Panorama9

P9 Dashboard
And
MSP Control Panel

Safety, Security & Personal Data Processing

Policies and Compliance

TABLE OF CONTENT

ABOUT THIS DOCUMENT

General Definitions

“**P9”** shall mean, Panorama9 Dashboard, the solution provided, covered by this document.

“**Panorama9**” shall mean, Panorama9 Inc., the company owning, developing, and issuer of “Right-to-use/Licenses” of the Panorama9 solution.

"**Customer Data**" shall mean the "personal data" that is processed through to the usage of the Panorama9 solution by the customer.

“**Hosting Provider**” shall mean the datacentre that Panorama9 utilize for its Panorama9 Dashboard.

“**Document Content Storage Agreement**” shall mean an optional add-on agreement for customers wishing to store Document Content beyond the standard default policy.

Panorama9 P9 Dashboard

Panorama9 is a subscription based true cloud-based IT management tool used by both MSPs (managed service providers) and IT administrators to gain full transparency, visibility and control of all endpoints – from servers, desktops, laptops, printers and switches to even Internet services such as websites and VPN connections. Gain a full overview of your network, improve uptime, keep your network secure and avoid things falling between the cracks.

- Discover all your machines, printers, switches, installed applications and more
- Monitor services are running and hardware is working problem-free around the clock
- Be the first to know when your IT environment encounters problems
- Use our patching solution to keep your applications up-to-date and secure
- Easily manage your machines with the built-in remote control feature

Purpose of this document

This document covers security and safety aspects in relationship to the usage of the P9 solution, including issues related to regulation and compliance. As with any other Software as a Service (SaaS) solution, there is no single layer that protects customer data, but rather a well-architected solution that considers every layer from the physical security measures at the data center, all the way through the access privileges that determine what data an individual user can access.

DATA AND USAGE

Data processing

Panorama9 will process data as described under *Type of data*. Panorama9 will not access or use Customer Data, except as necessary to provide the Service Offerings.

P9 Agent

The Panorama9 architecture allows users to leverage the power of the cloud without security headaches. We don't require users to setup and maintain dedicated servers that require patches and won't require working with ports in your firewall.

Panorama9 uses industry best practices to ensure data transmission is secure and that agents (the small application running on your machines) cannot be exploited by third parties. Our security protocols follow below:

- Agents use only HTTPS port 443 for data transmissions
- SSL connections use AES-256 bit encryption
- Each customer is issued a unique PKS certificate that can be revoked
- Agents are not able to view or collect sensitive data, such as passwords or documents
- Agents are designed to only execute tasks from a predefined whitelist
- Agents are automatically updated

Data storage

We are leveraging our Hosting Provider to host Panorama9 and store customer data. Our setup is fully redundant with fail-over servers, and data is replicated in order to secure continued service and prevention of data loss in case of disasters, etc.

- Data is stored in secure regional datacenters
- Datacenters are located in the US, Europe and Asia (your data stays within your region)
- Data can only be accessed by limited staff at Panorama9 and will never be shared with 3rd parties (read our privacy policy)
- High level of physical security in datacenters
- Sophisticated network security
- Ongoing penetration tests and 24/7 monitoring

Dashboard

P9's web interface - also known as “the dashboard” - is the final frontier in the data flow, and Panorama9 are applying industry best practices to maintain security. Panorama9 are continuously updating the software stack and have implemented various technologies to make sure that data stays secure.

- Full-session HTTPS encryption
- SSL with 256-bit encryption
- Passwords are guarded with multi-rounds of crypt hashing and salt
- Supports SAML 2.0 (for multi-factor authentication and user provisioning)
- Secured against XSS and other web-based attacks
- Automatic and manual vetting of the software stack, for security updates

Type of data

The P9 solution contains three (3) types of data, as described below.

Application Configuration Data

Application configuration data contains the customer specific configuration of the hosted solution. Data within this category is not classified as Customer Data and is not in violation with the ***General Data Protection Regulation - GDPR*** (EU)2016/679.

Hardware and software Metadata

Hardware Metadata contains information regarding hardware and software, which are specific information. Data within this category may be classified as Customer Data which may be covered by the ***General Data Protection Regulation - GDPR*** (EU)2016/679.

Document Content

Document content is the actual document content that any given end-user is processing through the P9 solution. This type of Customer Data may contain data which is covered by the ***General Data Protection Regulation - GDPR*** (EU)2016/679

Disclosure

Panorama9 will not disclose Customer Data to any government, except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends Panorama9 a demand for Customer Data, Panorama9 will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Panorama9 may provide Customer's basic contact information to the law enforcement agency. If compelled to disclosure Customer Data to a law enforcement agency, then Panorama9 will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Panorama9 is legally prohibited from doing so.

Panorama9 Personnel data access

Panorama9 restrict its personnel from accessing Customer Data without authorization by Panorama9 Management and without a reasonable cause. Panorama9 have established appropriate contractual obligations upon its personnel, regarding confidentiality, data protection and data security.

COMPLIANCE AND REGULATIONS

At Panorama9, our ambition is to follow industry leading compliance and regulations standards. Since the provided SaaS solution process customer data, including potential sensitive and critical customer data, compliance and regulation is critical to become accepted by our worldwide partners and end-customers. With the introduction of the General Data Protection Regulation by the European Union, a new standard has been established, which currently sets the highest ambition level among all other compliance and regulation policies worldwide. By following the GDPR (EU)2016/679 standard, the P9 solution will meet most of the worldwide requirements found within similar compliance and regulation standards.

