VMware Cloud Disaster Recovery Privacy Datasheet

ABOUT VMWARE CLOUD DISASTER RECOVERY

VMware Cloud Disaster Recovery™ offers on-demand disaster recovery to IT administrators who are responsible for IT infrastructure and resiliency, and who face the challenge of dealing with complex, expensive and unreliable data recovery products. It helps security and compliance teams ensure operations can resume after a disaster event.

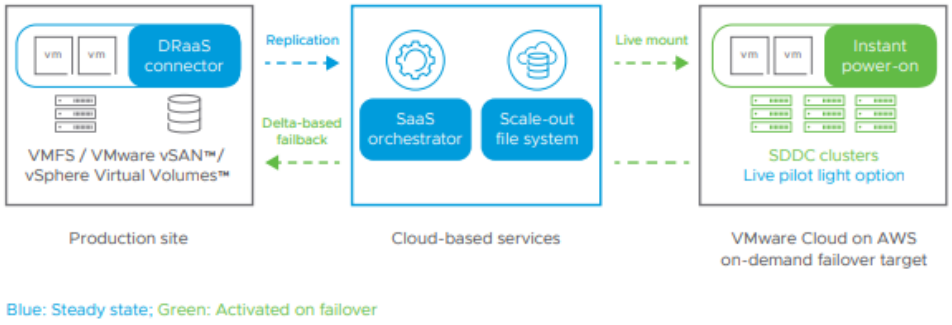
Learn more at: https://cloud.vmware.com/cloud-disaster-recovery

ABOUT VMWARE'S PRIVACY PROGRAM

- Cloud Trust Center – At VMware, we want to bring transparency that underlies trust. *The VMware Cloud 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 Cloud Disaster Recovery brings value to you!

VMware Cloud Disaster Recovery™ (the "Service Offering") can be used to protect your VMware vSphere® virtual machines by replicating them periodically to the cloud and recovering them as needed to a target VMware Cloud™ on AWS software defined data center ("SDDC"). The target SDDC can be created immediately prior to performing a recovery and will store the replicas/snapshots of the in-scope VMware vSphere® virtual machines. The Service Offering will also process customer's disaster recovery plans (e.g., failover rules) and plan names, including the names of the virtual machines, host IP address, and protection group (PG) names (i.e. group of one or more virtual machines that are handled in the same way).



For more information, see the VMware Cloud Disaster Recovery Service Description.

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 designing our products and services and VMware's Privacy Team 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 the VMware Cloud Disaster Recovery Service Offering.

SECURITY, CERTIFICATIONS AND THIRD-PARTY ATTESTATIONS

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

Types of Personal Data Collected by VMware Cloud Disaster Recovery

VMware collects and processes the following categories and types of personal data in connection with the provision of the Service Offering to the Customer.

Personal Data Category	Personal Data Attributes	Purpose of Processing
Contact Information	Administrators' Name Administrators' Email address	Access and authentication. Service functionality such as role-based access controls, alerting (including email notifications), user identification and auditing.
Online Identifiers	Administrators' IP address	Access and authentication. Service functionality such as role-based access controls, alerting and user identification.
Replicas/Snapshots of your Virtual Machine	VMware has no visibility into the content of your Virtual Machines	To store and make such replicas/snapshots available for disaster recovery purposes. Note: Replicas/Snapshots of your virtual machines are stored in the VMware Cloud™ on AWS offering (see *VMware Cloud on AWS Data Sheet*)

Personal data other than listed above may also be included in any content that the customer submits to the Service Offering. VMware may not know what types of personal data the Customer submits to the Service Offering and the customer is responsible for understanding the types of personal data processed in connection with the customer's use of the Service Offering.

How We Protect Data Processed in Connection with the Operation of Our Business (as a Controller)

In connection with VMware's provision of the Service Offering to the Customer, VMware collects and further processes the types of data shown in the below table related to the Service Offering, which may include personal data. In this instance, VMware is acting as a "controller" and determines the purposes of the processing.

