

NOTE: THIS DATA PROCESSING AGREEMENT IS VALID ONLY FOR THE ENTITY TO WHICH IT IS DELIVERED BY ACRONIS USING THE DOCUSIGN® ELECTRONIC SIGNATURE SYSTEM AND IS A PARTY TO AN AGREEMENT (DEFINED IN THE PREAMBLE BELOW) DIRECTLY WITH ACRONIS. IF THIS DATA PROCESSING AGREEMENT IS EXECUTED BY ANY OTHER PERSON OR ENTITY, IT IS VOID AND NOT LEGALLY BINDING. ON THE DATE OF ACRONIS' RECEIPT OF THE VALIDLY-EXECUTED DATA PROCESSING AGREEMENT THROUGH THE DOCUSIGN® ELECTRONIC SIGNATURE SYSTEM (THE "**RECEIPT DATE**"), THIS DATA PROCESSING AGREEMENT WILL BE LEGALLY BINDING PROVIDED THAT NO PROVISION IS OVERRITTEN OR MODIFIED OTHER THAN COMPLETING THE MISSING INFORMATION.

ACRONIS CUSTOMER DATA PROCESSING AGREEMENT

This Acronis Data Processing Agreement ("**Addendum**") forms part of all written and electronic agreements (the "**Agreement**") by and between the customer named in the signature block of this Addendum ("**Customer**") and Acronis International GmbH ("**Acronis**"). This Addendum is effective on the date signed by Customer ("**Addendum Effective Date**").

1. Defined Terms. Capitalized terms not defined in the body of this Addendum or the Agreement have the meanings given in this Section 1:

- (i) "**Affiliate**" means an entity that controls, is controlled by or is under common control with Customer or Acronis; for purposes of this defined term; "control" means ownership of more than fifty (50%) percent of the voting stock or other ownership interest in an entity. An Affiliate of Customer is a "**Customer Affiliate**" and an Affiliate of Acronis is an "**Acronis Affiliate**".
- (ii) "**Customer Personal Information**" means the Personal Information submitted by or for Customer as Controller to the Services, the Processing of which is subject to Data Protection Laws, as described in Attachment 1.
- (iii) "**Controller**" means the person or entity who or that that is responsible for and determines the purposes and means of Processing Personal Information under applicable Data Protection Laws.
- (iv) "**Data Protection Laws**" means all laws relating to privacy and data protection and applicable to Processing of Customer Personal Information pursuant to the Agreement, including the California Consumer Privacy Act of 2018 ("**CCPA**") and GDPR, each as amended, repealed, consolidated or replaced from time to time.
- (v) "**Data Subject**" means a natural person to whom Personal Information relates.
- (vi) "**GDPR**" means the General Data Protection 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, as amended or supplemented.
- (vii) "**Personal Information**" means any information relating to an identified or identifiable natural person (or an identified or identifiable entity where information about an entity is protected similarly to the protection afforded to information about an individual); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier.
- (viii) "**Process**" or "**Processing**" means any operation or set of operations performed on Personal Information, whether or not by automated means.
- (ix) "**Processor**" means any person or entity who or that Processes Personal Information for or on behalf of a Controller pursuant to the Agreement.
- (x) "**Restricted Transfer**" means a cross-border transfer of Customer Personal Information that is restricted by Data Protection Laws because the transfer is made to a person or entity located in a jurisdiction with Data Protection Laws that do not require at least the same

level of protection for Customer Personal Information as the jurisdiction from which the Customer Personal Information originates.

- (xi) **“Personal Data Breach”** means any accidental, unlawful or unauthorized access, acquisition, use, modification, disclosure, loss, destruction or other Processing of Customer Personal Information.
- (xii) **“Services”** has the meaning given in the Agreement or, if not defined, the products and/or services provided by Acronis to Customer.
- (xiii) **“Standard Contractual Clauses”** means the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as set forth in Attachment 3.
- (xiv) **“Sub-Processor”** means a Processor engaged by Acronis that Processes Customer Personal Information.

2. Description of Processing. This Addendum applies to Processing of Personal Information related to performing the Agreement.

