rubrik

RUBRIK, INC. DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the Rubrik End User License Agreement or other mutually accepted written or electronic agreement between Rubrik and Customer ("**Agreement**") and is effective on the date last signed below ("**Effective Date**"). This DPA reflects the Parties' agreement with respect to the Processing of Customer Personal Data in the provision of Products and Services pursuant to the Agreement. This DPA also consists of Exhibit 1 - The Details and Nature of the Processing, Exhibit 2 - The Data Security Schedule. Should Customer Personal Data be subject to a Transfer (as set forth in Section 10 (Data Transfers) below), the Parties agree that the attached Standard Contractual Clauses with its Appendices ("**SCC**") shall also form part of this DPA. In the event of any conflict or inconsistency between the terms of the Agreement and this DPA, the terms of this DPA shall prevail. The terms of this DPA shall also supersede any privacy policies or privacy statements made by Rubrik. For clarity, consistent with Clause 10 of the SCC, the terms of the SCC shall prevail over any other term in this DPA. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

This DPA has been pre-signed on behalf of Rubrik, Inc. as the data importer. In order for this DPA to become effective, Customer must (i) complete the information in the signature box on this DPA and sign; (ii) if applicable, complete the information as the data exporter on the SCC; and (iii) if applicable, complete the information in the signature box of the SCC and sign. In the event Customer is signing this DPA on behalf of itself and, to the extent required and authorized by applicable Data Protection Laws, its Affiliates, who qualify as Controllers, Customer shall indicate the foregoing on the DPA and if applicable, the SCC. Customer must then send the completed and signed DPA to Rubrik via email, indicating Customer's full entity name, as set forth in the Agreement to DPA@rubrik.com. Upon receipt of the properly completed DPA by Rubrik, this DPA shall become effective and legally binding on the Parties.

1. DEFINITIONS.

1.1 "**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

1.2 "**Data Protection Laws**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, including without limitation, the California Consumer Privacy Act ("**CCPA**"), applicable to the Processing of Customer Personal Data under this DPA. For the avoidance of doubt, if Rubrik's Processing involving Customer Personal Data is not within the scope of a given Data Protection Law, then such law is not applicable for purposes of this DPA.

1.3 "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

1.4 "**GDPR**" means the Regulation (EU) 2016/679 (General Data Protection Regulation) 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 of Directive 95/46/EC.

1.5 "**Personal Data**", "**Personal Information**", and "**Personally Identifiable Information**", which shall be referred to individually or collectively in this DPA as "Personal Data", mean (i) any information relating to an identified or identifiable national person, and/or (ii) any information that identifies, relates to, describes, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Unless prohibited or specifically governed by applicable Data Protection Laws, Personal Data shall not include information or data that is anonymized, de-identified and/or compiled on a generic basis and which does not name or identify a specific person.

1.6 "**Personal Data Breach**" means a breach of Rubrik's obligations set forth in Exhibit 2 to this DPA, (Data Security Schedule) which leads to any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.

1.7 "**Processor**" means an entity which is Processing Customer Personal Data on behalf of the Controller.

1.8 **"Process" or "Processing"** means any operation or set of operations which is performed upon Customer Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.9 "**Standard Contractual Clauses**" or "**SCC**" means the standard data protection clauses for the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission decision 2010/87/EC, dated 5 February 2010, or any set of clauses later approved by the European Commission which amend, replace or supersede such version.

1.10 **"Subprocessor"** means any party engaged by the Processor to process Customer Personal Data.

1.11 "**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

2. SCOPE AND DURATION. The Parties acknowledge and agree that with respect to the rights and obligations under this DPA, Customer is the Controller and Rubrik is the Processor of any Customer Personal Data. In the course of providing the Products and SaaS Services, Support Services, and Professional Services (collectively, "**Services**") to Customer pursuant to the Agreement, Rubrik may Process certain Customer Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Customer Personal Data. Rubrik shall not Process Customer Personal Data, except to perform and provide the Services and only in accordance with the terms of this DPA, Customer's Instructions (as defined below), and applicable Data Protection Laws. Rubrik will Process Customer Personal Data for the Term of the Agreement, unless otherwise agreed to by the Parties in writing or pursuant to a requirement under Data Protection Laws.

3. CUSTOMER INSTRUCTIONS. The Parties acknowledge and agree that for the purposes of this DPA, "**Customer Instructions**" means (i) the obligations and requirements set forth in this DPA and the Agreement, (ii) the applicable Documentation, (iii) Customer's use and configuration of the Services, and (iv) any additional written instruction Customer provides to Rubrik, which Rubrik agrees to in writing via an amendment to this DPA, regarding the Processing of any Customer Personal Data. In the event Rubrik becomes aware that a Customer Instruction potentially infringes a Data Protection Law to which Rubrik is subject, Rubrik shall inform Customer of that legal issue before Processing, unless the applicable Data Protection Law prohibits such disclosure, including for reasons such as on the important grounds of public interest. For purposes of clarity, under this DPA, Rubrik does not have a duty to investigate any Customer Instruction to determine whether it infringes any Data Protection Law. However, in the event Rubrik notifies Customer of any potential infringement of an applicable Data Protection Law, the Parties will work together in good faith to resolve such issue in a timely manner. In no event will either Party be required to perform any activity that violates any applicable Data Protection Law. Customer will be responsible for all liability for all claims and damages arising from any Processing by Rubrik in accordance with a Customer Instruction.

