Panda Security

Compliance of Panda Products with General Data Protection Regulation (GDPR)

Contents

1.1. Scope of this document

Panda Security is fully committed to complying with the new General Data Protection Regulation (GDPR), which requires the company to protect the personal data obtained through the access, installation and use of the products included in its corporate solution portfolio: *Panda Adaptive Defense*, *Panda Adaptive Defense 360, Panda Endpoint Protection, Panda Endpoint Protection Plus, Panda Systems Management, Panda Email Protection, Panda Data Control, Panda Advanced Reporting Tool, and Panda SIEMFeeder*.

Through this document, Panda Security aims to inform of the exact purpose of storing customer personal data, as well as of the procedures in place to collect, process and use the information stored in its IT infrastructure.

1.2. General Data Protection Regulation: Objectives

In strict compliance with the European Union's General Data Protection Regulation, Panda Security guarantees and protects, with regard to the processing of personal data, the public liberties and fundamental rights of individuals, and in particular their honor and personal privacy.

In that regard, the security and management measures adopted by Panda Security for the processing of persona data satisfy the principles and obligations set out in the European Union's directives:

- **Quality principle**: Panda Security ensures that the personal data collected is only used for a specific, particular purpose, and that the amount of said data is proportionate to the aim pursued. No unnecessary data is collected or stored, and under no circumstances are user profiles generated. Customer data is collected solely and exclusively to ensure that the contracted products and services fulfill their protection and security objectives.
- **Transparency principle**: Customers are properly informed of the purpose for which their personal data is obtained and of the existence of procedures for processing it.
- **Consent principle**: The personal data is only processed after the data subject's acceptance of the relevant EULA, which authorizes Panda Security to use the collected information only for the purpose of providing the contracted service to customers.
- **Privacy and security principle**: Panda Security ensures that it puts in place industry-standard measures to control the proper storage, access and security of the stored data against unauthorized access.
- **Personal data transfer principle**: No data is transferred to any third party without the customer's prior and explicit consent.
- **Data breach notification and response principle**: Through the development of response plans, Panda Security implements detection, forensic analysis, erasure and resolution procedures against unauthorized data access and leakage.
- **GDPR rights compliance principle**: Panda Security complies with the data protection rights provided to customers in the GDPR (Access, Rectification, Cancellation and Opposition).

1.3. Stored data: Types and purpose

The data collected by Panda Security's corporate products falls into four categories based on its type and purpose:

- Customer contract information.
- Access credentials.

- Data collected by the products in order to provide the service.
- Data collected in order to run statistical analyses on product usage.

1.3.1 Customer contract information

This is the customer contract information entered by Panda Security's salespersons and partners in their management systems. It includes account IDs and the name of the company that the service is provided to. This information resides in a CRM/ERP system and is used to identify and find customers during internal management processes (billing, email campaigns, contract modification, etc.).

1.3.2 Access credentials

This information includes the email addresses used by customers to log in to the management consoles of their products. Its purpose is to protect against unauthorized access to the product, and to assign the appropriate access permissions based on the specific product and the user type.

The access credentials for the different consoles are centralized in a single standalone service. Panda Security only stores a non-reversible hash of each password, and it is the service that manages customer access authorizations.

1.3.3 Data collected by the products

This information includes all data collected as a result of the active monitoring and management operations performed by Panda Security's products on customers' devices: computer names, user names, public and private IP addresses, file paths, process paths, Active Directory paths, URLs, etc. For more information, refer to Table 1: Types of data collected by the Panda Adaptive Defense and Panda Adaptive Defense 360 monitoring tools, Table 2: Types of data collected by the Panda Data Control process monitoring tools and Table 3: Types of data collected by Panda Systems Management.

The purpose of collecting such data is to provide customers with the service contracted when purchasing the product. The customers' conformity to the collection of said data is ensured by their acceptance of the EULA displayed the first time that they access the management console of the relevant product.

The attributes of the personal data collected from customers' devices are sent using standard references instead of user-specific information. This prevents storing personally identifiable information of the logged-in user or specific file paths. Only the download URLs of executable files are collected. Under no circumstances are the URLs of the websites visited by users gathered.

All customer data collected by Panda Security's products is processed in accordance with the obligations set out in the GDPR.

1.3.4 Product usage statistical information

Panda Security collects data about the usage of its products' management consoles via Google Analytics. This information is used to generate statistical models and identify areas for improvement in the most commonly used product features. The collection of such statistical data is covered in the EULA governing the use of the contracted service.

1.4. Management and security of the stored data and processes

1.4.1 Where is the collected data stored and processed?

Panda Security uses two external service providers (Microsoft Azure Cloud Platform and Amazon Web Services - AWS) to store all data required to provide the services contracted by its customers. Both data centers, located in Ireland, host the infrastructure required for the data repository and the data-processing servers.

Data repositories

- Each server or service accesses the data repository using its own credentials. It is important to note that access is only permitted from a limited pool of IP addresses.
- All connections to the data repository are audited and encrypted.
- The stored data is pseudonymized before being processed by automated tasks.
- The system makes a backup copy of all stored data automatically every 5 minutes.

Server infrastructure

- Only remote connections from a restricted pool of IP addresses are permitted.
- All servers are kept constantly up to date with the latest security patches, without interrupting the service.
- All servers have the latest available version of the operating system installed.
- Each server is protected by a firewall system that limits the traffic sent and received to the minimum required to run the service. Plus, these firewalls protect the servers from network attacks such as DDoS attacks and others.

Both Microsoft Azure Cloud Platform and Amazon Web Services comply with the most important general application certifications (ISO 27001 and ISO 27018) on security management and personal data protection. Furthermore, they comply with the most important specific certifications for the financial (PCI DSS Level 1), health care (HIPAA BAA), and education (FERPA) sectors, among others, as well as general regulations mandatory in specific regions and countries (LOPD Data Protection Act in Spain, EU's GDPR, UK Government G-Cloud v6, etc.).