3. Processing of Customer Personal Information

a. Except as set forth in Section 3b,

- 1) The parties acknowledge and agree that Customer is the Controller or Processor of Customer Personal Information and Acronis is a Processor of Customer Personal Information. Customer acknowledge and agrees that Acronis will engage Sub-Processors. The categories of Data Subjects, categories of Customer Personal Information, subject matter, nature, purpose, duration and location of Processing are described in Attachment 1.
 - 2) Acronis agrees to Process Customer Personal Information for the purposes set forth in the Agreement, as initiated by users of the Services, as instructed by Customer in writing and as required or permitted in compliance with applicable law (**“Processing Instructions”**). Acronis will notify Customer if Acronis believes that the Processing Instructions violate Data Protection Laws or if Acronis cannot comply with the Processing Instructions.
 - 3) Customer hereby represents to Acronis on a continuous basis during the term of the Agreement that (a) Customer obtains all necessary consents and authorizations from Data Subjects required under Data Protection Laws to enable Acronis to Process Customer Personal Information pursuant to the Agreement and to exercise its rights and fulfil its obligations under the Agreement; and (b) in its use of the Services, Customer does not violate the rights of any Data Subject and otherwise Processes Personal information in compliance Data Protection Laws.
 - 4) For Customer Personal Information subject to CCPA, Acronis will not: (a) sell, rent, release, disclose, disseminate, make available, transfer or otherwise communicate Customer Personal Information to a third party for monetary or other valuable consideration; (b) retain, use or disclose Customer Personal Information outside of the direct business relationship between Customer and Acronis; or (c) share, rent, release, disclose, disseminate, make available, transfer or otherwise communicate orally, in writing or by electronic or other means, Customer Personal Information to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration. By execution of this Addendum, Acronis certifies that it understands the specific restrictions contained in this sub-Section 3.a.4.
- b. Acronis and each relevant Acronis Affiliate are separate and independent Controllers and each will comply with the obligations of a Controller under Data Protection Laws when (i) Processing Customer Personal Information to analyze, measure the effectiveness of and improve the Services, to identify and track and record support, to ensure the security and integrity of the Services, for billing and account management and similar internal business purposes (**“Service Management Purposes”**); (ii) as set forth in the Acronis Privacy Statement (for those users of the Services who agree to it); (iii) Processing Personal Information that is generated or derived incidental to providing the Services including data obtained from locally-installed software or endpoints; and (iv) as permitted or required by Data Protection Laws.

4. **Confidentiality and Security Measures.**

- a. Acronis will impose written confidentiality and non-disclosure obligations on all of its personnel that Process Customer Personal Information on Acronis' behalf ("**Acronis Personnel**") and require that Acronis Personnel comply with the relevant requirements of this Addendum.
- b. Acronis will implement and maintain reasonable and appropriate technical, physical and organizational security measures, including the measures set forth in Attachment 2, (collectively, "**Technical and Organizational Security Measures**") to protect Customer Personal Information against unauthorized or unlawful Processing and to ensure a level of security appropriate to the risk. Customer agrees to promptly notify Acronis if Customer becomes aware of any actual or likely misuse of Customer's accounts or account authentication credentials.

5. **Personal Data Breaches.**

- a. Acronis will provide notification ("**Personal Data Breach Notification**") to Customer without undue delay (and within no more than forty eight (48) hours) after Acronis has a reasonable degree of certainty that a Personal Data Breach has occurred. Acronis will deliver the Personal Data Breach Notification to the Customer email address set forth in the signature block or such other contact as Acronis determines appropriate. Customer is responsible for ensuring that Acronis has Customer's up-to-date email address and other contact information for purposes of Personal Data Breach Notification.
- b. After delivering the Personal Data Breach Notification, Acronis will take steps it deems necessary to document, remediate and minimize the effects of the Personal Data Breach with respect to Customer Personal Information and to prevent recurrence. Customer is solely responsible for complying with its obligations under Data Protection Laws with respect to a Personal Data Breach but Acronis shall provide Customer timely assistance and cooperation as reasonably requested by Customer in order for Customer to fulfil those obligations.
- c. Customer understands and agrees that issuance of a Personal Data Breach Notification is not an acknowledgement of Acronis' fault or liability with respect to the Personal Data Breach and that Acronis may make public or notify a third party of any Personal Data Breach as Acronis determines in its discretion is required by law or other legal obligation applicable to Acronis.

6. **Sub-Processing.**

- a. Prior to any disclosure of Customer Personal Information to a Sub-Processor, Acronis shall ensure that all Sub-Processors on the Acronis Sub-Processor List are contractually obligated to protect Customer Personal Information in compliance with Data Protection Laws and consistent with the obligations imposed on Acronis in this Addendum.
- b. Customer agrees that the Sub-Processors and their respective Processing details that are authorized by Customer as of the Addendum Effective Date are set forth at <https://www.acronis.com/compliance/subprocessors/> ("**Acronis Sub-Processor List**").
- c. Customer hereby provides its general authorization to Acronis to appoint new or replacement Sub-Processors. At least fifteen (15) business days prior to any disclosure of Customer Personal Information to a new or replacement Sub-Processor, Acronis shall update Acronis Sub-Processor List to include the new or replacement Sub-Processor. Customer agrees that Acronis will provide notification of any change to the Acronis Sub-Processor List by use of an email to which Customer shall subscribe using the process set forth on <https://www.acronis.com/compliance/subprocessors/#subscription> ("**Sub-Processor Notification**").
- d. Customer may object in writing to a new or replacement Sub-Processor within fifteen (15) days after the date of the Sub-Processor Notification, which objection will provide a reasonably-detailed explanation for the objection. Customer and Acronis will use good-faith efforts to agree on a replacement for the objected-to Sub-Processor. If the parties are unable to agree on the new or replacement Sub-Processor within forty five (45) days after the date of the applicable Sub-Processor Notification, then Customer or Acronis may, upon written notice to the other party, terminate that part of the Agreement that relates to the Services provided by the objected-to Sub-Processor without penalty of any kind.
- e. Acronis is and will remain liable for the acts and omissions of its Sub-Processors to the same extent Acronis would be liable if performing the services of each Sub-Processor directly under the terms of this Addendum.

