

Commvault Customer Data Agreement
(Data Processing & Data Transfer Agreement)

Commvault may process personal data in the course of providing its products and services. This Data Processing Agreement (the “DPA”) incorporates the Standard Contractual Clauses Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors and forms part of the Terms of Service, or other agreement between Commvault and Customer for the purchase of Commvault’s products and services. Any terms not defined have the same definition ascribed to them in the Terms of Service or Standard Contractual Clauses. This DPA has been executed by Commvault as the data processor. To execute this DPA, Customer should complete Customer’s information and return the fully executed DPA to contracts@commvault.com.

SECTION I – INTRODUCTION

Clause 1 – Purpose and scope

- (a) The purpose of these Standard Contractual Clauses (“the Clauses”) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- (b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.
- (c) These Clauses apply to the processing of personal data as specified in Annex II.
- (d) Annexes I to IV are an integral part of the Clauses.
- (e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 - Invariability of the Clauses

- (a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
- (b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 - Interpretation

- (a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.
- (c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 – Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 – Docking clause

- (a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.
- (b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.
- (c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 6 – Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7 – Obligations of the Parties

7.1. Instructions.

- (a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
- (b) The processor shall immediately inform the controller if, in the processor’s opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation.

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data.

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing.

- (a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.
- (b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data.

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance.

- (a) The Parties shall be able to demonstrate compliance with these Clauses.
- (b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
- (c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.
- (d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors.

- (a) The processor shall not subcontract any of its processing operations performed on behalf of the controller in accordance with these Clauses to a sub-processor, without the controller's prior specific written authorisation. The processor shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub-processor in question, together with the information necessary to enable the controller to decide on the authorisation. The list of sub-processors authorised by the controller can be found in Annex IV. The Parties shall keep Annex IV up to date.
- (b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.
- (d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.
- (e) The processor shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the processor has factually disappeared, ceased to exist in law or has become insolvent – the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers.

- (a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
- (b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 – Assistance to the controller

- (a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.
- (b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.
- (c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
 - (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
 - (2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
 - (3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
 - (4) the obligations in Article 32 of Regulation (EU) 2016/679.
- (d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 - Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller.

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

- (a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- (b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:
 - (1) the nature of the personal data including where possible, the categories and approximate number of data subjects

concerned and the categories and approximate number of personal data records concerned;

- (2) the likely consequences of the personal data breach;
- (3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

- (c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor.

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

- (a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
- (b) the details of a contact point where more information concerning the personal data breach can be obtained;
- (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III - FINAL PROVISIONS

Clause 10 - Non-compliance with the Clauses and termination.

- (a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.
- (b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
 - (1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
 - (2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

- (3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.
- (d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I - List of parties

Controller(s):

1. Customer and its affiliates:

Name: ...

Address: ...

Contact person's name, position and contact details: ...

Data Protection Officer: ...

Signature and accession date: ...


Processor(s):

1. Commvault Systems, Inc.

Address: 1 Commvault Way, Tinton Falls, NJ 07724, USA

Contact person's name, position and contact details: Global Data Governance Officer (privacy@commvault.com)

Signature: ...


Jakub Lewandowski (Nov 7, 2023 09:13 GMT+1)

ANNEX II
Description of the processing

Categories of data subjects whose personal data is processed:

<i>Solution/Service</i>	<i>Categories of Data Subjects</i>
Software workloads	<ul style="list-style-type: none"> • <i>Customer’s staff involved in managing and using Solution (End users)</i> • <i>Other categories based on exact use case of the Solution</i>
SaaS Workloads	<ul style="list-style-type: none"> • <i>Customer’s staff involved in managing and using SaaS Solution (End users)</i> • <i>Other categories based on exact use case of the SaaS Solution</i>
ThreatWise	<ul style="list-style-type: none"> • <i>Customer’s staff involved in managing and using SaaS Solution (End users)</i> • <i>Threat actors</i>
Technical Support/Professional Services	<ul style="list-style-type: none"> • <i>Customer’s staff involved in managing and using Solutions (End users)</i> • <i>Other categories based on technical support case e.g. support tickets</i>

Categories of personal data processed:

