

Privacy Datasheet

Cloud NGFW for Azure

The purpose of this document is to provide customers of Palo Alto Networks with information needed to assess the impact of this service on their overall privacy posture by detailing how Personal Data is captured by the service and how the same data is processed and stored within the service.

Product Summary

Cloud NGFW by Palo Alto Networks is an Azure-native ISV Service. The ML-powered Next-Generation Firewall (NGFW) deployment model combines the power of the Palo Alto NGFW with the ease of use of Microsoft Azure to provide advanced application visibility and access control using Palo Alto Networks' App-ID and URL filtering technologies. Cloud NGFW provides threat prevention and detection through cloud-delivered security services and threat prevention signatures.

Personal Data Processed by Cloud NGFW for Azure

Cloud NGFW for Azure processes the personal data shown in Table 1.

- Cloud NGFW for Azure operates on and leverages PAN-OS; see the [PAN-OS Privacy Datasheet](#).
- As you request customer support for Cloud NGFW for Azure, the [Support Services, Customer Success, and Focused Services Privacy Data Sheet](#) provides more information on the personal data processed.

Table 1: Personal Data Processed by Cloud NGFW for Azure

Category of Personal Data	Type of Personal Data	Example(s)	Purpose of Processing
Contact information (customer administrator)	Name	John Smith	• Account creation • Billing and account management • Troubleshooting/support • Notification of updates
	Email address	jsmith@company.com	

Note: Palo Alto Networks does not intentionally process personal data via file(s) you submit to Cloud NGFW for Azure. However, unsolicited personal data may be contained in the files. Palo Alto Networks will not know the types of personal data collected at the moment the files are processed by Cloud NGFW for Azure.

Access by Customers

Customers can access Cloud NGFW Azure information via the Native Azure portal or through Panorama if you manage the firewall's policy using the Panorama interface. The customer's cloud portal admin or system admin can control access to Azure Portal or Panorama by granting appropriate access privileges

to authorized users. For licensing and operations purposes, the customer's system administrator must have an account on the Palo Alto Networks Customer Support Portal with appropriate access rights.

Access by Palo Alto Networks

Access by Palo Alto Networks to Personal Data is restricted to 1) Customer support teams, 2) Product development teams, and 3) Threat research analytics teams. All access privileges are managed by Palo Alto Networks engineering leadership and regularly audited for privilege access violations.

Processing Locations

Data Centers and Third-Party Service Providers

Table 2: Subprocessors in Cloud NGFW for Azure				
Subprocessor	Personal Data Processed	Service type	Location	
Microsoft Azure	Personal Data Identified in Table 1	PaaS	Australia Brazil Canada Hong Kong France Germany Japan	Norway Netherland Ireland Singapore Switzerland United Kingdom USA

Customer Support Locations

Customer support services for Cloud NGFW for Azure] will be provided globally. For more information on these locations, please refer to the [Support Services, Customer Success, and Focused Services Privacy Data Sheet](#).

Affiliates Processing Locations

Palo Alto Networks may process personal data in any of the locations of its subprocessor affiliates identified in its [List of Sub-processors](#).

Compliance with Privacy Regulations

Palo Alto Networks captures, processes, stores, and protects personal data in Cloud NGFW for Azure in accordance with the terms in (i) Palo Alto Networks [Privacy Policy](#), (ii) for our customers, the applicable [Data Protection Addendum](#), and (iii) this Privacy Datasheet. Visit our [Trust Center](#), the Palo Alto Networks one-stop-shop for everything privacy and security related where you will find numerous resources, including information on how our privacy practices comply with existing and applicable privacy legislations around the globe. For more information, please visit the [Privacy section](#) in the Trust Center.

Cross-Border Data Transfer

As part of provisioning the Cloud NGFW for Azure service and/or purchased support services, Palo Alto Networks may be required to transfer personal data to other countries outside the country/region where

the customer is located. To the extent that we need to transfer such data, we will comply with applicable requirements for the transfer of personal data, which include the [EU Standard Contractual Clauses](#), as approved by the European Commission and/or other legally binding instruments.

Data Subject Rights

Users whose personal data is processed by Cloud NGFW for Azure have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the service. Users can open a request via the Palo Alto Networks [Individual Rights Form](#).

Palo Alto Networks will confirm identification before responding to the request. Please note that if, for whatever reason, we cannot comply with the request, we will explain. For all users whose employer is a Palo Alto Networks customer, such users may be redirected to the relevant customer/employer for a response.

Data Portability

The cloud administrator of the Azure portal or the customer's system administrator can download the relevant reports from the portal directly as per their access privileges.

Retention and Deletion of Personal Data

On termination or expiration of your Cloud NGFW for Azure contract and upon your written request, Palo Alto Networks will delete the personal data from Table 1. Palo Alto Networks will delete such personal data in accordance with our contractual terms in place with you.

Security of Personal Data

Securing Personal Data

Palo Alto Networks supports a defense-in-depth security model to help protect the customer's data at all stages of its lifecycle, in transit, in memory, and at rest, as well as through key management.

- The [Trust 360 Program](#) details the corporate-wide security, compliance, and privacy controls in place to protect our customers' most sensitive data.
- Palo Alto Networks [Information Security Measures](#) document details the technical and organizational measures that will be implemented by us to secure systems, processes, and data. This document forms part of the Palo Alto Networks [Data Protection Addendum](#).

Resources

For more general information about Palo Alto Networks Privacy and Security Practices, please visit our [Trust Center](#).

About This Datasheet

The information provided with this paper that concerns technical or professional subject matter is for general awareness only, may be subject to change, and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws. Information concerning warranties and compliance with applicable laws may be found in [Palo Alto Networks End User License Agreement](#).

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2024 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks.
A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>.
All other marks mentioned herein may be trademarks of their respective companies.