VMware Cloud on AWS – Privacy Datasheet

ABOUT VMWARE CLOUD ON AWS

VMware Cloud on AWS delivers a seamless hybrid cloud by extending your on-premises Software-Defined Data Center to the public cloud. This enables you to manage your entire app portfolio across hybrid and native public clouds. Find more details at *https://cloud.vmware.com/vmc-aws/get-started.*

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 on AWS brings value to you!

VMware Cloud™ on AWS ("VMC on AWS" or "the Service Offering") brings VMware's enterprise-class SDDC offering to the AWS Cloud with optimized access to AWS services. Powered by VMware Cloud Foundation, VMware Cloud on AWS integrates our compute, storage and network virtualization products (VMware vSphere®, vSAN™ and NSX®) along with VMware vCenter management, optimized to run on dedicated, elastic, bare-metal AWS infrastructure. .

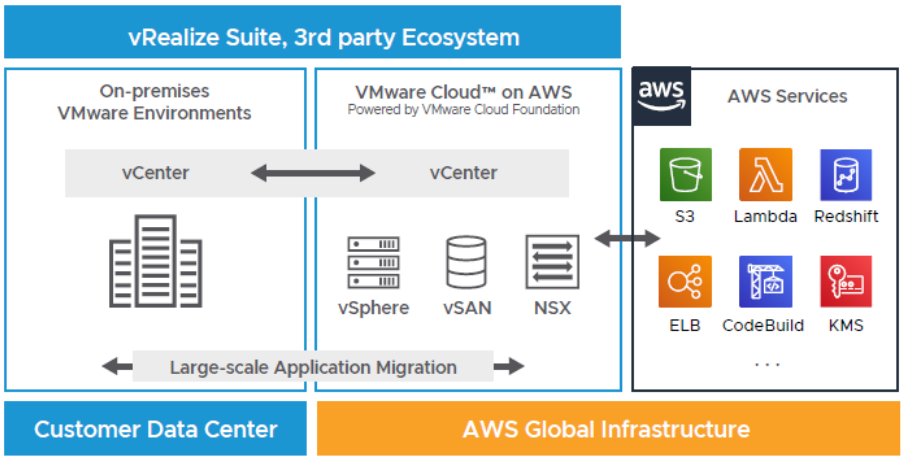

FIGURE 1: VMware Cloud on AWS Solution Architecture and Ecosystem.

For more information, see the *VMC on AWS 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 VMC on AWS.

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 VMC on AWS

VMware only collects and further 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
Identity Details	First Name, Last Name, and Email address of customer's IT administrator(s)	Service functionality such as role-based access controls, alerting and user identification. Note that VMC on AWS allows customers to anonymize the identity details of customers' IT administrators (Names and email addresses). For example, instead of using real names, customers can use alias such as ADMIN1, ADMIN2 etc.
Online Identifiers	IP addresses of customer's IT administrator(s)	Service functionality such as role-based access controls, alerting and user identification.

Personal data other than those listed above may also be included in any content that the customer submits to the Service Offering (i.e., "Customer Content"). VMware may not know what types of personal data are submitted to the Service Offering by the customer 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, which may include personal data. In this instance, VMware is acting as a "controller" in relation to such personal data and determines the purposes of the processing.

Data Category	Purposes for which it is used
Relationship Data – Authentication and customer account information	Used to provision the Service Offering, such as managing the account and maintaining relationship data.
Service Operations Data – Configuration Data, Feature Usage Data, Authentication Data, Performance Data, Service Logs, Memory Dumps, Security Logs, Diagnostic Data, Support and Survey Data.	Information used to facilitate the delivery of the Service Offering, including managing and monitoring the infrastructure, and providing support. See *VMware Products and Services Privacy Notice* for details.
Service Usage Data – Configuration Data, Feature Usage Data, Performance Data.	Information used for VMware's own analytics and product improvement purposes See *VMware Service Usage Data Program disclosure* for details.

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*.

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.

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.

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 Customer 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 Customer 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 each specific service, and other relevant legal document can be found *here*.

Data Storage and Cross-Border Data Transfers

VMware Cloud on AWS stores Customer Content inside of a geographic region chosen by the customer when they deploy a Software Defined Datacenter (SDDC). Hosting location options are constantly evolving so please visit the *Sub-Processors Addendum* or *https://cloud.vmware.com/vmc-aws* for up-to-date primary and disaster recovery location details. These locations include North America, Europe and Asia. Customer Content will not be relocated, replicated, archived, or copied without the explicit request or actions of the customer administrator.

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*.

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 at the *VMware End User Terms and Conditions page*.

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

Retention and storage policies associated with Customer Content (including any personal data stored within Customer Content) are solely managed by the Customer. VMware does not back up Customer Content and therefore will not be able to recover any personal data in any unforeseen event.

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*, the *Terms of Service,* and the relevant *Service Description* set forth how personal data contained in Customer Content is deleted after contract expiration or termination. The personal data collected as part of SDDC audit logs are retained for three (3) years and log events that exceed the three (3) year life cycle are automatically purged.

Security

VMware has implemented a wide range of security controls to protect our Customers' SDDCs. VMware maintains technical and organizational measures to protect against data breaches and to preserve the security and confidentiality of data processed by VMware on behalf of the Customer in the provision of the services. Controls are provided to enable the customer to configure the service in a manner compliant with its own security policies and practices.