<i>Solution/Service</i>	<i>Categories of Personal Data</i>
Software workloads	<ul style="list-style-type: none"> • <i>CommCell ID</i> • <i>Service usage information (metrics/logs)</i> • <i>Credentials such as passwords, account history, password hints, and similar security information used for authentication</i> • <i>Interactions with Commvault e.g., inquiries or complaints, support tickets.</i> • <i>Host names and IP addresses (depending on configuration)</i> • <i>File names and file paths (depending on configuration)</i>
SaaS Workloads	<ul style="list-style-type: none"> • <i>Customer Data subject to backup – due to nature of SaaS Solutions and encryption involved the exact types of data Customer personal data cannot be conclusively established and may vary depending on the exact use case of the SaaS Solution.</i> • <i>CommCell ID</i> • <i>Service usage information (metrics/logs)</i> • <i>Credentials such as passwords, account history, password hints, and similar security information used for authentication</i> • <i>Interactions with Commvault e.g. inquiries or complaints, support tickets.</i> • <i>Host names and IP addresses</i>
ThreatWise	<ul style="list-style-type: none"> • <i>Contact information (first name, last name, role, email, phone, fax, postal address)</i> • <i>Service usage information (metrics/logs)</i> • <i>Credentials such as passwords, account history, password hints, and similar security information used for authentication</i> • <i>Interactions with Commvault e.g., inquiries or complaints, support tickets.</i> • <i>Host names and IP addresses (e.g., source IP address, destination IP address)</i> • <i>Asset types (server listings, devices, applications)</i> • <i>Electronic identifiers</i> • <i>Network traffic information, event data</i> • <i>Threat actor’s attack patterns/behavioral analysis</i>
Technical Support/Professional Services	<ul style="list-style-type: none"> • <i>CommCellID</i> • <i>Contact information (first name, last name, role, email, phone, fax, postal address)</i> • <i>Company and/or employer</i> • <i>Title and/or position</i> • <i>Logs</i> • <i>Data types for respective Solution subject to technical support or in connection with Professional Services provisioned</i>

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

N/A. However, due to nature of Solutions and encryption involved, the exact types of personal data cannot be conclusively established and may vary depending on the exact use case of the Solution. No sensitive data is required in order to use the Solution.

Nature and purpose(s) of the processing:

<i>Solution/Service</i>	<i>Nature and purpose</i>
Software workloads	<ol style="list-style-type: none"> 1. Solution provisioning 2. Preventing, detecting, investigating, mitigating, and repairing problems, including security incidents; 3. Preventing frauds; 4. Auditing; 5. Billing; 6. Ongoing improvement (maintenance, including installing the latest updates and making improvements to the reliability, efficacy, quality and security) 7. Compliance with and enforcement of application legal requirements (e.g., maintaining records, litigation, mediation, arbitration, tax law, anti-money laundering, trade sanctions, whistle-blowing, complying with data subjects requests, etc.)
SaaS Workloads	<ol style="list-style-type: none"> 1. SaaS Solution provisioning 2. Preventing, detecting, investigating, mitigating, and repairing problems, including security incidents; 3. Preventing frauds; 4. Auditing; 5. Billing; 6. Ongoing improvement (maintenance, including installing the latest updates and making improvements to the reliability, efficacy, quality and security) 7. Compliance with and enforcement of application legal requirements (e.g., maintaining records, litigation, mediation, arbitration, tax law, anti-money laundering, trade sanctions, whistle-blowing, complying with data subjects requests, etc.)
ThreatWise	<ol style="list-style-type: none"> 1. Solution provisioning which includes deploying threat sensors around assets creating decoys within Customer environment allowing for anomalies tracking, threat detection and issuing warning alerts on threat activity. Activities in scope include threat actor profiling used to analyze and predict threat actors' behavior within that environment only. 2. Preventing, detecting, investigating, mitigating, and repairing problems, including security incidents; 3. Preventing frauds; 4. Auditing; 5. Billing; 6. Ongoing improvement (maintenance, including installing the latest updates and making improvements to the reliability, efficacy, quality and security) 7. Compliance with and enforcement of application legal requirements (e.g., maintaining records, litigation, mediation, arbitration, tax law, anti-money laundering, trade sanctions, whistle-blowing, complying with data subjects requests, etc.)
Technical Support/Professional Services	Technical support/Professional Services as defined by relevant purchase order

Duration of the processing:

As defined by the relevant purchase order.