7. Cross-Border Transfers.

- a. **Restricted Transfers by Customer.** Acronis agrees that it will comply and will ensure that each Acronis Affiliate and Sub-Processor comply with Data Protection Laws and Processing Instructions with respect to any Restricted Transfer of Customer Personal Information. Acronis agrees to work in good faith with Customer to enter into additional contractual provisions with respect to Restricted Transfers as and when required by Data Protection Laws, including as set forth in Attachment 3.
- b. **Restricted Transfers by Acronis.** Acronis will notify Customer prior to any Restricted Transfer by Acronis to a location that is not listed on Attachment 1 as of the Addendum Effective Date. Acronis will ensure that all Restricted Transfers comply with Data Protection Laws, including as set forth in Attachment 3.

8. Cooperation.

- a. Acronis will provide to Customer timely assistance and cooperation as reasonably requested by Customer for Customer to demonstrate its compliance with Data Protection Laws, including mandatory data protection impact assessments and consultations with government authorities.
- b. Unless prohibited by applicable law, Acronis will notify Customer when Acronis receives a valid request, complaint, demand, legal process or order related to Customer Personal Information from a Data Subject, government authority or other third party ("**Request**").
- c. Acronis represents that it has and will maintain appropriate measures to assist Customer in responding to Requests, including processes to authenticate, record, investigate and resolve Requests. Acronis will not respond to a Request unless authorized to do so in writing by Customer or if Acronis believes its response is required by applicable law.
- d. Acronis will use reasonable efforts to limit disclosure of Customer Personal Information in response to a Request and to cooperate with Customer with respect to any action taken with respect to a Request, such as a Customer's efforts to obtain a protective order.
- e. Acronis will promptly notify Customer in writing if Acronis: (i) believes that it is unable to comply with its obligations under this Addendum or Data Protection Laws or cannot comply within a reasonable timeframe; or (ii) becomes aware of any circumstance or change in applicable law that may prevent Acronis from complying with this Addendum.

9. Customer Audits.

- a. Acronis makes available audit reports, documentation and other compliance information ("**Documentation**") for its customers upon request.
- b. If the Documentation does not meet the audit requirements for Acronis' Processing of Customer Personal Information allowed to Customer under Data Protection Laws, then Acronis will allow for and contribute to an audit or inspection relating to Acronis' Processing of Customer Personal Information (each, a "**Customer Audit**"), whether conducted by Customer or a qualified third party mandated by Customer. If a Customer Audit reveals non-compliance with this Addendum or Data Protection Laws, then Acronis will undertake all reasonably necessary and material corrective actions in a timely manner, provide periodic written updates to Customer and notify Customer when corrective actions are complete. Customer shall pay Acronis' reasonable costs for any assistance in connection with a Customer Audit unless such costs are incurred due to Acronis' breach of Data Protection Laws applicable to Acronis.
- c. Unless otherwise required by a government authority, Customer will use best efforts to ensure that a Customer Audit is conducted during normal business hours in a manner that will minimize disruption to Acronis' business operations and that Customer's third-party auditor is not a competitor of Acronis. Customer acknowledges and agrees that a Customer Audit: shall not oblige Acronis to provide or permit access to information concerning Acronis' internal pricing information or relating to other recipients of products or services from Acronis shall be subject to Acronis' reasonable policies, procedures or instructions for the purposes of preserving security and confidentiality.
- d. Prior to a Customer Audit conducted by a third party on Customer's behalf, Customer shall require that all of the third party's personnel execute a confidentiality agreement with Acronis that requires the third party's personnel to (i) use information accessed during the Customer Audit solely for purposes of performing the Customer Audit and (ii) handle that information in accordance with the

same procedures that apply to Acronis' handling of its own confidential information as described in the relevant provision of the Agreement.

10. Personal Information Return or Destruction.

- a. After the end of the performance of its obligations under the Agreement, Acronis will destroy all Customer Personal Information in Acronis' possession or control in its role as a Processor unless otherwise specified in the Agreement and, if Customer requests, provide a written certification upon completion of destruction. Customer acknowledges and agrees that the Services permit Customer to delete Customer Personal Information that is stored in or through in the Services.
- b. If law applicable to Acronis, in its role as a Processor, requires storage of Customer Personal Information in Acronis' possession or control after Acronis has performed its obligations under the Agreement, Acronis will store Customer Personal Information in compliance with the relevant terms of this Addendum until such time as Acronis can anonymize or destroy the Customer Personal Information.

