DATA PROCESSING AGREEMENT

Commvault may process personal data in the course of providing its products and services. This Data Processing Agreement (the "DPA") addresses various personal data processing scenarios that may apply in course of providing such products and services including processor to processor relation, joint-controllership and separate controllership. 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 Partner Agreement, Master Terms and Conditions, or other agreement between Commvault and MSP related to Commvault's products and services. Any terms not defined have the same definition ascribed to them in the Partner Agreement or Standard Contractual Clauses. To execute this DPA, MSP should complete MSP's information and return the fully executed DPA to contracts@commvault.com together with a description of Technical and Organizational Measures in place (this requirement may also be addressed by providing proof of a relevant security/privacy certification e.g, ISO 27001, SOC 2 Type 2 or other similar).

1. Separate Controllers Processing Activities. The parties acknowledge that Commvault and MSP remain sole controllers of the personal data they do not collect, transmit, store and otherwise process in connection with reselling, marketing and distribution of Commvault's products and services as part of MSP's managed service offering for its customers, and shall be solely responsible for compliance with the obligations of the applicable data protection laws. In particular MSP will be considered a separate controller for the purpose of complying with accountancy and tax obligations.

2. Joint Controllership Processing Activities. The parties acknowledge that Commvault and MSP act as joint controllers of the personal data they collect, transmit, store and otherwise process in connection with reselling, marketing and distribution of Commvault's products and services as part of MSP's managed service offering for MSP's customers, in particular via the MSP portal, within the processing activities and within the scope of personal data stated in Appendix A, where categories of data subjects cover: (i) customer employees, agents and representatives and (ii) Commvault's and MSP's employees who have been granted access to the MSP portal ("MSP Personal Data"). The parties agree that essential elements of the MSP portal, including the performance, design and construction of the MSP portal, shall be determined solely by Commvault, provided that this is without prejudice to the parties' capability to carry out the processing activities set forth in Appendix A.

3. Respective responsibilities; Join Controllership. The respective responsibilities for compliance with the obligations of the GDPR and/or other applicable data protection laws in relation to the joint controllership of MSP Personal Data, shall be allocated as set forth in Appendix B, and each party shall comply with their requirements under Appendix B.

4. Processor to Processor(sub-processor) Processing Activities. The parties acknowledge that MSP and Commvault act respectively as processor and sub-processor of the customer's personal data they collect, transmit, store and otherwise process in connection with provisioning of Commvault's products and services ("Customer Personal Data").

5. Respective responsibilities; Processor to Processor(sub-processor). The respective responsibilities for compliance with the obligations of the GDPR and/or other applicable data protection laws in relation to processor to processor(sub-processor) processing activities in relation to Customer Personal Data, shall be allocated as set forth in Appendix C, and each party shall comply with their requirements under Appendix C.

6. Accountability. The parties shall be able to demonstrate compliance with their requirements under Appendix B and C in conformity with the principle of accountability set forth in Article 5(2) of the GDPR.

7. Assistance. If necessary, the parties shall provide each other with reasonable assistance in complying with their requirements under this DPA. The parties shall without undue delay provide each other with all information necessary for addressing requests for exercising the data subject's rights laid down in Articles 15 – 22 of the GDPR and/or applicable data protection laws. In the case of a Personal Data breach affecting the security of MSP Personal Data and/or Customer Personal Data parties shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the Personal Data breach to each other. This applies mutatis mutandis to the suspected Personal Data breach. The Parties shall not be entitled to request reimbursement of costs incurred in connection with providing assistance under this section.

8. Engaging processors. Commvault has MSP's general authorization for the engagement of sub-processors, on behalf of both parties with respect to the processing activities set forth in in Appendix A. Commvault shall remain fully responsible for compliance with the obligations set forth in Article 28 of the GDPR and/or in the applicable data protection laws.

9. Point of contact. The Parties agree to designate following points of contact in all matters related to personal data processing and this DPA:

On behalf of Commvault: Global Data Governance Officer at gdgo@commvault.com

On behalf of the MSP: _____

at _____

10. International data transfers. Parties agree that where either party carries out specific processing activities that involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679 (or similar requirements of applicable data protection laws), parties shall ensure compliance 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. Parties herewith execute standard contractual clauses (Module 1 Controller to Controller and/or Module 3 Processor to Processor), which are included as Appendix D to this Data Processing Agreement.