4. RUBRIK'S OBLIGATIONS. Rubrik shall limit access to Customer Personal Data to only those persons authorized by Rubrik to Process Customer Personal Data and who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. When providing or making available Customer Personal Data to Rubrik, Customer shall only disclose or transmit Customer Personal Data that is necessary for Rubrik to perform the applicable Services. Rubrik will protect the confidentiality of Customer Personal Data through implementing and maintaining the technical and organizational measures set out in Exhibit 2 to this DPA, (Data Security Schedule) which takes into account the state of the art of technology, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons and offers a level of security appropriate to the risk of the Processing of Customer Personal Data. Rubrik shall notify Customer without undue delay, but in no event in less than seventy-two (72) hours of becoming aware of any Personal Data Breach, and Rubrik will take reasonable steps to: (i) identify the cause of such Personal Data Breach; and (ii) take the steps necessary and reasonable to remediate the cause of such Personal Data Breach to the extent such remediation is within Rubrik's reasonable control. To the extent Rubrik has the information, Rubrik will provide reasonable assistance to Customer with respect to Customer's obligations under applicable Data Protection Laws, including without limitation, Article 33(3) of the GDPR.

5. CUSTOMER'S OBLIGATIONS. Customer is solely responsible for the accuracy and legality of Customer Personal Data provided to Rubrik. Customer represents and warrants that it complies with all applicable Data Protection Laws, including without limitation, possessing all necessary rights to provide the Customer Personal Data to Rubrik for the Processing to be performed in relation to the Services. Customer agrees that it shall be responsible for obtaining all necessary consents and providing all necessary notices to Data Subjects, as required under the relevant Data Protection Law. In addition, Customer is responsible for determining whether the Services are appropriate for the storage and Processing of Customer Personal Data subject to any specific Data Protection Law or regulation, as well as for the configuration and use of any Services in a manner consistent with Customer's legal

and regulatory obligations. Customer shall defend and indemnify Rubrik in the event of a third-party claim alleging any breach of the foregoing Customer obligations.

6. AUDITS AND ASSISTANCE.

6.1 Rubrik undertakes to perform regular audits to verify its technical and organizational security measures. Such audits will be conducted: (i) by a qualified independent third party; (ii) at least annually; (iii) in accordance with SOC 2 or ISO 27001 standards or substantially equivalent standards; and (iv) will result in an audit report ("**Report**"). Upon Customer's written request, and subject to the confidentiality obligations set forth in the Agreement, Rubrik agrees to make available the Report and its applicable certifications in order to demonstrate the technical and organizational security measures implemented by Rubrik.

6.2 Rubrik will provide reasonable assistance to Customer so that Customer may comply with Customer's obligations to perform a data protection impact assessment related to Customer's use of the Products and Services, to the extent Customer does not otherwise have access to the relevant information and to the extent such information is available to Rubrik. Rubrik shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in relation to this DPA, to the extent required by GDPR. Further, Rubrik will take such steps as are reasonably required to assist Customer with its obligations under Articles 32 to 36 of GDPR taking into account the nature of the Processing.

7. DATA ERASURE. Upon Customer's request, Rubrik will return or delete all Customer Personal Data following the termination of the Agreement, unless such Customer Personal Data is required to be maintained by applicable Data Protection Laws, in which case it shall be held in accordance with the terms of this DPA.

8. SUBJECT ACCESS REQUESTS. Taking into account the nature of the Processing, Rubrik will reasonably assist the Customer with Data Subject requests. For the avoidance of doubt Rubrik will not respond directly to Data Subjects requests, but to the extent legally permissible, Rubrik will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to any such request.

9. SUBPROCESSORS. Customer acknowledges and agrees that Rubrik may retain its Affiliates and third parties as Subprocessors in connection with the provision of the Services. Rubrik maintains a current list of Subprocessors required to provide its Products and Services, which can be found at https://www.rubrik.com/en/legal/rubrik-subprocessors. Rubrik will only appoint any new Subprocessors pursuant to Article 28(2) of the GDPR. At the web link set forth above, Customer may also find a mechanism to subscribe to notifications of new Subprocessors for each applicable Service, and if Customer subscribes, Rubrik shall provide notification of a new Subprocessor(s) before authorizing any new Subprocessor(s) to process Customer Personal Data in connection with the provision of the applicable Service. If Customer does not object to the appointment of any new Subprocessors within 30 days after notification of such appointment by Rubrik, Customer will be deemed as having provided its consent to the new appointment. Should Customer object (acting reasonably) to a new Subprocessor, upon prior written notice, Rubrik will use reasonable efforts to make available to Customer a change in the Service or recommend a commercially reasonable change to Customer's configuration or use of the Service to avoid Processing of Customer Personal Data by the objected-to new Subprocessor without unreasonably burdening Customer. If Rubrik is unable to make available such change within a reasonable time period, which shall not exceed thirty (30) days, Customer may terminate the Agreement with respect to those specific Services that cannot be provided without the objected-to new Subprocessor. Such termination right is Customer's sole and exclusive remedy with respect to such objection. Rubrik undertakes to enter into a written agreement with any applicable Subprocessors in accordance with the requirements under Data Protection Laws and such obligations will in no event be less protective than this DPA. Rubrik will restrict the Subprocessors' access to only what is necessary to provide or maintain the Products and Services. Rubrik will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Subprocessors.

