VMware Horizon Cloud Service – next-gen

Privacy Datasheet

ABOUT VMWARE HORIZON CLOUD SERVICE – NEXT-GEN

VMware Horizon Cloud Service – next-gen provides desktop and app virtualization, which is a software technology that centrally hosts simulated desktops and applications in a data center or cloud, allowing users to access resources from a remotely connected device.

Learn more at: *https://www.vmware.com/products/desktop-virtualization.html*

ABOUT VMWARE'S PRIVACY PROGRAM

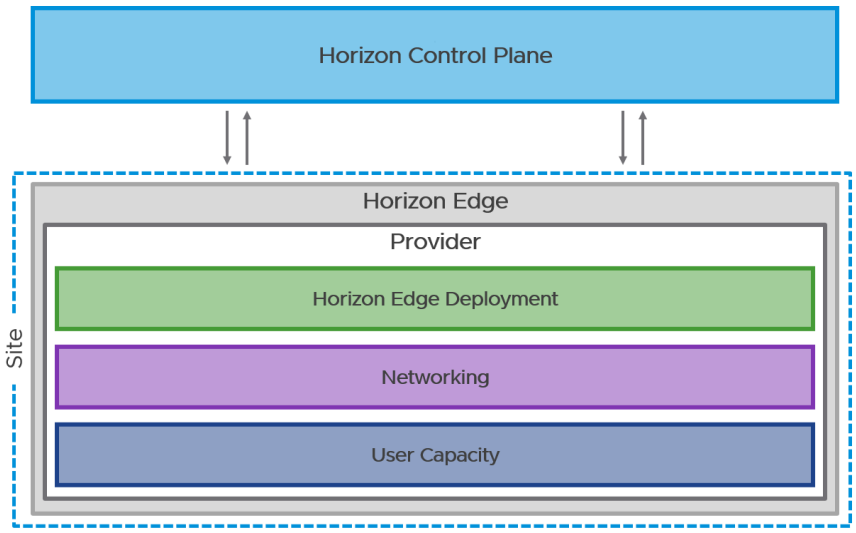
- Trust Center – At VMware, we want to bring transparency that underlies trust. *The VMware Trust Center* is the primary vehicle to bring you that information.
- Data Privacy Officer - Please contact VMware's Privacy Team at *privacy@vmware.com* or by mail at Office of the General Counsel of VMware, Inc., 3401 Hillview Ave, Palo Alto, California, 94304, USA.

How VMware brings value to you!

VMware Horizon® Cloud Service – next-gen is a new, desktop-as-a-service (DaaS) architecture that delivers a modern, cloud-native, hybrid and multi-cloud desktop and app virtualization platform built to support today's remote workforce.

The core elements of Horizon Cloud Service – next-gen include:

- Horizon Control Plane
- Horizon Edge
- Provider
- Horizon Edge Deployment
- Provider Networking
- User Capacity



For more information, see the *Horizon Service section of the VMware Cloud Services Guide*.

VMware and Privacy

In a complex world of data and the digital era our goal is simple: At VMware, you, our customers, and your data are our primary concern. VMware takes privacy and data protection very seriously and is committed to providing clear information about how we collect, use and process your personal data. We have established policies and practices designed to protect the personal data we process on behalf of our customers (as a processor), and as a controller. We are also committed to privacy-by-design when

developing products and services. VMware's Privacy Team actively works with the development teams to identify and embed privacy controls for customers.

The personal data collected and processed by VMware are largely dependent on the type of offering you purchase. This Privacy Datasheet provides you with information about how VMware processes and protects your personal data in connection with Horizon Cloud Service – next-gen.

Horizon Cloud Service – next-gen is comprised of various components such as those outlined in *Horizon Cloud Service – next-gen Architecture*

Location of Horizon Cloud Service – next-gen offering by component

Component	Regions	Purpose
Control Plane Instance	North Europe (Ireland) West US2: (Washington) Japan East: (Tokyo)	The Horizon Control Plane is a globally distributed cloud-based control plane that contains the containerized services that deliver Horizon Cloud Service – next-gen. It is used for all administrative functions and policy management and to provide user services. It provides access to Horizon Universal Console (Admin Console) and Universal Broker (End-User Brokering)
Control Plane Hub (CP HUB)	Australia East Japan East German West Central North Europe UK South East US2 West US2	Connection points that facilitate communication between the customer's Site and the Regional Control Plane Instance Horizon Agent connectivity and communication with the service
Edge Hub	North Europe (Ireland) West US2: (Washington) Japan East: (Tokyo)	Management of the Horizon Edge Gateways