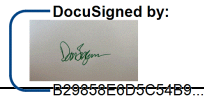
11. General Terms.

- a. **Order of Precedence.** If a term of this Addendum and any term of the Agreement conflict, the terms of this Addendum will prevail with respect to the Processing of Personal Information. If requirements set forth in Attachment 3 for a Restricted Transfer apply in connection with any Restricted Transfer and any term of this Addendum conflicts with requirements in Attachment 3, then the applicable requirements in Attachment 3 will prevail.
- b. **Survival.** Notwithstanding any contrary provision of the Agreement, the obligations of Acronis under this Addendum shall survive for as long as Acronis has access to Customer Personal Information, even if all agreements between Acronis and Customer are expired or terminated.
- c. **Additional Terms.**
 - (i) This Addendum (including all addenda, annexes and attachments incorporated herein) is the complete understanding of the parties in respect of the subject matter hereof and supersedes all prior agreements relating to the same subject matter.
 - (ii) This Addendum will inure to the benefit of and will be binding upon Acronis and Customer and their respective successors and assigns. Customer may not assign or transfer any right or obligation under this Addendum as a whole or in part without the prior written consent of Acronis.
 - (iii) The parties agree to treat the terms of this Addendum as confidential information.
 - (v) If any provision of this Addendum is determined invalid or unenforceable by a court of competent jurisdiction, the remaining provisions will continue in full force. In place of the invalid or unenforceable provision, a provision shall be deemed to be agreed which comes closest to the economic meaning and purpose of the invalid or unenforceable provision.
 - (vi) This Addendum may be executed in any number of counterparts (including delivery via facsimile or electronic mail), all of which will be deemed to be an original but all of which together will constitute one and the same instrument. Each party agrees that any Electronic Signature to this Addendum is intended to authenticate this writing and to have the same force and effect as a manual signature. "**Electronic Signature**" means any electronic sound, symbol or process attached to or logically associated with a record and executed and adopted by either party with the intent to sign.
 - (iv) Except as amended hereby, the Agreement remains in full force and effect in accordance with its terms.

[signature page follows]

SIGNATURE PAGE TO ACRONIS DATA PROCESSING AGREEMENT

CUSTOMER



Signature

Dan Thordahl Jørgensen

Printed Name

Managing Director

Title

dtj@ims.dk

Email Address

Visma IMS A/S, Soren Frichs vej 44D, 8230 Aabyhøj

Customer's Legal Name and Address

25862015

Official registration number (if any) (company number or similar identifier)

9/22/2022

Date Signed

ACRONIS INTERNATIONAL GMBH



Signature

Mikhail Novikov

Printed Name

Geschäftsführer

Title

Data-protection-office@acronis.com

Email Address

Acronis International GmbH, Rheinweg 9,
Schaffhausen

Acronis Legal Name and Address

CHE-113.666.835

Official registration number (if any) (company number or similar identifier)

31 August 2022

Date Signed

Attachment 1

PROCESSING DESCRIPTION

Last updated: Addendum Effective Date

Data Subjects

Customer determines in its sole discretion the Customer Personal Information relating to Data Subjects that is Processed via the Services, which includes Data Subjects authorized by Customer to access and use the Services (including use of Acronis' customer support services) and clients, customers, business partners and vendors of Customer (who are natural persons)

- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's Users authorized by Customer to use the Services

Categories of Personal Information

Customer determines in its sole discretion the categories of Customer Personal Information that is Processed via the Services, including but not limited to name, title, contact information (email, phone, physical business address) of Data Subjects authorized by Customer to access and use the Services, including use of Acronis' customer support services.

Nature of the Processing

The nature of Processing of the Customer Personal Information is the performance of the Services pursuant to the Agreement and for Services Management Purposes. The Processing is on a continuous basis depending on the use of the Services by Customer.

Purpose(s) of Processing

Customer Personal Information is Processed by Acronis for the purpose of providing the products and services specified in the Agreement and otherwise performing the Agreement (including for clarity the Addendum).

Location(s) of the Processing

The location of the Processing of Customer Personal Information is set forth in the Agreement or otherwise as Customer determines.

Duration of the Processing

The duration of the Processing is the term of the Agreement unless agreed in writing by the parties or Processing for Services Management Purposes.

Attachment 2**TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES**

The following Technical and Organizational Security Measures apply to Customer Personal Information Processed by Acronis pursuant to the Agreement.