Panda Security sends the data collected from its European customers only to data centers located in the European Union, in order to comply with the EU data protection regulations and improve the service provided to its European customers. This is a differentiating factor compared to other vendors which store data in data centers located in the United States.

1.4.2 Data access procedures

- Access to the production environment is limited to the head of the IT Department area that manages the service (database, servers, applications and communications) and their deputy. The administration credentials used to access the servers are unknown and generated on access.
- All servers have their own set of credentials. The access credentials required to physically access the servers are different from those needed to access data stores.
- Access to all systems is audited and access is only possible from monitored locations.
- All communications with data storage systems are encrypted.

1.4.3 Data security

Security checks

- Panda Security performs continuous security test runs of all components involved in the operation of its products searching for vulnerabilities. These test runs also cover the software deployed across its customers' computers.
- The company's technicians check the code generated for each new version deployed in the production environment, looking for vulnerabilities that could be exploited by a third party.
- All vulnerabilities discovered internally are tested, fixed and published as soon as possible based on their severity. In addition to this, any vulnerability reported by a third party is also analyzed and assessed. Constant communication is maintained with the reporting agent in order to determine the vulnerability impact and severity, as well as notifying the release date of the relevant fix.

Management console access control

- Customers' credentials are stored using a standalone service whose only purpose is to guarantee security. All passwords are stored encrypted using non-reversible algorithms.
- Panda Security provides customers with two-factor authentication mechanisms for accessing the contracted products, as well as automated password reset procedures.

Communication security

- All data sent from customers' devices to Panda Security's platform is encrypted using strong algorithms and short-lived temporary tokens.
- All communications established between the protected devices and the management platforms are protected with standard protocols for device authentication. In addition to this, access from the protected devices to the management platform is protected using temporary encrypted tokens

1.4.4 Data modification and deletion

All data stored in our repositories is deleted after the termination of the contract signed between Panda Security and the customer. This information will be retained for 30 days to keep customers from having to go through the registration process again should the contract be renewed after the stipulated date of renewal.

Panda Security's systems are designed to accept any data modifications required by customers within that 30 day-period.

2.1. Data collected by the process monitoring tools

Attribute	Data	Description	Example
File	Hash	Hash value of the file that the event refers to	N/A
URL	URL	The URL from which the PE (Portable Executable) file was downloaded	http://www.malware.com/ executablefile.exe
Path	Path	Standardized path where the file that the event refers to is located	APPDATA\
Registry	Key/Value	Windows registry key and its associated content	HKEY_LOCAL_MACHINE\ SOFTWARE\Panda Security\Panda Research\Minerva\Version = 3.2.21
Operation	Operation ID	ID of the operation performed in the event (create/modify/load executable file, download executable file, communicate, etc.)	0-type events indicate the execution of a PE (Portable Executable) file
Communication	Protocol/ Port/ Direction	Communication event triggered by a process (not its content) along with its protocol and direction	Malware.exe sends data using UDP port 4865
Software	Installed software	List of all software installed on the workstation or server according to the Windows API	Office 2007, Firefox 25, IBM Client Access 1.0

Table 1: Types of data collected by the Panda Adaptive Defense and Panda Adaptive Defense 360 monitoring tools.

2.2. Data collected by Panda Data Control

Attribute	Data	Description	Example
Computer	Name/IP address	Workstation/server name and IP address.	WIN_MACHINE_1, 192.168.0.1
User	User name	User name of the process that operated on the file	DOMAIN\User
Document		File size, file name, file path, file hash value	Document path: SYSTEMDRIVE\Data\dlp
Operation		Operation performed on the PII (Personally Identifiable Information) file	Create: File created
Process		Information about the process that operated on the file: FatherHash, FatherPath, FatherCategory	FatherPath: WINDOWS | \Explorer.EXE

Attribute	Data	Description	Example
Drive		Drive where the PII file that was operated on resides	0: UNKNOWN 1: NO_ROOT_DIR: The path is invalid or does not exist 2: REMOVABLE: Portable device (external hard drive, card reader, USB device, etc.) 3: FIXED: Internal hard drive 4: REMOTE: Network drive 5: CDROM 6: RAMDISK
Number of PII file occurrences by type		Number of times different types of PII files have been found. Under no circumstances is personal information sent to Panda Security's cloud. The service only sends the number of times that each type of personal information has been found in a document	Number of credit card numbers, bank account numbers, identity card numbers, driving license numbers, passport numbers, social security card numbers, email addresses, tax ID numbers, IP addresses, first and last names, addresses, and telephone numbers.

Table 2: Types of data collected by the Panda Data Control process monitoring tools

2.3. Data collected by Panda Systems Management

By design and default, Panda Systems Management collects only limited amounts of personally identifiable information (PII). The types of PII collected are those that Panda Systems Management has determined to provide the services our customers have requested.

Attribute	Data	Description
Computer	Name/IP address	Workstation/server/tablet/mobile name and IP address.
User	Domain and user name	Domain and user name of the user logged
Hardware	Hardware information	Hardware information such as asset tag and date, serial number, OS, processor, memory, motherboard, BIOS, IP and MAC addresses, video, and physical disk drive size and free space. Hardware information is obtained for workstations, servers, mobiles and ESXi host devices
Software	Software information	Software information: software name, version and vendor Software information is obtained for workstations, servers, mobiles and ESXi host devices
Monitoring data	Monitoring data	Monitoring data such as log on times, IP address and files accessed

Table 3: Types of data collected by Panda Systems Management

Adaptive Defense

Adaptive Defense 360