10. DATA TRANSFERS. Customer and Rubrik agree that any transfers of Customer Personal Data outside the European Economic Area to a third country that has not been given adequacy by the European Commission ("**Transfer**"), shall be subject to the Standard Contractual Clauses, or other permitted transfer mechanisms under the GDPR, to be executed between the Parties if applicable. If required, the Parties will also execute the attached SCC which will become part of this DPA.

11. CERTIFICATIONS. Customer agrees that execution of this DPA by Rubrik shall be deemed to constitute any certification that is required under applicable Data Protection Law, including without limitation, the CCPA, as to the restrictions on sale, retention, use or disclosure of Customer Personal Data.

12. **LAW ENFORCEMENT ACCESS**. Rubrik will not disclose or provide access to any Customer Personal Data Processed by Rubrik under this DPA to a law enforcement agency, unless required by law. If a law enforcement agency contacts Rubrik with a demand for Customer Personal Data, Rubrik will attempt to redirect the law enforcement agency to request that data directly from Customer. If Rubrik is compelled to disclose or provide access to any Customer Personal Data Processed under this DPA to the law enforcement agency, Rubrik will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

13. **ADDITIONAL TERMS FOR POLARIS FOR MICROSOFT 365 PROTECTION.** In the event Customer has licensed Rubrik's Polaris for Microsoft 365 Protection SaaS Services (the "**M365 Services**"), this Section shall also apply with respect to the Processing of Customer Personal Data. The M365 Services provide backup services of Customer's Microsoft 365 environment through Rubrik's Polaris, which is a data plane hosted within the Google Cloud Platform environment. In the event Customer elects to use hosted environment, Rubrik will provision a Microsoft Azure environment for Customer's use, and Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls as part of Customer's use of the M365 Services. Customer acknowledges and agrees that Customer has verified that the applicable security measures Google and Microsoft use as part of their services are adequate for purposes of Processing Customer Personal Data. For technical and organizational measures applicable to Microsoft Azure and Google Cloud Platform, please refer to the applicable terms and documentation, respectively, at: https://www.microsoft.com/en-us/trust-center/privacy, and https://cloud.google.com/terms/data-processing-terms.

14. **CHANGES IN LAWS.** In the event of (i) any newly enacted Data Protection Law, (ii) any relevant change to an existing Data Protection Law (including generally-accepted interpretations thereof), (iii) any interpretation of a new or existing Data Protection Law by Customer, or (iv) any material new or emerging cybersecurity threat, which individually or collectively requires a change in the manner by which Rubrik is delivering the Services to Customer, the Parties shall agree upon how Rubrik's delivery of the Services will be impacted and shall make equitable adjustments to the terms of the Agreement and the Services.

IN WITNESS WHEREOF the Parties have caused this DPA to be executed and delivered by their respective authorized signing officers, effective as of the Effective Date.

Rubrik, Inc.:	**Customer:**
Authorized Signature:	Authorized Signature:
By: DocuSigned by: Peter McGoff 6450C691E25945E...	By:
Name: Peter McGoff	Name:
Title: CLO	Title:
Date: 30 March 2021	Date:

EXHIBIT 1 TO THE DATA PROCESSING ADDENDUM

DESCRIPTION OF PROCESSING OF CUSTOMER PERSONAL DATA

Subject matter and duration of the Processing of Customer Personal Data:

The subject matter of the Processing of the Customer Personal Data is set out in the Agreement (including all applicable attachments); namely, for Rubrik to provide the relevant Products and Services. The duration of the Processing of Customer Personal Data shall be for the Term of the Agreement.

The nature and purpose of the Processing of Customer Personal Data:

The nature and purpose of the Processing of the Customer Personal Data are set out in the Agreement and include:

1. Provision of the relevant Products and Services;
2. Delivering any additional services, including providing technical support, deployment, and solution/software development services, troubleshooting, detecting, investigating, mitigating, and repairing problems, including security incidents; and
3. Ongoing improvement by Rubrik of the relevant Products and Services, including without limitation, any maintenance, including installing the latest updates, and making improvements to the reliability, efficacy, quality, and security of the Products and Services.

The categories of Data Subject to whom the Customer Personal Data relates:

Due to the nature of backup services and the encryption of Customer Personal Data in Customer's environment, the exact categories of Data Subjects cannot be determined by Rubrik and may vary depending on Customer's use of the Services. In general, the categories of Data Subjects may include Customer's end users, employees, contractors, customers, vendors and other affiliated entities; provided, however, Customer acknowledges and agrees that Customer elects the categories of Data Subjects to whom the Customer Personal Data relates in Customer's sole discretion. In the case of Services set forth in line items 2 and 3 above, the categories of Data Subjects for Customer Personal Data would include Customer's employee's name, surname, company, role, support ticket, contact details, and electronic identifiers.

