Commvault

Technical and Organisational Measures

(including technical and organisational measures to ensure the security of the data)

Commvault has implemented and maintains a security program that leverages a combination of the ISO/IEC 27000-series of control standards, NIST 800-30/CSF, and Information Security Forum ISF best practices.

As for provision of the SaaS Solution, Commvault is leveraging Microsoft Azure and/or Oracle Cloud Infrastructure, certain technical and organizational measures are inherited from that offering.

For Technical and Organizational Measures applicable to Microsoft Azure (sub-processor) please refer to applicable terms and documentation here:

https://www.microsoft.com/en-us/trust-center/privacy

For Technical and Organizational Measures applicable to Oracle Cloud Infrastructure (sub-processor) please refer to applicable terms and documentation here:

https://www.oracle.com/pl/corporate/contracts/cloud-services/contracts.html

For Technical and Organizational Measures applicable to AWS (sub-processor) please refer to applicable terms and documentation here:

https://aws.amazon.com/compliance/data-privacy/

Measures for Ensuring Physical Security of Locations at Which Personal Data are Processed

Web applications, communications, and database servers of Commvault are located in secure data centers. Commvault has implemented suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment. This is accomplished by:

- Establishing security areas;
- Securing the data processing equipment and personal computers;
- Establishing access authorizations for employees and third parties, including the respective documentation;
- Regulations/restrictions on card-keys;
- Restricting physical access to the servers by using electronically-locked doors and separate cages within facilities (e.g., production and development);
- Access to the data center is logged, monitored, and tracked via electronic and CCTV video surveillance by personnel; and
- Data centers are protected by security alarm systems, and other appropriate security measures, such as user-related authentication procedures, including biometric authentication in some instances, and/or electronic access cards.

Measures for Ensuring Ongoing Confidentiality, Integrity, Availability and Resilience of Processing Systems and Services

Commvault has implemented suitable measures to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services. This is accomplished by:

- Utilizing firewall, router and VPN-based access controls to protect the private service networks and back-end-servers;
- Continuously monitoring infrastructure security;
- Regularly examining security risks by internal employees and third party auditors;
- Role-based access control implemented in a manner consistent with principle of least privilege;
- Remote access to Commvault's network infrastructure is secured using various two-factor authentication tokens, or multi-factor authentication.
- Access to host servers, applications, databases, routers, switches, etc., is logged;
- Access and account management requests must be submitted through internal approval systems;
- Access must be approved by an appropriate approving authority. In most cases, the approval for a request requires two approvals at minimum: the employee's manager and the role approver or "owner" for the particular system or internal application;
- Passwords must adhere to the Commvault password policy, which includes minimum length requirements, enforcing complexity and set periodic resets;
- Password resets are handled via Commvault ticketing system. New or reset passwords are sent to the employee using internal secure, encrypted email system or by leaving a voicemail for the employee;
- Commvault's intrusion detection systems include signature-based network IDS, host-based IDS, and security incident and event management (SIEM) systems. Commvault also uses commercial and custom tools to collect and examine its application and system logs for anomalies; and
- The SaaS Solution is developed leveraging solution architecture ensuring confidentiality, integrity, availability, and resilience.

Measures for User Identification and Authorization

Persons entitled to use the systems are only able to access data within the scope and to the extent covered by their respective access permission (authorization). This is accomplished by:

- Employee policies and training;
- Users have unique log in credentials – role-based access control systems are used to restrict access to particular functions;
- Monitoring activities;
- Effective and measured disciplinary actions;
- Controlling access in compliance with the security principle of "least privilege";
- Internal segmentation and logical isolation of Commvault's employees to enforce least privilege access policies;
- Regular review of accounts and privileges (typically every 12 months depending on the particular system and sensitivity of data it provides access to);
- Control of files, controlled and documented destruction of data; and policies controlling the retention of back-up copies

Measures for Ensuring the Ability to Restore the Availability and Access to Personal Data in a Timely Manner in the Event of a Physical or Technical Incident

Commvault has implemented suitable measures to ensure that data is protected from accidental destruction or loss. This is accomplished by:

- Commvault has implemented a Business Continuity and Disaster Recovery plan, which is subject to periodical testing;
- Global and redundant infrastructure that is set up with disaster recovery;
- Constantly evaluating data centers and Internet service providers (ISPs) to optimize performance for its customers in regard to bandwidth, latency and disaster recovery isolation;
- Situating data centers in secure co-location facilities that are ISP carrier neutral and provide physical security, redundant power, and infrastructure redundancy;
- Service level agreements from ISPs to ensure a high level of uptime;
- Rapid failover capability; and
- Commvault maintains full capacity disaster recovery (DR) sites and tests its DR centers.

Measures of Pseudonymization and Encryption of Personal Data

Commvault has implemented suitable measures to prevent Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:

- Use of adequate firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
- Sensitive Personal Data is encrypted during transmission using up to date versions of TLS or other security protocols using strong encryption algorithms and keys;
- Protecting web-based access to account management interfaces by employees through encrypted TLS;
- End-to-end encryption of screen sharing for remote access, support, or real time communication; and
- Use of integrity checks to monitor the completeness and correctness of the transfer of data.

Measures for Ensuring Data Quality

Commvault has implemented suitable measures to ensure that it is possible to check and establish whether and by whom Personal Data have been input into data processing systems or removed. This is accomplished by:

- An authorization policy for the input of Personal Data into memory, as well as for the reading, alteration and deletion of such stored data;
- Authentication of the authorized personnel;
- Protective measures for Personal Data input into memory, as well as for the reading, alteration and deletion of stored Personal Data, including by documenting or logging material changes to account data or account settings;
- Segregation and protection of all stored Personal Data via database schemas, logical access controls, and/or encryption;
- Utilization of user identification credentials;
- Physical security of data processing facilities; and
- Session time outs.

Measures for Ensuring Accountability

Commvault has implemented suitable measures to monitor, in accordance with applicable privacy laws, access restrictions of Commvault's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by:

- Individual appointment of system administrators;
- Adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for a reasonable period of time;
- Regular audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by Controller and applicable laws; and
- Keeping an updated list with system administrators' identification details (e.g., name, surname, function, or organizational area) and responsibilities.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Commvault has implemented annual testing of the SaaS Solution and relevant processes including security incident response tests, Business Continuity and Disaster Recovery tests, Penetration testing.

Measures for certification/assurance of processes and products

For relevant certifications refer to:

- https://www.commvault.com/legal/trust-center
- https://trust.commvault.com
- https://documentation.commvault.com/commvault/