Regional Data Shards	Australia East Japan East German West Central North Europe UK South West US2	Customer Data (such as PII) reside in Regional Data Shards to help achieve Data Sovereignty. Please review the table below for an overview of data collected by the service
Horizon Edge	The Edge location is determined by customers upon initial setup of the service.	A Horizon Edge is deployed into the customer's resource capacity in a specified primary provider in a selected site. It is based in a single physical location or region and can be divided into multiple blocks to provide scalability.
Horizon Pod	The Horizon Pod location is determined by customers upon initial setup of the service. In this type of deployment, Horizon Cloud Service – next-gen would leverage Pods instead of a thin edge architecture	Logical construct that defines a Horizon Cloud Service resource in the customers' on premise SDDC capacity. This component is used with Horizon 8

Although the Control Plane Instance resides in the Regions outlined above, the Control Plane communicates with the regional data shards via API for processing activities.

Communication Security

The Horizon Cloud Service – next-gen encrypts data in transit via TLS 1.2. The CPHub leverages MQTT protocol, which is encrypted by default, to establish a secure connection and communicate with the appropriate in-region data shards. The Horizon Cloud Service – next-gen leverages AES 256 to encrypt data at rest for those components managed by VMware.

Edge appliances such as the Edge Gateway and User Access Gateway encrypt communications via TLS 1.2 to help ensure secure connections. Customers maintain responsibility for how they configure their pools, including the level of encryption leveraged within their specific deployment.

Data Separation

The Horizon Control Plane contains a set of cloud management services referred to as Control Plane Services that provides customers with the ability to efficiently deploy, manage and scale their virtual desktop and application deployments.

Horizon Cloud Service – next-gen is a multi-tenant cloud service. The Horizon Control Plane Services is multi-tenant while the customer uses their own dedicated Provider (such as Microsoft Azure) to host their specific workloads

Within the Horizon Control Plane, customers are separated at the application layer. Additionally, each customer is encrypted with a per tenant key.

Types of Data Collected by Horizon Cloud Service – next-gen

VMware collects and further processes the following categories of data in connection with the delivery of the service. As noted above, CPHubs and Data Shards storing customer content remain in region.

The Control Plane Instance, which may reside outside of your home region (please see the table above for more detail) which is tied to your Horizon Cloud Service – next-gen deployment store the following information for the delivery of the service.

Please see the table below which outlines the information collected by the Horizon Cloud Service – next-gen.

VMware Data Classification	Description and Purpose of processing	Categories of Personal Data
Customer Content*	Content uploaded by customer or its users to the Cloud Service (as set forth in *VMware's General Terms*). To the extent the Cloud Service processes Customer Content, VMware processes such Content to provide the Service.	The Horizon Cloud control plane does not collect any customer workloads or other content from virtualized desktops or applications. The personal data processed will depend on the customer's specific configurations and deployment. Contact Information, such as end-user name (if the Service Offering is configured by customer to process such information). • Object GUIDs of users. These are their Active Directory object GUIDs.
Support Request Content	Content uploaded or otherwise provided by customer to VMware to address a technical support issue (a "Support Service" under *VMware's General Terms*).	Any personal data customer shares with VMware in connection with a support request (as controlled and determined by Customer).
Account Data	Data collected and used by VMware to manage the customer account and maintain the relationship with customer, such as to bill the customer or deliver notifications and alerts.	Contact Information, such as customer name, email address, address and phone number. Online Identifiers such as customer's IP address, login credentials or Object GUIDs of users.

Service Operations Data	Data used by VMware to facilitate the delivery of the Cloud Service. This may include (i) tracking entitlements, (ii) providing support, (iii) monitoring the performance, integrity, and stability of the Service's infrastructure, and (iv) preventing or addressing Service or technical issues. For example: • Configuration, usage and performance data • Authentication Data • Service logs, security logs, and diagnostic data	Contact Information, such as administrators' name and email address. Online Identifiers such as administrators', developers' or users' IP address, login credentials or login time stamps. Online Information: • IP/MAC Address of customer systems • IP/MAC Address of end-user desktops and devices • Device Information including unique identifiers, device type, carrier, operating system, model, system, etc. • Unique identifier(s) Configuration data of end user devices or desktops (e.g. fonts, apps used, etc.) Credential Storage, Username and Password information may be stored for the following use cases, please note, we do not store Passwords for your AD users. • Images • Horizon Availability Monitoring • Connection Server service account • AD Bind and Domain join service accounts Location Data such as Geo-location information (reverse IP look-up, GPS coordinates, Wi-Fi) of customer systems; Geo-Location Information (reverse IP look-up, GPS coordinates, Wi-Fi, cell ID) of end-user desktops and devices; Location of Edges that will be communicating with the service • Configuration, usage and performance data • Authentication Data • Service logs, security logs, and diagnostic data • Survey and feedback data