The types of Customer Personal Data to be Processed:

Due to the nature of backup services and the encryption of Customer Personal Data in Customer's environment, the exact types of Customer Personal Data cannot be determined by Rubrik and may vary depending on Customer's use of the Services. In general, the types of Customer Personal Data to be Processed under the Agreement may include Customer's end users, employees, contractors, customers, vendors and other affiliated entities; provided however, Customer acknowledges and agrees that Customer elects the types of Customer Personal Data to be Processed in Customer's sole discretion. In the case of Services set forth in line items 2 and 3 above, the types of Customer Personal Data would include Customer's employee's name, surname, company, role, support ticket, contact details, and electronic identifiers.

EXHIBIT 2 TO THE DATA PROCESSING ADDENDUM

DATA SECURITY SCHEDULE

This Data Security Schedule ("**Schedule**") sets forth the technical and organizational measures that Rubrik and Customer will maintain in order to protect the security of Customer Personal Data during the Term of the applicable End User License Agreement (the "**Agreement**"). In the event of an inconsistency between the terms of the Agreement and the terms of this Schedule, this Schedule will govern. All capitalized terms used but not defined herein have the meanings ascribed to them in the Agreement or in the Rubrik Data Processing Addendum ("**DPA**").

1. Security and Data Protection Program

Rubrik will maintain and enforce a written information security and data protection program including policies and procedures that are aligned with industry standards. Additionally, Rubrik will maintain a risk management program for purposes of identifying and mitigating security and data concerns proactively, and as such, risks are continuously monitored, measured, and mitigated in accordance with industry practices. On an annual basis, Rubrik, through independent third parties, conducts security and privacy assessments to validate its information security controls against standards such as SOC2 Type II, ISO 27001, or an industry equivalent for its Services. Rubrik updates its security program on an ongoing basis to respond to changes in technology, the evolving threat environment, and current industry practices. Rubrik may update this Schedule accordingly in its discretion; however, no such updates will materially reduce the protections set forth herein.

2. Security Audit Reports

Rubrik will provide the Customer, or the Customer's designee, reasonable responses to a security questionnaire designed to assess Rubrik's systems, processes, policies, and records as they relate to the scope of Services provided, not more than once per calendar year. In addition, upon Customer's request, Rubrik will provide a copy of its most recent SOC2 Type II (or successor standard) audit report under confidentiality agreements in place between Rubrik and the Customer.

3. Access Controls

Rubrik will implement appropriate access controls and segregation of duties in the assignment of all critical job functions related to its Processing of Customer Personal Data and the Services provided to the Customer. Rubrik will limit access to Customer Personal Data to personnel using the concept of "least privileged access," meaning individuals are granted access to only those systems that are required to perform their role. Access and privileges for Rubrik personnel will be audited on a quarterly basis as a minimum standard to confirm that concept of "least privileged access" is in place. In addition, Rubrik limits access to those personnel who have been trained in Rubrik's information security practices and are bound by an obligation of confidentiality. Continuous training on new security practices, privacy standards, and organizational policies also occurs on an annual basis to build on Rubrik's employees' body of knowledge. Rubrik maintains processes designed to confirm that each authorization for access to Customer Personal Data has been approved by the appropriate Rubrik management personnel. Access to all systems Processing Customer Personal Data will produce audit logs that provide non-repudiation through verified multi-factor authentication access controls. Audit logs of Rubrik's personnel access of Customer Personal Data will show identification, authentication, and authorization if a member of Rubrik's personnel accesses Customer Personal Data. If access to Customer Personal Data is no longer necessary, Rubrik will remove such personnel's access promptly. Customers should configure and maintain industry-standard security controls to manage access to its infrastructure, devices, equipment, and applications that interface with Rubrik Products. Customer is responsible for securing the Rubrik Products in its environments and for implementing the requirements prescribed in the security hardening documentation provided by Rubrik.

4. Physical and Environmental Security

Rubrik implements and maintains reasonable physical security safeguards for all Rubrik facilities where Customer Personal Data is used, stored, maintained, or accessed. Physical access to Rubrik's third-party data centers is restricted to authorized personnel primarily in technical operations and provisioned upon an authorized request by Rubrik management. A review of the physical access is performed on an annual basis by Rubrik management. Rubrik maintains badging requirements for its onsite personnel and visitors and uses video cameras, video camera footage, and other access control mechanisms to monitor individual physical access to sensitive areas. Rubrik has a facilities security policy that mandates security principles for internal and third-party security staff. Rubrik is committed to protecting all facilities and physical assets that are used during the course of the Agreement.

5. Security and Privacy Awareness training

Rubrik requires its personnel to complete appropriate training for the type of data, systems, and information assets they may use or access. Rubrik will maintain a security and privacy awareness program to address the evolving non-technical security threats. These programs include:

- Security and Privacy teams that provide assistance and guidance to personnel, as appropriate;
- Regular phishing campaigns and training throughout the year for Rubrik's specific user populations; and
- Annual security and privacy awareness training throughout the organization to cover current and relevant training content for key threats such as phishing, use of privileged access, data security, social engineering and other relevant areas.

6. Penetration Testing and Vulnerability Assessments

Rubrik conducts annual application penetration testing by an independent third-party organization for products and/or applications within the scope of services provided to the Customer. Rubrik will also engage in social engineering penetration testing to test the security posture and awareness of Rubrik's personnel. Further, Rubrik will complete internal and external vulnerability scans of its systems and services periodically, and will update and patch operating systems, applications, firewalls, and all other in-scope systems and applications and remediate or mitigate all such vulnerabilities in accordance with industry standard timelines based on risk.