Description of TOM	Customer Minimum Requirement(s), if any
Measures of pseudonymisation and encryption of Personal Information	<p>Acronis:</p> <ul style="list-style-type: none"> • stores Customer Personal Information (archives and disk and data system backups) using strong encryption techniques with a minimum of Advanced Encryption Standard with a 256-bit key size (AES-256); • encrypts Customer Personal Information and Confidential Information prior to moving and/or using encrypted connections (HTTPS, TLS, FTPS, etc.) to protect the information in transit; • does not use Customer Personal Information in development or test environments unless no alternative exists, in which case Customer Personal Information is anonymized.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	<p>Acronis implements and maintains a comprehensive written information security and compliance program that includes administrative, physical, and technical controls based on ongoing risk assessment (the "Information Security Program"). Acronis' Information Security Program is aligned to recognized international security standards such as ISO 27001 and the National Institute of Standards and Technology (NIST).</p> <p>Acronis conducts periodic risk assessments and reviews at least annually its Information Security Program or whenever a material change in Acronis's business practices may affect the security, confidentiality or integrity of Customer Personal Information. Acronis adjust controls and revises its Information Security Program to address risks identified.</p> <p>Acronis employ high-availability and redundant infrastructure which is designed to minimize associated risks and eliminate single points of failure. Acronis follows the approach of need plus one (N+1) for greater redundancy across all hardware layers of its infrastructure. This helps to ensure that a failure in a hardware-layer component does not affect Acronis' critical infrastructure or Acronis customers.</p> <p>Acronis stores Customer Personal Information through its own software-defined storage solution, using proprietary Acronis CloudRAID technology, which provides additional data redundancy.</p>
Measures for ensuring the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident	<p>Acronis implements appropriate back-up, disaster recovery and business resumption plans to enable recovery from events that impact Acronis's ability to perform in accordance with the Agreement. These plans include defined criteria to determine if a system is critical to the operation of Acronis's business and its prioritization for recovery. Acronis regularly (and no less than annually) tests these plans and makes changes as needed based on its risk assessments and testing to ensure that they are up to date and effective.</p>
Processes for regularly testing, assessing and evaluating the effectiveness of technical and	<p>Acronis undertakes and documents network assessments, change logs and scan results.</p> <p>Acronis performs at least annual penetration tests on Acronis' systems and infrastructure and facilities in accordance with Acronis' policies and industry best practices.</p>

Description of TOM	Customer Minimum Requirement(s), if any
organisational measures in order to ensure the security of the processing	<p>Acronis performs periodic scanning of operating systems, databases, server applications and network devices for vulnerability and configuration compliance.</p> <p>Acronis reviews the security of applications processing Customer Personal Information including automated and manual testing for common vulnerabilities.</p> <p>Acronis maintains a policy for its mobile devices containing Customer Personal Information that, at a minimum, enforces device encryption and prohibits use of blacklisted applications.</p>
Measures for user identification and authorisation	<p>Acronis has strict and granular access control, identification and lockout procedures.</p> <p>Acronis has an established process to review user access to Customer Personal Information, including clearly defined user roles and procedures to approve and justify roles. Acronis enforces access and confidentiality restrictions through disciplinary measures.</p> <p>Acronis has documented password management practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed; monitor repeated attempts to gain access to its information systems using an invalid password; deactivate authentication credentials upon notification that access is no longer needed (e.g. employee termination, project reassignment, etc.); deactivate passwords that are corrupted or inadvertently disclosed; ensure that de-activated or expired identifiers and/or passwords are not granted to other individuals; deactivate authentication credentials when not used; and ensure that where more than one individual has access to its systems containing Customer Personal Information, the individuals have unique identifiers/log-ins (i.e. no shared IDs).</p> <p>Acronis enforces “least privilege” by restricting access to Customer Personal Information to those individuals who require access to perform their job functions and supporting segregation of duties between its environments so that no individual person has access to perform tasks that create a security conflict of interest (e.g. developer/ reviewer, developer/tester).</p>
Measures for the protection of data during transmission	Acronis transmits Customer Personal Information using the following secure protocols and methods: SFTP, TLS, SSH, Site-to-Site VPN with IPSec.
Measures for the protection of data during storage	<p>Acronis stores Customer Personal Information using strong encryption techniques with a minimum of Advanced Encryption Standard with a 256-bit key size (AES-256).</p> <p>Acronis provides its Customers additional encryption capabilities to protect and restrict access to the data, as described at https://www.acronis.com/support/documentation/CyberProtectionService/#encryption.html, as updated from time to time.</p>
Measures for ensuring physical security of locations at which Personal Information are processed	Acronis maintains commercially-reasonable security systems and processes at all Acronis facilities at which information systems that use or store Customer Personal Information are located, such as allowing only authorized individuals to access its facilities.
Measures for ensuring events logging	Acronis maintains logs and records of all processing of Customer Personal Information and records all user activity and actions to Customer Personal Information.
Measures for ensuring system configuration, including default configuration	Acronis ensures that, for as long as Acronis holds Customer Personal Information, Acronis does not and will not purposefully create any process (e.g. “back doors” or similar programming) that does or could permit or facilitate unauthorized access to Customer Personal Information.