11. Termination of the MSP Agreement. Notwithstanding with the provisions of the Agreement, the parties acknowledge that upon the termination of the Agreement: (i) MSP Personal Data should remain on the MSP portal within the disposal of Commvault; (ii) MSP shall cease access to the MSP portal; (iii) MSP will be entitled to request an export of the selected MSP Personal Data related to customers. Commvault may agree to provide an export of selected MSP Personal Data related to customers provided that: (i) MSP provides Commvault with a legal basis for further processing of the requested MSP Personal Data after the termination date; (ii) MSP will not use MSP Personal Data related to customer for any other purposes other than those provided to Commvault;(iii) in any event, MSP shall not use MSP Personal Data related to customer for any marketing activities whatsoever related or unrelated to MSP's scope of services.

12. Other. All appendices and annexes constitute an integral part of the DPA.

Commvault Systems, Inc. and Commvault affiliates

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

Email: gdgo@commvault.com

Signature: Jakub Lewandowski

Accession date:

MSP

Address:

Email:

Signature:

Accession date:

Appendix A – Joint Controllership

Technical support

Billing

Auditing

Co-sell

Marketing and remarketing campaigns

Appendix B - Allocation of responsibilities with regards to MSP Personal Data collected in connection with Processing Activities listed in Appendix A, as follows:

No	Requirement	Allocation	
		Commvault	MSP
1	Draw up and post a privacy policy setting forth how MSP Personal Data are handled by the Parties Article 5 (1)(a) and Articles 12 to 14 of the GDPR	Yes	Yes (where relevant linking to Commvault's Privacy Policy)
2.	Indicate a designated contact point for data subjects in the privacy policy Article 26(1) of the GDPR	Yes	Yes
3.	Ensure that MSP Personal Data has been collected and are processed in conformity with the lawfulness principle Article 5 (1)(a) of the GDPR	Yes	Yes
4.	Ensure that MSP Personal Data are processed in conformity with the purpose limitation principle Article 5 (1)(b) of the GDPR	Yes	Yes
5.	Ensure that MSP Personal Data are processed in conformity with the data minimisation principle Article 5(1)(c) of the GDPR	Yes	Yes
6.	Ensure that MSP Personal Data are processed in conformity with the accuracy principle Article 5(1)(d) of the GDPR	Yes	Yes
7.	Ensure that MSP Personal Data are processed in conformity with the storage limitation principle Article 5(1)(e) of the GDPR	Yes (for the processing within the MSP portal)	Yes (for any potential processing outside of MSP portal)
8.	Ensure integrity and confidentiality of MSP Personal Data - Articles 5(1)(f) and 32 of the GDPR	Yes (for the processing within the MSP portal)	Yes (for any potential processing outside of MSP portal)
9.	Provide a contact point for requests for exercising the data subject's rights	Yes. As defined in Section 10 of the DPA	Yes. As defined in Section 10 of the DPA
10.	Ensure that requests for exercising the data subject's rights are addressed Articles 15 – 22 of the GDPR	Yes	Yes
11.	Ensure data protection by design and default Article 25 of the GDPR	Yes	No
12.	Implement appropriate technical and organisational measures, including appropriate data protection policies Articles 24 of the GDPR	Yes	Yes – to the extent data is exported/extracted from the MSP portal
13.	Maintain records of processing activities Article 30	Yes	Yes
14.	Notify Personal Data breach to the supervisory authority Article 33 of the GDPR	Yes	No
15.	Communicate a Personal Data breach to the data subject Article 34 of the GDPR	Yes	No
16.	Carry out a data protection impact assessment Article 35 of the GDPR	N/A	N/A
17.	Consult the supervisory authority prior to processing Article 36 of the GDPR	N/A	N/A
18.	Safeguard transfers of Personal Data to third countries or international organisations Articles 44 – 49 of the GDPR	Yes	Yes
19.	Obtain customer's (Data Controller) authorization for engaging subprocessors as defined under this Data Processing Agreement	N/A	Yes

Appendix C – Standard Contractual Clauses Controller to Processor

Parties acknowledge and agree that: (i) with regard to the processing of Customer Personal Data, and as more fully described in Appendix 1 hereto, customer is the data controller, MSP is the data processor and Commvault acts as a sub-processor; (ii) MSP received customer's authorization for engaging Commvault and other sub-processor as indicated in the Annex 4 hereto and herewith enters into contract with the Commvault to impose on Commvault materially same data protection obligations as the ones imposed on MSP by its' customer; and (iii) for this purpose, parties enter into this contract based on the standard contractual clauses as implemented by the Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors and the agree that the terms and obligations applicable to the data controller will apply mutatis mutandis to MSP acting as the processor and terms and obligations applicable to the data processor will apply mutatis mutandis to the Commvault as a sub-processor.

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):

Customer and its affiliates:

Name: …

Address: …

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

Data Protection Officer….

Signature and accession date: …

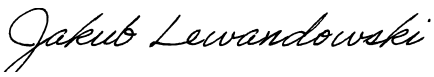
Processor(s):

Commvault Systems, Inc.