7. Endpoint Security and Security Protection

Rubrik uses current industry-standard endpoint security measures to protect its internal systems from malware, worms, trap doors, back doors, spyware, malicious logic, trojan horses, time bombs, or other malicious code or programs intentionally designed to damage or enable unauthorized use of or access to Rubrik's IT systems. These endpoint security measures include system monitoring, antivirus software, and endpoint threat detection software.

8. Encryption

To the extent technically feasible, but in all situations where required by applicable law, Rubrik agrees to store and transmit Customer Personal Data in a commercially reasonable format using industry accepted encryption technology. All data transmissions over the internet are encrypted with Transport Layer Security version 1.2. All data at rest is encrypted using Advanced Encryption Standard (AES) 256.

9. Network and Host Security

Rubrik maintains network intrusion detection/prevention, firewalls and security monitoring capabilities that monitor all traffic on Rubrik's corporate network in connection with the Services. Firewalls are used to protect Rubrik's corporate network from the internet and separate the internal network from the internet and Customer's connections. Firewall settings have been configured to deny traffic by default and allow only authorized traffic in accordance with corporate standards. Rubrik reviews and validates firewall rulesets every six months. Network segmentation occurs to prevent Rubrik's corporate network from accessing Customer Personal Data without the Customer's explicit permission.

10. Security Monitoring and Alerting

Rubrik will implement detection tools to prevent data exfiltration through Rubrik provided laptops, workstations and cloud environments. Rubrik will monitor its on-premise and multi-cloud environment 24x7, detect security threats, investigate and respond to security events and incidents.

11. Personal Data Breach Management

Rubrik will maintain at all times during the Term a written security incident response program, including event reporting and escalation procedures, that is used by Rubrik's personnel to report and manage Personal Data Breaches. The incident response program will be regularly tested, including through tabletop exercises involving all parts of the enterprise having responsibilities relating to Personal Data Breach responses. To the extent permitted and in accordance with applicable Data Protection Laws, Rubrik will promptly, but in no later than seventy-two (72) hours, notify the Customer of any confirmed Personal Data Breach. Rubrik will cooperate with Customer's reasonable requests for information regarding any such Personal Data Breach, and Rubrik will provide regular updates, upon request, on the incident and the investigative action and corrective action taken.

12. Business Continuity and Disaster Recovery

While Rubrik continually strives to anticipate and prevent problems from occurring, Rubrik recognizes that the potential exists for unforeseen or unpreventable events and emergencies, such as:

- Utility interruptions
- Labor shortages
- Equipment failures
- Interruption from externally provided products, processes and services
- Recurring natural disasters
- Infrastructure disruptions
- Cyber-attacks on Rubrik or Rubrik's Suppliers' systems

In the event of an unforeseen or unpreventable event, Rubrik maintains processes and procedures to minimize the disruption of important and time critical operations, even during an emergency. The Business Continuity Plan guides Rubrik to effectively establish and implement a consistent management and response method so that Rubrik is capable of performing mission-critical functions and services under threats and conditions. Business continuity is an ongoing process and provides for the prevention, preparation, response and recovery for the security of a company. In addition, Rubrik leverages systems and services with high availability and redundancy.

13. Secure Development Practices

Rubrik adheres to security and privacy by design principles and builds those principles into Rubrik's Products such that security and privacy are considered at each stage of development, rather than only at the end of the development process. Rubrik's development practices follow the guidance of OWASP Top 10, SANS Top 20, and CIS Control Benchmarks. Rubrik's formal Software Development Life Cycle ("**SDLC**") policy governs the development, acquisition, configuration, implementation, and maintenance of system components. Management reviews and approves the SDLC policy on an annual basis and the SDLC policy is made available to all personnel.

14. Configuration Management

Changes to any of Rubrik's Products go through a multi-step processes and are reviewed by an internal change control board prior to being deployed into production.

15. Incident Response Policy

Rubrik's Incident Response Policy includes directions to be followed in the event of any action deemed a security incident. This policy includes the roles and responsibilities of personnel assigned to the security incident, the leadership responsibilities, command and control methods, and guidance on developing and implementing corrective action plans.

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

Name of the data exporting organisation:
Address:
Tel.: ; **e-mail:**
Other information needed to identify the organisation
……
(the data exporter)
And

Name of the data importing organisation: Rubrik, Inc.
Address: 3495 Deer Creek Road, Palo Alto, CA 94304, United States
Tel.: +1 844 478 2745; **e-mail:** dpa@rubrik.com
Other information needed to identify the organisation:
……
(the data importer)
each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Background

The data exporter has entered into a data processing addendum ("**DPA**") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:
Name:
Position:
Address: Signature…….

On behalf of the data importer:
Name: Rubrik, Inc.
Position: CLO
Address: 3495 Deer Creek Road, Palo Alto, CA 94304, United States Signature…….

DocuSigned by:
Peter McGoff
6450C691E25945E...

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

DESCRIPTION OF PROCESSING OF CUSTOMER PERSONAL DATA

Data exporter	**Data importer**
The data exporter is:	The data importer is: **Rubrik, Inc.**

Subject Matter and Duration of the Processing of Customer Personal Data:
The subject matter of the Processing of the Customer Personal Data is for Rubrik to provide the relevant Products and Services.