Description of TOM	Customer Minimum Requirement(s), if any
	Acronis does not use software or hardware that is past its 'End of Life' in connection with the Services without a mutually agreed risk management process.
Measures for internal IT and IT security governance and management	<p>Acronis identifies dedicated security officer who is responsible for coordinating and monitoring the Information Security Program.</p> <p>Acronis incorporates (and ensures its sub-contractors incorporate) security-by-design principles in software development.</p> <p>Acronis has a risk management program in place to identify, assess and take appropriate actions with respect to risks related to the processing of Customer Personal Information in connection with the Agreement.</p> <p>Acronis promptly take actions to mitigate any actual or potential harm caused by an unauthorized or unlawful Processing of Customer Personal Information.</p> <p>Acronis maintains (and requires Sub-Processors and sub-contractors each maintain) a record of actual and suspected security incidents (including Personal Data Braches), which contains at least a description of the incident, the time period, the consequences of the incident, the name of the reporter and to whom the incident was reported, and the process for recovering data, and otherwise complies with the requirements of the Agreement.</p>
Measures for certification/assurance of processes and products	<p>If Customer requests, Acronis provides to Customer no less than annually valid ISO 27001 or SOC 2 reports and those of its Sub-Processors, if available.</p> <p>If Acronis or a Sub-Processor does not have a valid ISO 27001 or SOC 2 report, Acronis provides to Customer documentation that demonstrates that Acronis or the applicable Sub-Processors conform to an industry-recognized cybersecurity framework.</p>
Measures for ensuring data minimisation	<p>Acronis limits access to Customer Personal Information in its systems to only that data minimally necessary to perform the services.</p> <p>Acronis conducts data protection impact assessments to ensure that the Customer Personal Information collected by or on behalf of Customer is limited to what is necessary in relation to the purposes for Processing. Acronis' data minimization measures are accompanied by technical measures to ensure that Customer Personal Information is not subject to unauthorized access.</p> <p>Acronis conducts regular audits and strong disciplinary measures to monitor and enforce compliance with the data minimization measures, including for cross-border transfers.</p>
Measures for ensuring data quality	<p>Acronis uses up-to-date web application firewalls (WAF), which include instant protection against SQL injection, cross-site scripting, unauthorized resource access, remote file inclusion, and other Open Web Application Security (OWASP) threats.</p> <p>Acronis system interfaces go through input validation testing which prevents improperly formed data from entering an information system.</p>
Measures for ensuring accountability	<p>Acronis compiles and maintains all Processing Instructions and ensures that they are accessible to all Acronis Personnel, including Sub-Processors.</p> <p>Acronis trains Acronis Personnel about privacy and security principles, policies and procedures and their respective roles and possible consequences of breaching the principles, policies and procedures and applicable laws. Acronis maintains records of training attendance.</p>

Description of TOM	Customer Minimum Requirement(s), if any
Measures for allowing for data portability, processing restrictions, erasure and consent	<p>Acronis maintains commercially reasonable and documented procedures for complying with Data Subjects' exercise of their privacy rights, including ensuring that privacy rights requests are timely and effectively addressed.</p> <p>Acronis maintains records of the date and time of requests, involvement of Sub-Processors (if applicable), Acronis' response to the request (whether requests are denied) and evidence of when Customer was informed and Customer's review and approval.</p> <p>Acronis posts the complete and current Acronis Privacy Statement as appropriate when Acronis collects Customer Personal information from Data Subjects.</p>

Attachment 3

ADDITIONAL TERMS APPLICABLE TO RESTRICTED TRANSFERS

Acronis agrees to the following contractual clauses and other requirements with respect to Restricted Transfers. Customer's signature on this Addendum shall be deemed to constitute Customer's signature and acceptance of the relevant contractual terms set forth below and incorporated into this Addendum and the Agreement. Accordingly, the parties to the relevant contractual terms shall be the same as the parties to the Addendum.

A. FOR RESTRICTED TRANSFERS SUBJECT TO GDPR

When Customer or a Customer Affiliate as a Controller ("data exporter") makes a Restricted Transfer of Customer Personal Information subject to GDPR to Acronis or an Acronis Affiliate as a Processor (each, a "data importer") who or that is located in a non-EEA jurisdiction which is not covered by an adequacy decision under GDPR Article 45 and the data importer's Processing of Customer Personal Information is not otherwise subject to the GDPR, then each data exporter and data importer shall complete and execute the Standard Contractual Clauses (*Module Two*).

When Customer or a Customer Affiliate as a Processor ("data exporter") makes a Restricted Transfer of Customer Personal Information subject to GDPR to Acronis or an Acronis Affiliate as a Processor (each, a "data importer") who or that is located in a non-EEA jurisdiction which is not covered by an adequacy decision under GDPR Article 45 and the data importer's Processing of Customer Personal Information is not otherwise subject to the GDPR, then each data exporter and data importer shall complete and execute the Standard Contractual Clauses (*Module Three*).