General Data Protection Regulation - GDPR (EU)2016/679

Prior to establishing the initial P9 account setup, end-customers may determine whether the need for GDPR compliance is needed (location of servers within the EU). The following describes the policies used by Panorama9 to ensure a default configuration, which offers best possible performance for a wide range of our end-customers.

For EU Customers

Unless otherwise agreed between Panorama9 and the Customer prior to account setup, all processing and storage of Customer Data within the P9 solution will be handled according to and in compliance with the EU regulation (EU)2016/679 with the P9 solution hosted at servers within the EU. Customer can request to have its Hosting Provider location moved to a location outside the EU, by signing the “Panorama9 (EU)2016/679 Waiver or Option Agreement” provided by Panorama9 upon request.

For Non-EU Customers

For Non-EU Customer’s the P9 Hosting Provider location will as default be within Customers local geographical region (U.S or Asia/Australia).

Safety & Security Practices

To ensure GDPR compliance, Panorama9 maintains a number of internal procedures governed by the Data Protection Officer, including

- Management of events involving Customer Data
- Access logging
- Reviewing safety & security practices

INFRASTRUCTURE

All data as defined under Section ***Definition of data and usage*****,** will be managed within the P9 solution and temporarily stored within the Hosting Provider in use.

Hosting Provider compliance

The P9 solution is unless otherwise agreed, installed at a Hosting Provider that comply and are certified under key industry standards, such as ISO/IEC 27001:2005. Furthermore, all servers and network environment have the SSAE 16/ISAE 3402 attestation. In addition, the server platform complies with HIPAA Business Associate Agreement (BAA), a United States law which applies to healthcare entities with access to patient information (called Protected Health Information, or “PHI”).

Data Storage

Data Storage within the P9 solution will as default be managed through a Hosting Provider within Customers local geographical region (EU, U.S or Asia).

Customer may optionally specify any other geographic region(s) of the Hosting Provider in which Customer Data will be stored. At present, the available major regions are Europe (EU), Asia, and the United States.

Data Redundancy

P9’s hosting provider may transfer Customer Data within a major geographic region (e.g., within Europe, U.S. or Asia) for data redundancy or other purposes.

P9’s hosting provider will not transfer Customer Data outside the major geographic region(s) customer specifies (for example, from Europe to U.S. or from U.S. to Asia).

Data Retention

Document Content will only temporarily be stored until each job has been completed.

Data Disposal

When *Document Content* has been erased within the P9 solution, it will no longer be recoverable.

Backup and Recovery

Within the server side of the P9 solution, backup and recovery processes have been established to ensure high availability and a fault tolerant platform with zero point of failure. The P9 operations team have established monitoring tools and procedures which ensures full transparency and surveillance of the platforms operational status. In case of platform or software regression issues, a full disaster recovery procedure is established to ensure minimal platform down-time.

Application Configuration and Customization

The P9 solution can be customized and configured to support Customer chosen structures, which will allow Customer to meet Customer-specific compliance and regulation policies.

This includes configuration of specific and/or multiple locations for Data Storage and Data Processing.

APPLICATION SAFETY

Application resilience

Upon each release of new developments and application improvements, Panorama9 validates the P9 solutions vulnerability. These assessments have been deployed for vulnerability, configuration and compliance assessments and is based on widely known industry technologies, which helps prevent network attacks that can cause unwanted persons to penetrate the solution and its Customer Data. This validation includes all elements of the P9 solution.

To protect data between Customers and the P9 Hosting Provider, all data is transferred using Secure Sockets Layer (SSL)/Transport Layer Security (TLS), creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. All data in transit always encrypted via SSL/TLS.

INFRINGEMENTS POLICY

Panorama9 will immediately inform the Customer of any disruptions to the operation schedule that imply risks for the Client's data, and when suspicion arises concerning Customer Data protection infringements in connection with the Customer Data. The same will apply if Panorama9 discovers that the security measures it has introduced do not meet the applicable legal requirements.

Incident Notification

Actual, suspected, or potential breaches will be reported immediately to Panorama9's Data Protection Officer (DPO). In case of breach, the DPO shall notify the relevant Data Protection Authority, and the implicated end-customer(s) within 72 hours.

Depending on the size and seriousness of a data breach, the Office of the Data Protection Commissioner may conduct an investigation into the circumstances surrounding the breach. Investigations may include an examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident if end-customer has not already done so. Where necessary, the Office of the Data Protection Commissioner may use its enforcement powers to demand appropriate action from end-customer in order to protect the interests and rights of data subjects.

Data Loss Incident logging

All data breaches will be recorded in an incident log as required by the Office of the Data Protection Commissioner. The log will maintain a summary record of each incident which has given rise to a risk of unauthorized disclosure, loss, destruction, or alteration of personal data. The record will include a brief description of the nature of the incident and an explanation of why the Office of the Data Protection Commissioner was not informed. Such records will be provided to the Office of the Data Protection Commissioner upon request.

DISCLAIMERS

Force Majeure

Panorama9 shall not be liable for non-delivery due to force majeure, including but not limited to labour conflicts, blockade or lock-out, war, government intervention of any kind or other circumstances beyond the Panorama9's or its Hosting Providers control. Panorama9, or its Hosting Providers are in no way responsible for any damage, loss of profits, direct or indirect losses and damages by users or third parties.

Liability

In no event shall Panorama9 or its Hosting Providers be liable for direct, special, indirect, incidental, punitive or consequential damages (including, without limitation, damages resulting from loss of use, loss of data, loss of profits, loss of goodwill or loss of business) arising out of or in connection with the use of or inability to use the Software or Documentation furnished hereunder and any service supplied from time to time, even if its Hosting Providers have been advised of the possibility of such damages.