Data Category	Purposes for which it is used
Relationship Data • Customer account information (including contact information)	Information used in connection with the provision of the Service Offering, such as managing the account and maintaining the relationship with the customer.
Service Operations Data • Configuration, usage and performance data • Authentication Data • Service logs, security logs, and diagnostic data	Information used to facilitate the delivery of the Service Offering, including maintaining, managing, monitoring and securing the infrastructure.
Service Usage Data • Configuration, usage and performance data.	Information used by VMware for analytics and product improvement purposes. See *VMware Trust & Assurance Center* for additional details regarding VMware's customer experience improvement programs.

The following privacy notices explain the different ways in which 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, such as your email address.

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 products and services; and (iii) any data we collect to improve our products and services and our customer's experience.

How We Protect Data as a Service Provider (as a Processor)

In connection with the provisioning of the Service Offering, VMware will process personal data contained in Your Content (as such term is defined in the relevant VMware agreement, e.g. *VMware Terms of Service* on behalf of the Customer. In this instance, 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 Your Content in accordance with the applicable agreement and the DPA. The applicable agreements for each product and service, including the VMware Terms of Service, the Service Descriptions for VMware Cloud Disaster Recovery, and other relevant legal documents can be found *here [https://www.vmware.com/download/eula.html]*.

Data Storage and Cross-Border Data Transfers

VMware Cloud Disaster Recovery currently stores Your Content in the VMware Cloud™ on AWS offering hosted in the United States, Australia, United Kingdom, Canada, India, Singapore, France, Canada, Japan, South Korea, Sweden, Brazil, Italy and Germany. Hosting location options are constantly evolving so please visit the *Sub-Processors list* for up-to-date primary and disaster recovery location details.

For cross-border personal data transfers, VMware has achieved Binding Corporate Rules ("BCR") as a processor, thus acknowledging we have met the standards of the EU General Data Protection Regulation for international transfers of personal data it processes on behalf of our customers. View the VMware BCR or the EU Commission BCR Listing in the *VMware Cloud Trust Center*.

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 Cloud Trust Center's Privacy Page*.

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*

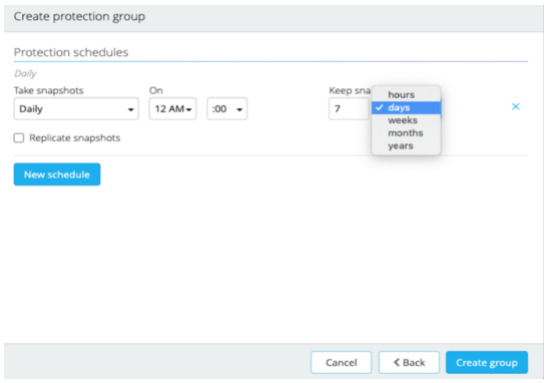
Additional sub-processors providing supporting functionality for the Service Offering is available in the *Support Services Sub-Processer List*.

VMware also provides customers with an easy mechanism to monitor changes to our list of sub-processors. If you would like to receive notifications, please visit this page *here*

Data Retention and Deletion Practices

VMware retains personal data that we may collect in connection with the customer's use of the Service Offering for as long as it is needed to fulfill the obligations of the VMware Terms of Service. The *VMware Data Processing Addendum*, and the *VMware Cloud Disaster Recovery Service Description* set forth how Customer Content, including any personal data contained in Customer Content, is deleted after contract expiration or termination.

During the subscription term, using the configuration feature shown below, you can select the applicable frequency (i.e. how often is a snapshot taken) and retention (i.e., how long is a snapshot retained) of the snapshots grouped under the same "protection group" transmitted to VMware Cloud Disaster Recovery. The frequency default is set to 'every four hours' and the retention default is set to '4 days.'



Following termination or expiration of your service agreement, Your Content (i.e. virtual machine snapshots) stored within the Service Offering will be permanently deleted as further described in the *Service Description*

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