VMC on AWS undergoes independent third-party audits on a regular basis to provide assurance to our Customers that VMware has implemented industry leading practices and controls. VMware Cloud on AWS has been audited for key industry certifications including ISO 27001, ISO 27017, ISO 27018 and SOC2. You can view existing compliance and certifications for VMC on AWS at *https://cloud.vmware.com/trust-center/compliance*.

Shared Responsibility Model

VMware Cloud on AWS Software-Defined Data Centers (SDDCs) provide a private environment for workloads underpinned by a shared accountability model where security and compliance responsibilities are shared between Amazon Web Services (AWS), VMware, and the Customer.

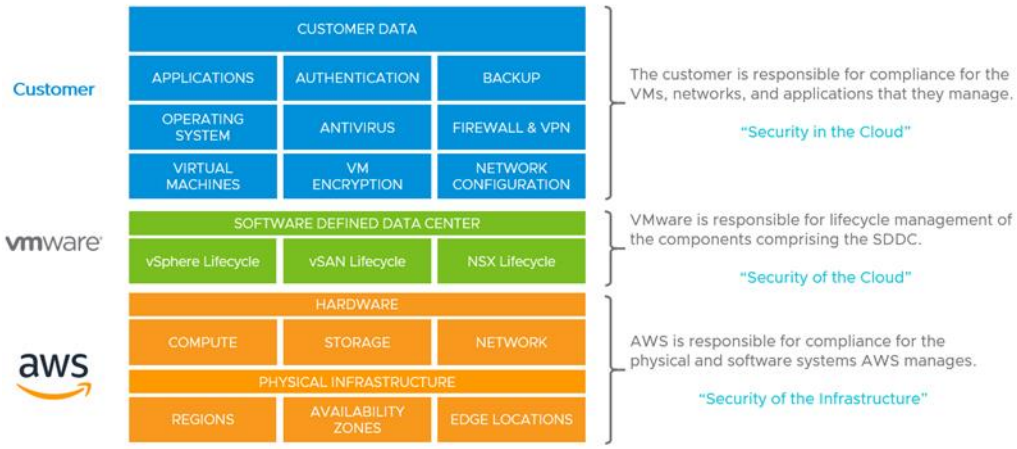

Figure 2: Shared Responsibility Model

Access Controls

Access to Customer Content is governed by Customer's use of authentication and authorization mechanisms to Virtual Machines (VMs) and filesystems that hold the VMs' data. Neither VMware nor Amazon Web Services (AWS) require any user accounts that would provide access to any Customer Content. The separation of Customer Content from VMC Operations is shown below:

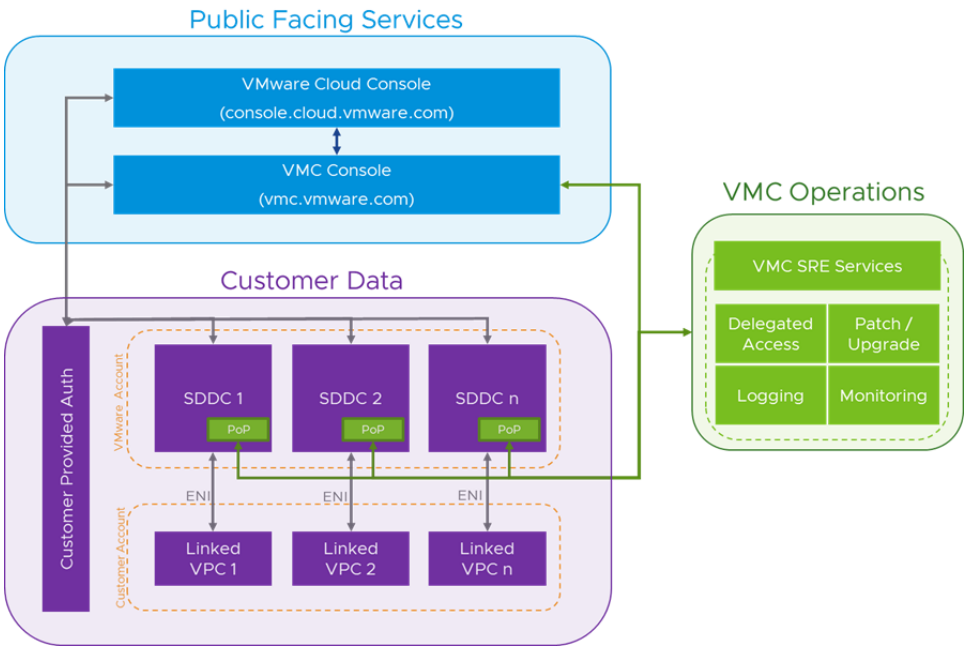

Figure 3: Separation of Customer Content

VMware will not access or use Customer Content except as necessary to maintain or provide support for the Service Offerings as provided in the Agreement.

To provide support to the VMware Cloud on AWS platform, VMware has implemented a tightly controlled "Delegated Access" process. This process enables only VMware Support personnel with the appropriate permissions to authenticate (using MFA) to a VMware operated system to generate one-time use certificates and credentials that are support user-specific with limited time-bound access to a specific customer environment.

VMware employees sign confidentiality agreements, receive regular training on security, and are required to follow code of conduct and data handling policies.

For further details on VMware Cloud on AWS security, please see our security whitepaper at *VMware Cloud Services Security Overview*