For processing by sub-processors, also specify subject matter, nature and duration of the processing:

Sub-processor	Location	Commvault Solution			Technical Support / Professional Services	Description of Processing Additional comments
		Software workloads	SaaS Workloads	ThreatWise		
Commvault Systems Limited (UK)	UK	X	X	X	X	Commvault staff
Commvault Systems (India) Pvt. Ltd	India	X	X	X	X	Commvault staff
Commvault Systems (Australia) Pty. Ltd	Australia	X	X	X	X	Commvault staff
Microsoft Corporation	US/Other	X	X	X	X	<p>Cloud storage provider/Security analytics (Sentinel)/Technical support platform</p> <p>In case of cloud storage relevant Microsoft entity will be determined depending on the configuration choices made by the Customer.</p> <p>EU affiliate: Microsoft Ireland Operations Limited</p> <p>List of Microsoft sub-processors: https://servicetrust.microsoft.com/ViewPage/PrivacyDataProtection</p>
Oracle Corporation	US/Other	N/A	X	N/A	N/A	<p>Cloud storage provider</p> <p>In case of cloud storage relevant Oracle entity will be determined depending on the configuration choices made by the Customer.</p> <p>EU affiliate: Oracle EMEA Ltd</p> <p>List of Oracle affiliates: https://www.oracle.com/corporate/oracle-affiliates.html</p>
Commvault Systems (Israel) Ltd.	Israel	N/A	N/A	X	N/A	Commvault staff
Egnyte	US	N/A	N/A	X	N/A	Security and compliance tools for cloud content.
Triple C Cloud Computing Ltd.	Israel	N/A	N/A	X	N/A	Colocation services

ANNEX III

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>

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:

- [Trust Center \(commvault.com\)](https://trustcenter.commvault.com)
- <https://documentation.commvault.com/commvault/>

ANNEX IV

List of sub-processors

The controller has authorised the use of the following sub-processors:

1. **Microsoft Corporation**

Address: One Microsoft Way, Redmond, WA 98052, USA

Contact: Microsoft EU Data Protection Officer, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland.

Telephone: +353 (1) 706-3117

Description of the processing: Cloud Storage/Technical Support platforms

<https://www.microsoft.com/en-us/concern/privacy>

2. **Oracle Corporation**

Address: Oracle Corporation, Global Data Protection Officer, Willis Tower, 233 South Wacker Drive, 45th Floor, Chicago, IL 60606, USA

Description of the processing: Cloud Storage

3. **Commvault Affiliates**

Commvault Systems Limited (UK), Commvault Systems (India) Pvt. Ltd., Commvault Systems (Australia) Pty. Ltd., Commvault Systems (Israel) Ltd.

Address: 1 Commvault Way, Tinton Falls, NJ 07724, USA

Contact: Attn: Global Data Governance Officer & Legal (gdgo@commvault.com)

Description of the processing: Technical support/Professional service/development staff locations

4. **Egnyte, Inc.**

Address: Attn: Kris Lahiri, Data Protection Officer
1350 W. Middlefield Road Mountain View, CA 94043

Contact: privacy@egnyte.com

Description of the processing: Security and compliance tools for cloud content.

5. **Triple C Cloud Computing Ltd.**

Address: Ha-Sivim St 49, Petah Tikva, Israel

Description of the processing: Colocation services

DATA TRANSFER AGREEMENT

Commvault may transfer personal to a third country when provisioning its products and services for technical support or in the event Customer selects a data center location outside Customer's country of origin. This Data Transfer Agreement (the "DTA") incorporates the Standard Contractual Clauses as implemented by Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries and forms part of the Terms of Service, or other agreement between Commvault and Customer for the purchase of Commvault's products and services. Any terms not defined have the same definition ascribed to them in the Terms of Service or Standard Contractual Clauses. This DTA has been executed by Commvault as a data importer. To execute this DTA, Customer should complete Customer's information and return the fully executed DTA to contracts@commvault.com.

SECTION I – INTRODUCTION

Clause 1 – Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)1 for the transfer of personal data to a third country.
- (b) The Parties:
 - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A. (hereinafter each 'data exporter'), and
 - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer").
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 – Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 – Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
 - (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18. (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 – Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 – Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 – Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Docking clause

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 – Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions.

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation.

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency.

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy.

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data.

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing.

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data.

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers.

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance.

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 – Use of sub-processors

- (a) The data importer shall not subcontract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the subprocessor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

- (c) The data importer shall provide, at the data exporter's request, a copy of such a subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the subprocessor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 – Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11 – Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

- (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 – Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage. (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 – Supervision

- (a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards

the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 – Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- (i) the specific circumstances of the transfer, including the length of the processing chain, the

number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

- (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
- (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 – Obligations of the data importer in case of access by public authorities

15.1 Notification.

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it: (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization.

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These

requirements are without prejudice to the obligations of the data importer under Clause 14(e).

- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 – Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to

the extent and for as long as required under that local law.

- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 – Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party

beneficiary rights. The Parties agree that this shall be the law of Netherlands.

Clause 18 – Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of the Netherlands.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. List of parties

Data Exporters:

Company Name: [Customer and/or its affiliates] ...