1 Commvault Way, Tinton Falls, NJ 07724, USA

Global Data Governance Officer

gdgo@commvault.com

Signature: 

ANNEX II – Description of the processing

Processing Customer Personal Data for the purposes of provisioning MSP's managed service offering for its customer.

Service	Subject matter	Duration
Metallic	SaaS-delivered backup and recovery eDiscovery (Data Discovery)	As per term of the engagement with customer
Metallic Cloud Storage Services	Cloud storage	As per term of the engagement with customer
Technical Support	Troubleshooting, technical support, maintenance	As per term of the engagement with customer

Categories of data subjects whose personal data is processed

Service	Categories of Data Subjects
Metallic / Metallic Cloud Storage Services	• customer's staff involved in managing and using SaaS Solution (End users) • other categories based on exact use case of the Services
Technical Support	• customer's staff involved in managing and using SaaS Solution (End users) • other categories based on technical support case e.g. support tickets

Categories of personal data processed

Metallic and Metallic Cloud Storage Services	• Customer Data subject to backup – due to nature of SaaS Solution 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 Services. • CommCell ID • Service usage information (metrics/logs) • Credentials such as passwords, account history, password hints, and similar security information used for authentication • Interactions with Commvault e.g. inquiries or complaints, support tickets. • Host names and IP addresses • File names and file paths
Technical Support	• First and last name, • CommCell ID • Contact information (including postal address, email, phone, fax) • Company and/or employer • Title and/or position • Logs • Data types for respectively Metallic Service or Metallic Cloud Storage Service subject to technical support

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.

Customer Data subject to backup – due to nature of SaaS Solution 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.

No sensitive data is required in order to use the SaaS Solution.

Nature and purpose of the processing

Service	Nature and purpose
Metallic/ Metallic Cloud Storage Services	1. Service provision 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	Technical support

Duration of the processing

As defined by the engagement with customer.

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

Name of Subprocessor	Description of Processing	Location of Subprocessor
Commvault Systems (India) Pvt. Ltd.	Technical Support Personnel	India
Commvault Systems Limited	Technical Support Personnel	United Kingdom
Commvault Systems (Australia) Pty. Ltd.	Technical Support Personnel	Australia
Microsoft Corporation	Azure Cloud/Technical Support Platform	Location (Azure region) based on customer selection/US

ANNEX III - Technical and organisational measures

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 IaaS, 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 in particular available here: https://www.microsoft.com/en-us/trust-center/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.
- 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 implemented a Business Continuity and Disaster Recovery plan, 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 regards 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;
- 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;
- 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;
  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://metallic.io/trust
- https://documentation.commvault.com/commvault/

ANNEX IV - List of sub-processors

MSP has authorised and where necessary obtained the customer's authorization for the use of the following sub-processors:

For Commvault:
1. Name: Microsoft Corporation
Address: One Microsoft Way, Redmond, WA 98052, USA
Contact person's name, position and contact details:
Microsoft EU Data Protection Officer
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18
D18 P521
Ireland
Telephone: +353 (1) 706-3117
https://www.microsoft.com/en-us/concern/privacy

Description of the processing: Cloud Storage

2. Name: Commvault Affiliates including: Commvault Systems Limited (UK), Commvault Systems (India) Pvt. Ltd., Commvault Systems (Australia) Pty. Ltd.
Address: 1 Commvault Way ,Tinton Falls, NJ 07724, USA
Contact person's name, position and contact details: Global Data Governance Officer [gdgo@commvault.com]

Description of the processing: Technical support staff locations

Appendix D - Standard Contractual Clauses for transfer of personal data to third countries

Parties acknowledge and agree that: (i) due to the fact that processing both MSP Personal Data and Customer Personal Data involves or may involve international data transfers, parties enter into this contract based on the standard contractual clauses as implemented by the European Commission Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries; (ii) with regards to the processing and transfers of Customer Personal Data, and as more fully described in Annex 1 hereto, customer is the data controller, MSP is the data processor (data exporter) and Commvault acts as a sub-processor (data importer). Consequentially any transfers in connection with Customer Personal Data is subject to Module three of the standard contractual clauses; and (iii) with regards to the processing and transfers of MSP Personal Data, and as more fully described in Annex 1 hereto, MSP and Commvault act as data controllers. Consequentially any transfers in connection with MSP Personal Data is subject to Module one of the standard contractual clauses.

STANDARD CONTRACTUAL CLAUSES

SECTION I- INTRODCUTION

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) 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') have agreed to these standard contractual clauses (hereinafter: 'Clauses').
(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 Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);
(iii) Module Three: Clause 9(a), (c), (d) and (e);
(iv) Clause 12 – Module One: Clause 12(a) and (d); Module 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 and Three: Clause 18(a) and
(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 – Optional 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.