The Nature and Purpose of the Processing of Customer Personal Data:
The nature and purpose of the Processing of the Customer Personal Data include:

1. Provision of the relevant Products and Services;
2. Delivering any additional services, including providing technical support, deployment, and solution/software development services, troubleshooting, detecting, investigating, mitigating, and repairing problems, including security incidents; and,
3. Ongoing improvement by Rubrik of the relevant Products and Services, including without limitation, any maintenance, including installing the latest updates, and making improvements to the reliability, efficacy, quality, and security of the Products and Services.

The Categories of Data Subject to Whom the Customer Personal Data Relates:
Due to the nature of backup services and the encryption of Customer Personal Data in Customer's environment, the exact categories of Data Subjects cannot be determined by Rubrik and may vary depending on Customer's use of the Services. In general, the categories of Data Subjects may include Customer's end users, employees, contractors, customers, vendors and other affiliated entities; provided however, Customer acknowledges and agrees that Customer elects the categories of Data Subjects to whom the Customer Personal Data relates in Customer's sole discretion. In the case of Services set forth in line items 2 and 3 above – the categories of Data Subjects for Customer Personal Data would include Customer's employee's name, surname, company, role, support ticket, contact details, electronic identifiers.

The Types of Customer Personal Data to be Processed:
Due to the nature of backup services and the encryption of Customer Personal Data in Customer's environment, the exact types of Customer Personal Data cannot be determined by Rubrik and may vary depending on Customer's use of the Services. In general, the types of Customer Personal Data to be Processed may include Customer's end users, employees, contractors, customers, vendors and other affiliated entities; provided however, Customer acknowledges and agrees that Customer elects the types of Customer Personal Data to be Processed in Customer's sole discretion. In the case of Services set forth in line items 2 and 3 above – the types of Customer Personal Data would include Customer's employee's name, surname, company, role, support ticket, contact details, electronic identifiers.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. Security and Data Protection Program

Rubrik will maintain and enforce a written information security and data protection program including policies and procedures that are aligned with industry standards. Additionally, Rubrik will maintain a risk management program for purposes of identifying and mitigating security and data concerns proactively, and as such, risks are continuously monitored, measured, and mitigated in accordance with industry practices. On an annual basis, Rubrik, through independent third parties, conducts security and privacy assessments to validate its information security controls against standards such as SOC2 Type II, ISO 27001, or an industry equivalent for its Services. Rubrik updates its security program on an ongoing basis to respond to changes in technology, the evolving threat environment, and current industry practices. Rubrik may update this Schedule accordingly in its discretion; however, no such updates will materially reduce the protections set forth herein.

2. Security Audit Reports

Rubrik will provide the Customer, or the Customer's designee, reasonable responses to a security questionnaire designed to assess Rubrik's systems, processes, policies, and records as they relate to the scope of Services provided, not more than once per calendar year. In addition, upon Customer's request, Rubrik will provide a copy of its most recent SOC2 Type II (or successor standard) audit report under confidentiality agreements in place between Rubrik and the Customer.

3. Access Controls

Rubrik will implement appropriate access controls and segregation of duties in the assignment of all critical job functions related to its Processing of Customer Personal Data and the Services provided to the Customer. Rubrik will limit access to Customer Personal Data to personnel using the concept of "least privileged access," meaning individuals are granted access to only those systems that are required to perform their role. Access and privileges for Rubrik personnel will be audited on a quarterly basis as a minimum standard to confirm that concept of "least privileged access" is in place. In addition, Rubrik limits access to those personnel who have been trained in Rubrik's information security practices and are bound by an obligation of confidentiality. Continuous training on new security practices, privacy standards, and organizational policies also occurs on an annual basis to build on Rubrik's employees' body of knowledge. Rubrik maintains processes designed to confirm that each authorization for access to Customer Personal Data has been approved by the appropriate Rubrik management personnel. Access to all systems Processing Customer Personal Data will produce audit logs that provide non-repudiation through verified multi-factor authentication access controls. Audit logs of Rubrik's personnel access of Customer Personal Data will show identification, authentication, and authorization if a member of Rubrik's personnel accesses Customer Personal Data. If access to Customer Personal Data is no longer necessary, Rubrik will remove such personnel's access promptly. Customers should configure and maintain industry-standard security controls to manage access to its infrastructure, devices, equipment, and applications that interface with Rubrik Products. Customer is responsible for securing the Rubrik Products in its environments and for implementing the requirements prescribed in the security hardening documentation provided by Rubrik.

4. Physical and Environmental Security

Rubrik implements and maintains reasonable physical security safeguards for all Rubrik facilities where Customer Personal Data is used, stored, maintained, or accessed. Physical access to Rubrik's third-party data centers is restricted to authorized personnel primarily in technical operations and provisioned upon an authorized request by Rubrik management. A review of the physical access is performed on an annual basis by Rubrik management. Rubrik maintains badging requirements for its onsite personnel and visitors and uses video cameras, video camera footage, and other access control mechanisms to monitor individual physical access to sensitive areas. Rubrik has a facilities security policy that mandates security principles for internal and third-party security staff. Rubrik is committed to protecting all facilities and physical assets that are used during the course of the Agreement.