SECURITY, CERTIFICATIONS AND THIRD-PARTY ATTESTATIONS

- All compliance certifications are available in the *VMware Trust Center's Compliance Page.*

Service Usage Data	Information used by VMware for analytics, product improvement purposes, and proactive support. See *VMware Trust & Assurance Center* for additional details regarding VMware's Service Usage Data Program (SUDP). For example: • Configuration, usage and performance data • Survey and feedback data	Online Information, IP/MAC address of customer systems (not individual end-user desktops or devices but from servers located, for example in data centers) Online Behavior Data such as browsing behavior of Administrators within the Horizon Universal Console.

Ancillary Services		
Intelligence for Horizon	Certain data collection is configured upon initial setup while others are configured by customer administrators through the use of the service.	The Dashboards enabled by default collect the following data elements: • Pool Information • Performance Details • User Entitlement information This component may be disabled if customers are only leveraging Horizon 8. This is not part of the Horizon Plus suite of offerings

Content submitted by Customer to the Service Offering (described as "Customer Content" in *VMware's General Terms).* Customer is responsible for determining which types of personal data (if any) it includes in workloads submitted to the Service Offering.

How We Process and Protect Data as a Controller

To the extent VMware acts as the Controller, the following privacy notices explain how VMware collects, uses and protects any personal data included in the above categories of data:

VMware Privacy Notice: This notice addresses the personal data we collect when you purchase VMware products and services and provide account-related personal data.

VMware Products and Services Privacy Notice: This notice applies only to the limited personal data we collect and use for our own purposes in connection with our provision of VMware products and services, including (i) any cookies and similar tracking technologies we may use when providing the products or services; (ii) any information we use to facilitate the delivery of VMware services; and (iii) any data we collect to improve our products and services and our customer's experience.

DATA PRIVACY REQUESTS

If you wish to exercise any of your rights under applicable data privacy laws for personal data processed by your organization while using the Service Offering, please contact your organization. See *VMware's Privacy Notice* for information about how to exercise your rights where VMware is processing personal data in connection with its business operations.

FOR MORE INFORMATION OR TO PURCHASE VMWARE PRODUCTS

Contact your VMware account representative or call 877-4-VMWARE (outside North America, +1-650-427-5000), visit *vmware.com/products*, or search online for an authorized reseller.

UPDATES

Reading from a PDF? Don't be outdated, be informed! Find the latest information in the current version of this document from the *VMware Trust Center's Privacy Page*.

How We Process and Protect Data as a Processor

In connection with the provisioning of the Service Offering, VMware will process personal data contained in Customer Content on behalf of the Customer. With respect to personal data included in Customer Content, VMware is acting as a "processor" (acts on the instruction of the controller), while the Customer has the role of the "controller" (determines the purposes of the processing).

Data Protection Addendum

VMware's obligations and commitments as a data processor are set forth in VMware's *Data Processing Addendum* ("DPA"). VMware will process personal data contained within Customer Content in accordance with the DPA and VMware General Terms available *here*.

Data Storage and Cross-Border Data Transfers

Horizon Service may currently store data processed by the Control Plane Instance in the in the United States of America, Ireland, and Japan. Hosting location options may be added from time to time so please visit the *Sub-Processors list* for up-to-date primary and disaster recovery location details.

For cross-border personal data transfers from the EEA, Switzerland and the UK, VMware relies on Binding Corporate Rules ("BCR") as a processor. You can view VMware's BCR's in the *VMware Trust Center*.

Sharing with Sub-Processors

For the Service Offering, VMware utilizes third-party companies to provide certain services on its behalf. As set forth in the *Data Processing Addendum*, VMware has agreements and data transfer mechanisms in place with each sub-processor. A list of these sub-processors is available *here*.

Additional sub-processors providing supporting functionality for the Service Offering is available in the *Support Services Sub-Processer List*.

VMware also provides customers with an easy mechanism to monitor changes to our list of sub-processors. If you would like to receive notifications, you can subscribe through the *Sub-processor page on VMware ONE Contract Center*.

Data Retention and Deletion Practices

VMware retains personal data collected in connection with the customer's use of the Cloud Service for as long as it is needed to fulfill the obligations of the VMware General Terms.

The *VMware Data Processing Addendum* and *Services Guide* set forth how personal data contained in Customer Content is deleted after contract expiration or termination. Customer Content will be deleted within 90 days from customer's deletion request. VMware advises you to retrieve any data you wish to retain before the account termination takes place. VMware has no obligation to retain data beyond 30 days of the effective termination date.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.