The parties agree to complete the Standard Contractual Clauses as follows:

- 1) Clause 7 (Docking Clause) of the Standard Contractual Clauses (*Module Two* and *Module Three*) does not apply.
- 2) Before disclosing a copy of the Standard Contractual Clauses (*Module Two* and *Module Three*) per Clause 8.3, the disclosing party must use commercially-reasonable efforts to redact all commercial terms but will provide a meaningful summary if the data subject would otherwise not be able to understand the content or exercise his/her rights as a result of the redaction.
- 3) Per Clause 9(a) of the Standard Contractual Clauses (*Module Two* and *Module Three*), the data exporter hereby provides a general authorization (Option 2) for the Processing of Customer Personal Information as set forth in the Addendum. The data importer shall specifically inform the data exporter in writing of any intended change to Sub-Processors as set forth in the Addendum.
- 4) The optional provision in Clause 11(a) (Redress) of the Standard Contractual Clauses (*Module Two* and *Module Three*) does not apply.
- 5) The parties choose Option 1 of Clause 17 of the Standard Contractual Clauses (*Module Two* and *Module Three*), and agree that the law of the EU Member State in which the data exporter is established will govern and per Clause 18(b) disputes arising under the Standard Contractual Clauses (*Module Two* and *Module Three*) shall be resolved in the courts of the same EU Member State.
- 6) Attachment 2 to this Addendum shall serve as ANNEX II to the Standard Contractual Clauses (*Module Two* and *Module Three*).
- 7) The Acronis Sub-Processor List described in Section 6a of the Addendum shall serve as the list of Sub-Processors for ANNEX III to the Standard Contractual Clauses (*Module Two* and *Module Three*).
- 8) Attachment 1 to this Addendum includes the description of Processing for ANNEX 1 and ANNEX III to the Standard Contractual Clauses (*Module Two* and *Module Three*).
- 9) Nothing in the Standard Contractual Clauses shall make data importer responsible for the implementation and maintenance of any security controls relating to the equipment or

- information systems of data exporter. All such controls shall be the responsibility of data exporter except as otherwise expressly agreed in the Agreement.
- 10) All audits by data exporter specified in the Standard Contractual Clauses (*Module Two* and *Module Three*) shall be carried out in accordance with the terms of the Addendum unless otherwise expressly required by Data Protection Laws.
 - 11) The parties agree that Acronis shall provide the certification of deletion of personal data described in clauses 8.5 and 16(d) of the Standard Contractual only upon Customer's written request.
 - 12) Any limitations of liability, including limitations on indemnities, set forth in the Agreement apply with respect to liability arising under the Standard Contractual Clauses.

If applicable, the legal name of the Customer entity acting as data exporter under the Standard Contractual Clauses (*Module Two* and *Module Three*) is _____.

The Standard Contractual Clauses also will apply to a Restricted Transfer by Customer or a Customer Affiliate to Acronis or an Acronis Affiliate or when the Customer Personal Information is not subject to GDPR but the competent government authority for that Customer Personal Information authorizes the use of the Standard Contractual Clauses.

B. FOR RESTRICTED TRANSFERS SUBJECT TO THE PRIVACY LAWS OF ARGENTINA

For a Restricted Transfer subject to the Data Protection Laws of Argentina, Customer and Acronis hereby agree to the model contract set forth in the Annexes to [Regulation No. 60-E/2016](#).

Jurisdictions considered to provide an adequate level of data protection under the Data Protection Laws of Argentina are set forth at <http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.ht> and include the EU Member States and members of the European Economic Area, Switzerland, Guernsey, Jersey, the Isle of Man, the Faroe Islands, Canada (only for the private sector), the Principality of Andorra, New Zealand, the Republic of Uruguay, the State of Israel (only for data that is automated processing), and the United Kingdom of Great Britain and Northern Ireland. An international transfer of personal information to any other jurisdiction requires use of the model contract set forth in the Annexes to [Regulation No. 60-E/2016](#).

If applicable, the legal name of the Customer entity acting as data exporter under the model contract set forth in the Annexes to [Regulation No. 60-E/2016](#) is _____.

C. FOR RESTRICTED TRANSFERS SUBJECT TO THE PRIVACY LAWS OF SWITZERLAND

For Restricted Transfers subject exclusively to the Data Protection Laws of Switzerland ("**Swiss Data Protection Law**"), (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law have the same meaning as the equivalent reference in Swiss Data Protection Law and any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established refers to an obligation under Swiss Data Protection Law; (ii) if Customer is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Law or the relevant data transfer is governed by Swiss Data Protection Laws, the Swiss Federal Data Protection and Information Commissioner is the competent supervisory authority for a Restricted Transfer governed by Swiss Data Protection Law pursuant to Clause 13 of the Standard Contractual Clauses; (iii) for any Data Subject who resides in Switzerland, the courts of Switzerland are an alternative place of jurisdiction for dispute resolution; (iv) the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity when such information is protected similarly as Personal Data is protected to the extent expressly required by Swiss Data Protection Law.