MODULE ONE: Transfer controller to controller
8.1 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. It may only process the personal data for another purpose:
(i) where it has obtained the data subject's prior consent;
(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency. (a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
(i) of its identity and contact details;
(ii) of the categories of personal data processed;
(iii) of the right to obtain a copy of these Clauses;
(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.
(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.
(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimization. (a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation. The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 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 personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they 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 subject. 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.
(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
(d) 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 personal data breach, including measures to mitigate its possible adverse effects.
(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 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 or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers. The data importer shall not disclose the personal data 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') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:
(i) it 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 of Regulation (EU) 2016/679 with respect to the processing in question;
(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.
Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer. The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.
8.9 Documentation and compliance. (a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor
8.1 Instructions. (a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

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 rectify or erase 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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by 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 of Regulation (EU) 2016/679;
(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 or the controller 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 controller.
(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
(f) 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.
(g) 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

MODULE THREE: Transfer processor to processor
GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).
(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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 sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor 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

MODULE ONE: Transfer controller to controller
(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.
(b) In particular, upon request by the data subject the data importer shall, free of charge:
(i)provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);
(ii)rectify inaccurate or incomplete data concerning the data subject;
(iii)erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:
(i)inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
(ii)implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.
(e)Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
(f)The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.
(g)If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE THREE: Transfer processor to processor
(a)The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
(b)The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by 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

MODULE ONE: Transfer controller to controller
(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)Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.
(c)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.
(d)The Parties agree that if one Party is held liable under paragraph (c), 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.
(e)The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE THREE: Transfer processor to processor
(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

MODULE ONE: Transfer controller to controller
MODULE THREE: Transfer processor to processor
(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
MODULE ONE: Transfer controller to controller
MODULE THREE: Transfer processor to processor

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

MODULE ONE: Transfer controller to controller
MODULE THREE: Transfer processor to processor

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.For Module Three: The data exporter shall forward the notification to the controller.
(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.). For Module Three: The data exporter shall forward the information to the controller.
(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. [For Module Three: The data exporter shall make the assessment available to the controller.]
(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 [for Module Three: and the controller] 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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the 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 – List of parties

A. LIST OF PARTIES

Data exporter(s):
1. For Customer Personal Data – MSP or respective MSP affiliate (as controller and/or processor)
2. For MSP Personal Data – either MSP or Commvault (as controller)

Data importer(s):
1. For Customer Personal Data - Commvault or respective Commvault affiliate (as controller and/or processor(sub-processor))
2. For MSP Personal Data – either MSP or Commvault as controller (as controller)

Commvault Systems, Inc. and Commvault affiliates
1 Commvault Way, Tinton Falls, NJ 07724, USA
Global Data Governance Officer at gdgo@commvault.com

_____

Name: …
Address: …
Contact person's name, position and contact details: …
Signature and accession date: …

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

Categories of data subjects whose personal data is transferred

- *MSP's staff involved in managing and using Commvault's products and services (in particular authorized users of the MSP portal)*
- *MSP's customers and further MSP's staff involved in managing and using Commvault's products and services*
- *Commvault's staff*

Categories of personal data transferred
Electronic identifiers (including Commcell ID, Customer ID); e-mail; First name; Last name; Company name; Services purchased/used; Provisioning country; Address/Country; Billing county; Billing information;
Phone; Inquires/request/support tickets; Timestamps; Service usage data; Contact preferences; Severity (low/medium/high/critical); Issue type; Brief Description; Troubleshooting steps attempted; Additional details
-referred to collectively as "MSP Personal Data" under the Data Processing Agreement

Sensitive data transferred (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

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
Continuous basis

Nature of the processing
Access through MSP Portal

Purpose(s) of the data transfer and further processing
Service provisioning
Billing
Audit
Preventing, detecting, investigating, mitigating, and repairing problems, including security incidents
Ongoing improvement (maintenance, including installing the latest updates and making improvements to the reliability, efficacy, quality and security)
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.)
Preventing frauds

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
10 years from the point when the relation with the MSP ends

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
Note applicable

MODULE THREE: Transfer processor to processor

Description of the processing related to Customer Personal Data is contained in Annex II to Appendix C.

C. COMPETENT SUPERVISORY AUTHORITY

Dutch Data Protection Authority

ANNEX II – Technical and Organizational Measures

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

For Commvault: as described in Annex III to Appendix C

For MSP: to be provided by MPS when executing this DPA

ANNEX III – List of sub-processors

LIST OF SUB-PROCESSORS

For Commvault: as described in Annex IV to Appendix C

For MSP: N/A