in place* • *Encryption of data storage devices applied whilst in transit*
Input Control	• *Access regulations / user authorizations implemented to enable the identification of all users and devices* • *Modern technologies employed for monitoring and logging controls*
Availability and Resilience	• *Personal data is stored in systems which are protected against hardware-related data loss* • *Personal data is stored in secure and redundant systems* • *Systems are equipped with hardware / software technology that enables defined data to be recovered from certain points of time* • *Regular backups are carried out in accordance with existing service*

	level agreements ● *Data is replicated between a minimum of two geographically dispersed data center facilities* ● *Systems are powered without interruption*
Privacy by Design and Default	● *Data protection is taken into account at the earliest opportunity to prevent unlawful processing / misuse of data* ● *Principles of data minimization and purpose limitation employed* ● *Transparency employed with regard to procedures and processing of data*
Other Data Privacy Measures	● *Pure has registered for EU-US Privacy certification, has received written confirmation that it is certified and is awaiting addition to the Privacy Shield List.* ● *Pure uses the industry-leading privacy management platform to maintain its compliance posture against data protection regulations such as the GDPR* ● *Data Protection / Privacy programs have been implemented to ensure that key staff that handle customer personal data are trained appropriately* ● *With regard to individual's right of access to personal data, Pure have clearly defined this process on this website: https://www.purestorage.com/privacy.html*