If applicable, the legal name of the Customer entity acting as data exporter under Swiss Data Protection Law is _____.

D. FOR RESTRICTED TRANSFERS SUBJECT TO THE PRIVACY LAWS OF UNITED KINGDOM

For Restricted Transfers subject to the Data Protection Laws of the United Kingdom, Customer and Acronis hereby agree to the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0) (**UK Addendum**) as follows:

Part 1: Tables

Table 1: Parties

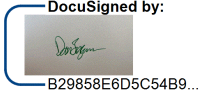

Start date	Addendum Effective Date	
The Parties	Customer as Exporter (which sends the Restricted Transfer)	Acronis as Importer (which receives the Restricted Transfer)
Parties' details	As set forth in the Acronis Customer Data Processing Addendum and Agreement	As set forth in the Acronis Customer Data Processing Addendum and Agreement
Key Contact	As set forth in the Acronis Customer Data Processing Addendum and Agreement	As set forth in the Acronis Customer Data Processing Addendum and Agreement
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	<p><input type="checkbox"/> The version of the Approved EU SCCs which this UK Addendum is appended to, detailed below, including the Appendix Information:</p> <p>Date: <input type="text"/></p> <p>Reference (if any): <input type="text"/></p> <p>Other identifier (if any): <input type="text"/></p> <p>Or</p> <p><input checked="" type="checkbox"/> the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this UK Addendum:</p>
-------------------------	---

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	N/A					
2	SEE ATTACHMENT 3.A TO THE ADDENDUM.					
3	SEE ATTACHMENT 3.A TO THE ADDENDUM.					
4	N/A					

Table 3: Appendix Information

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

Annex 1A: List of Parties: The Parties are set forth in Table 1 to this UK Addendum.

Annex 1B: Description of Transfer: Attachment 1 to the Addendum includes the description of Processing for this UK Addendum.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Attachment 2 to the Addendum shall serve as ANNEX II to this UK Addendum.

Annex III: List of Sub processors (Modules 2 and 3 only): The Acronis Sub-Processor List described in Section 6a of the Addendum shall serve as the list of Sub-Processors for ANNEX III to this UK Addendum.

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Ending this UK Addendum when the Approved UK Addendum changes	Which Parties may end this UK Addendum as set out in Section 19: <input checked="" type="checkbox"/> Importer <input type="checkbox"/> Exporter <input type="checkbox"/> neither Party
--	---

Part 2: Mandatory Clauses

Entering into this UK Addendum

- Each Party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other Party also agreeing to be bound by this UK Addendum.
- Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this UK Addendum in any way

that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum . Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this UK Addendum

3. Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this UK Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this UK Addendum, UK Data Protection Laws applies.
7. If the meaning of this UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this UK Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this UK Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this UK Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This UK Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
 - a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
 - b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
 - c. this UK Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
 - a. References to the “Clauses” means this UK Addendum, incorporating the Addendum EU SCCs;
 - b. In Clause 2, delete the words:

“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”;
 - c. Clause 6 (Description of the transfer(s)) is replaced with:

“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;
 - d. Clause 8.7(i) of Module 1 is replaced with:

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;
 - e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”
 - f. References to “Regulation (EU) 2016/679”, “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)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
 - g. References to Regulation (EU) 2018/1725 are removed;
 - h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
 - i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
 - j. Clause 13(a) and Part C of Annex I are not used;
 - k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
 - l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”

n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this UK Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
18. From time to time, the ICO may issue a revised Approved Addendum which:
 - a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
 - b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
 - a its direct costs of performing its obligations under the Addendum; and/or
 - b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this UK Addendum , but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.
--------------------------	---

E. FOR RESTRICTED TRANSFERS SUBJECT TO THE PRIVACY LAWS OF Japan.

To the extent that Acronis Processes Customer Personal Information of Data Subjects located in Japan, Customer authorizes Acronis to transfer that Customer Personal Information to a third party in a jurisdiction outside of Japan only if: (i) the jurisdiction in which the recipient is located has a legal system that is deemed equivalent to the Japanese data protection regime as designated by the Personal Information Protection Commission (“PPC”); (ii) the recipient has adequate measures for the protection of Customer Personal Information, as specified by the PPC; (iii) the Data Subject consents to the International Data Transfer; or (iv) the International Data Transfer is otherwise permitted under Japan’s Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in thereafter) (“APPI”). When providing Customer Personal Information to a Subprocessor or other third party outside Japan, Acronis shall, when required by the PPC (i) take necessary measures as specified by the PPC to ensure the continuous implementation of measures equivalent to the terms of this DPA by such third party and provide information about such necessary measures to the relevant Data Subject upon his/her request; and (ii) provide information regarding the Personal Information protection system in the jurisdiction in which the third party is located, the measures taken by the third party to protect Customer Personal Information, and other relevant information to the Data Subject in advance, as required by the PPC.