5. Security and Privacy Awareness training

Rubrik requires its personnel to complete appropriate training for the type of data, systems, and information assets they may use or access. Rubrik will maintain a security and privacy awareness program to address the evolving non-technical security threats. These programs include:

- Security and Privacy teams that provide assistance and guidance to personnel, as appropriate;
- Regular phishing campaigns and training throughout the year for Rubrik's specific user populations; and,

- Annual security and privacy awareness training throughout the organization to cover current and relevant training content for key threats such as phishing, use of privileged access, data security, social engineering and other relevant areas.

6. Penetration Testing and Vulnerability Assessments

Rubrik conducts annual application penetration testing by an independent third-party organization for products and/or applications within the scope of services provided to the Customer. Rubrik will also engage in social engineering penetration testing to test the security posture and awareness of Rubrik's personnel. Further, Rubrik will complete internal and external vulnerability scans of its systems and services periodically, and will update and patch operating systems, applications, firewalls, and all other in-scope systems and applications and remediate or mitigate all such vulnerabilities in accordance with industry standard timelines based on risk.

7. Endpoint Security and Security Protection

Rubrik uses current industry-standard endpoint security measures to protect its internal systems from malware, worms, trap doors, back doors, spyware, malicious logic, trojan horses, time bombs, or other malicious code or programs intentionally designed to damage or enable unauthorized use of or access to Rubrik's IT systems. These endpoint security measures include system monitoring, antivirus software, and endpoint threat detection software.

8. Encryption

To the extent technically feasible, but in all situations where required by applicable law, Rubrik agrees to store and transmit Customer Personal Data in a commercially reasonable format using industry accepted encryption technology. All data transmissions over the internet are encrypted with Transport Layer Security version 1.2. All data at rest is encrypted using Advanced Encryption Standard (AES) 256.

9. Network and Host Security

Rubrik maintains network intrusion detection/prevention, firewalls and security monitoring capabilities that monitor all traffic on Rubrik's corporate network in connection with the Services. Firewalls are used to protect Rubrik's corporate network from the internet and separate the internal network from the internet and Customer's connections. Firewall settings have been configured to deny traffic by default and allow only authorized traffic in accordance with corporate standards. Rubrik reviews and validates firewall rulesets every six months. Network segmentation occurs to prevent Rubrik's corporate network from accessing Customer Personal Data without the Customer's explicit permission.

10. Security Monitoring and Alerting

Rubrik will implement detection tools to prevent data exfiltration through Rubrik provided laptops, workstations and cloud environments. Rubrik will monitor its on-premise and multi-cloud environment 24x7, detect security threats, investigate and respond to security events and incidents.

11. Personal Data Breach Management

Rubrik will maintain at all times during the Term a written security incident response program, including event reporting and escalation procedures, that is used by Rubrik's personnel to report and manage Personal Data Breaches. The incident response program will be regularly tested, including through tabletop exercises involving all parts of the enterprise having responsibilities relating to Personal Data Breach responses. To the extent permitted and in accordance with applicable Data Protection Laws, Rubrik will promptly, but in no later than seventy-two (72) hours, notify the Customer of any confirmed Personal Data Breach. Rubrik will cooperate with Customer's reasonable requests for information regarding any such Personal Data Breach, and Rubrik will provide regular updates, upon request, on the incident and the investigative action and corrective action taken.

12. Business Continuity and Disaster Recovery

While Rubrik continually strives to anticipate and prevent problems from occurring, Rubrik recognizes that the potential exists for unforeseen or unpreventable events and emergencies, such as:

- Utility interruptions
- Labor shortages
- Equipment failures
- Interruption from externally provided products, processes and services
- Recurring natural disasters

- Infrastructure disruptions
- Cyber-attacks on Rubrik or Rubrik's Supplier's systems

In the event of an unforeseen or unpreventable event, Rubrik maintains processes and procedures to minimize the disruption of important and time critical operations, even during an emergency. The Business Continuity Plan guides Rubrik to effectively establish and implement a consistent management and response method so that Rubrik is capable of performing mission-critical functions and services under threats and conditions. Business continuity is an ongoing process and provides for the prevention, preparation, response and recovery for the security of a company. In addition, Rubrik leverages systems and services with high availability and redundancy.

13. Secure Development Practices

Rubrik adheres to security and privacy by design principles and builds those principles into Rubrik's Products such that security and privacy are considered at each stage of development, rather than only at the end of the development process. Rubrik's development practices follow the guidance of OWASP Top 10, SANS Top 20, and CIS Control Benchmarks. Rubrik's formal Software Development Life Cycle (SDLC) policy governs the development, acquisition, configuration, implementation, and maintenance of system components. Management reviews and approves the SDLC policy on an annual basis and the SDLC policy is made available to all personnel.

14. Configuration Management

Changes to any of Rubrik's Products go through a multi-step processes and are reviewed by an internal change control board prior to being deployed into production.

15. Incident Response Policy

Rubrik's Incident Response Policy includes directions to be followed in the event of any action deemed a security incident. This policy includes the roles and responsibilities of personnel assigned to the security incident, the leadership responsibilities, command and control methods, and guidance on developing and implementing corrective action plans.

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

ADDITIONAL SAFEGUARDS ADDENDUM

This Additional Safeguards Addendum ("**Safeguards Addendum**") is in response to the Schrems II case and provides information regarding Rubrik's data access and additional safeguards for Customer's benefit. This Safeguards Addendum supplements and is made part of, but is not in variation or modification of, the Standard Contractual Clauses ("**SCC**").