Address: ...

Contact person's name, position, and contact details: [Data Protection Officer]

Activities relevant to the data transferred under these Clauses:

Signature and accession date: ...

Role: Controller

Data Importers:

Company Name: Commvault Systems, Inc.

Company Address: 1 Commvault Way, Tinton Falls, NJ 07724, USA

Contact person's name, position and contact details: Global Data Governance Officer (privacy@commvault.com)

Activities relevant to the data transferred under these Clauses: provision of the Commvault Solutions

Signature: 
Jakub Lewandowski (Nov 7, 2023 09:13 GMT+1)

Role: Processor

ANNEX I

B. Description of transfer

Refer to Annex II of the Data Processing Agreement

ANNEX I

C. Competent Supervisory Authority

The competent supervisory authority is Autoriteit Persoonsgegevens, The Netherlands.

ANNEX II

Refer to Annex III of the Data Processing Agreement

ANNEX III

List of sub-processors

Refer to Annex IV of the Data Processing Agreement

ADDITIONAL CLAUSES

1. **Switzerland.** This clause applies solely to transfers of personal data from Switzerland to data importers located outside of Switzerland, insofar as the data transfer is governed by FADP. In such case parties agree, that the Data Transfer Agreement and the Standard Contractual Clauses will be governed by the law of Switzerland and any dispute arising from the Data Transfer Agreement and/or Standard Contractual Clauses will be resolved by the courts of Switzerland and subject to supervisory authority of the FDPIC. The term 'member state' used in Standard Contractual Clauses must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18c of the Standard Contractual Clauses. The references to the GDPR should be understood as references to the FADP insofar as the data transfers are subject to the FADP.

2. **United Kingdom.** This clause applies solely to transfers of personal data from the United Kingdom of Great Britain and Northern Ireland to data importers located outside of UK, insofar as the data transfer is governed by applicable UK data protection laws, including amongst others, the UK GDPR. In such case the parties agree to be bound by the terms and conditions set out in the Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses with the adaptations as set out below.

International data transfer addendum to the European Commission's standard contractual clauses for international data transfers

Table 1: Parties

Start date	As per effective date of relevant purchase order	
The Parties	Exporter (who sends the Restricted Transfer) - further	Importer (who receives the Restricted Transfer)
Parties' details	Customer and its affiliates	Commvault Systems Inc.
Key Contact	As indicated in the Annex I to the Appendix A	As indicated in the Annex I to Appendix A
Signature (if required for the purposes of Section 2)	By executing the Data Processing Agreement and the Data Transfer Agreement parties agree to be bound by the mandatory clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022 with the adaptations as set out herein.	

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	<input checked="" type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to.
-------------------------	---

Table 3: Appendix Information

“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As set out in Annex I to the Data Transfer Agreement
Annex 1B: Description of Transfer: As set out in Annex I to the Data Transfer Agreement
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set out in Annex II to the Data Transfer Agreement
Annex III: List of Sub processors (Modules 2 and 3 only): As set out in Annex III to the Data Transfer Agreement

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section Error! Reference source not found.:
	<input checked="" type="checkbox"/> Importer
	<input checked="" type="checkbox"/> Exporter
	<input type="checkbox"/> neither Party

3. **CCPA/CPRA Compliance.** To the extent that Commvault accesses, hosts, retrieves, or processes any personal data, personal information, or personally identifiable information in connection with the Commvault Solutions which in the Terms constitutes “Personal Information” of a “Consumer”, as both terms are defined in CCPA/CPRA, Customer and Commvault agree to the following:

- (a) Customer and Commvault agree and acknowledge that Customer is a “Business” and Commvault is

- a “Service Provider” as both terms are defined in CCPA/CPRA.
- (b) Commvault will not Sell Personal Information (as the term “Sell” is defined in the CCPA/CPRA).
 - (c) Commvault will not retain, use, or disclose Personal Information:
 - (i) for purposes other than for the specific purpose of providing Solutions;
 - (ii) for a Commercial Purpose other than providing the Solutions, or
 - (iii) outside of a direct business relationship between Commvault and Customer.
 - (d) Commvault will not combine the personal information it receives from, or on behalf of, Customer with personal information that Commvault receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that Commvault may combine the personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this section and in regulations adopted by the California Privacy Protection Agency.


1. Customer and its affiliates: ...

Signature and accession date: ...

Role: Controller / Business

2. Commvault Systems, Inc.

Signature: ...


Jakub Lewandowski (Nov 7, 2023 09:13 GMT+1)

Role: Processor / Service Provider