Rubrik remains committed to securing a strong privacy posture and is actively reviewing global privacy trends and guidelines. Current guidance on the use of SCC as a transfer tool post-Schrems II, including the guidance outlined in the EDPB recommendation 01/2020, makes it clear that each data transfer must be reviewed on a case-by-case basis in order to evaluate the effectiveness of the transfer tool.

Rubrik's assessment of the use of SCC post-Schrems II takes into account the additional safeguards set forth in this Safegaurds Addendum. While Rubrik is a U.S. company and is subject to U.S. laws, to date Rubrik has not received a U.S. law enforcement request regarding any Customer Personal Data. In the event Rubrik receives such a request going forward, Rubrik will abide by the terms of this Safeguards Addendum and the DPA.

1. Challenges to Orders. In addition to Clause 5(d)(i) of the SCC, in the event Rubrik receives an order from a U.S. law enforcement agency for compelled disclosure of any personal data that has been transferred under the SCC, Rubrik shall:

(i) use every reasonable effort to redirect U.S. law enforcement agency to request data directly from Customer;

(ii) promptly notify Customer, unless prohibited under the law applicable to the U.S. law enforcement agency, and, if prohibited from notifying Customer, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and

(iii) use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies or any relevant conflicts with the law of the European Union or applicable Member State law.

For purpose of this Section, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

2. Rubrik's Subprocessors. Rubrik has engaged Subprocessors in order to facilitate the provision of Rubrik products and services, provide product support, analyze product usage and authenticate users. Rubrik's Subprocessors use industry standard organizational and technical measures, including the use of encryption, to protect any Customer Personal Data they may have access to, and Rubrik works with Subprocessors whom Rubrik believes enables Rubrik to comply with its obligations under GDPR. The Subprocessors who may Process Customer Personal Data include:

(i) Cloud infrastructure to support delivery of products and services: Subprocessors such as Microsoft, AWS, Google, Box, ExaVault, Papertrail, and Salesforce provide the infrastructure to facilitate Rubrik's delivery of Rubrik products and services, the filing of support tickets and cases including the upload and transfer for support files and logs. Subprocessors such as Sentry.io aggregate platform logs to proactively identify service issues.

(ii) Collection of data regarding product usage: Subprocessors such as Grafana Labs and Logz collect, aggregate, and measure product metrics and statistics to enable Rubrik to monitor product performance and service health.

(iii) Provision of authentication services: Subprocessors such as Auth0 provide authentication services for Rubrik's Polaris product.

(iv) Provision of support services: Subprocessors such as Spry IQ assist Rubrik with the provision of support services.

All Subprocessors contracted by Rubrik are private companies in sectors that are not heavily government regulated. Subprocessors engaged by Rubrik typically have limited access to Customer Personal Data, such as contact information of Customer's employees who manage Rubrik's accounts, Product usage information such as IP addresses and login events, and information shared with Rubrik as part of support services.

For a complete up to date list of Rubrik's Subprocessors, Customer may visit: https://www.rubrik.com/en/legal/rubrik-subprocessors.

3. Indemnification of Data Subjects. Subject to Sections 4 and 5 of this Safeguards Addendum, Rubrik shall indemnify a data subject for any material or non-material damage to the data subject caused by Rubrik's disclosure of personal data of the data subject that has been transferred under the Standard Contractual Clauses in response to an order from a U.S. law enforcement agency (a "**Relevant Disclosure**"). Notwithstanding the foregoing, Rubrik shall have no obligation to indemnify the data subject under this Section 3 to the extent the data subject has already received compensation for the same damage, whether from Rubrik or otherwise.

4. Conditions of Indemnification. Indemnification under Section 3 of the Safeguards Addendum is conditional upon the data subject establishing, to Rubrik's reasonable satisfaction, that: (i) Rubrik engaged in a Relevant Disclosure; (ii) the

Relevant Disclosure was the basis of an official proceeding by the U.S. law enforcement agency against the data subject; and (iii) the Relevant Disclosure directly caused the data subject to suffer material or non-material damage. The data subject bears the burden of proof with respect to conditions (i) though (iii). Notwithstanding the foregoing, Rubrik shall have no obligation to indemnify the data subject under Section 3 of the Safeguards Addendum if Rubrik establishes that the Relevant Disclosure did not violate its obligations under Chapter V of the GDPR.

5. **Scope of Damages**. Indemnification under Section 3 of the Safeguards Addendum is limited to material and non-material damages as provided in the GDPR and excludes consequential damages and all other damages not resulting from Rubrik's infringement of the GDPR.

6. **Exercise of Rights**. The data subject may only bring a claim under this Safeguards Addendum on an individual basis, and not part of a class, collective, group or representative action. Rights granted to data subjects under this Safeguards Addendum are personal to the data subject and may not be assigned.

7. **Termination**. This Safeguards Addendum shall automatically terminate if the European Commission, a competent Member State supervisory authority, or an EU or competent Member State court approves a different lawful transfer mechanism that would be applicable to the data transfers covered by the SCC (and if such mechanism applies only to some of the data transfers, this Safeguards Addendum will terminate only with respect to those transfers) and that does not require the additional safeguards set forth in this Safeguards Addendum.