arcserve

DATA PROTECTION AGREEMENT
FOR ARCSERVE CLOUD SERVICES

1. Scope, Order of Precedence and Term

1.1. This data protection agreement (the "Data Protection Agreement") applies to Arcserve's Processing of Personal Data as part of Arcserve's provision of Arcserve Cloud Services ("Cloud Services"). The Cloud Services are described in (i) the applicable order for Cloud Services, (ii) the applicable Agreement or other applicable master agreement (including all exhibits thereto) by and between You and Arcserve in which this Data Protection Agreement is referenced, (iii) Arcserve's Acceptable Use Policy and/or (iv) the definitive technical description of the Cloud Services provided by Arcserve (i, ii, iii and iv collectively the "Cloud Services Agreement").

1.2. Unless otherwise expressly stated in the order, this version of the Data Protection Agreement is incorporated into and subject to the terms of the Cloud Services Agreement and shall be effective and remain in force for so long as Arcserve continues to provide any Cloud Services.

1.3. Except as expressly stated otherwise in this Data Protection Agreement or the order, in the event of any conflict between the terms of the Cloud Services Agreement, including any policies or schedules referenced therein, and the terms of this Data Protection Agreement, the relevant terms of this Data Protection Agreement shall take precedence.

2. Definitions

2.1. "Applicable Data Protection Law" means (i) Regulation (EU) 2016/679 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, applicable as of May 25, 2018; and (ii) any other data privacy or data protection law or regulation that applies to the Processing of Personal Data under this Data Protection Agreement;

2.2. "You" means the customer entity that has executed the order;

2.3. "Data Subject", "Data Protection Impact Assessments", "Process/Processing", "Supervisory Authority", "Controller", "Processor" and" (or any of the equivalent terms) have the meaning set forth under Applicable Data Protection Law;

2.4. "EU Model Clauses" means the standard contractual clauses annexed to the EU Commission Decision 2010/87/EU of 5 February 2010 for the Transfer of Personal Data to Processors established in Third Countries under the Directive 95/46/EC, or any successor standard contractual clauses that may be adopted pursuant to an EU Commission decision;

2.5. "Arcserve" means the Arcserve Affiliate that has executed the order;

2.6. "Arcserve Affiliate(s)" means the subsidiar(y)(ies) of Arcserve (USA) LLC that may assist in the performance of the Cloud Services as set forth in Section 3.3;

2.7. "Personal Data" means any information relating to a Data Subject that Arcserve may Process

on Your behalf as part of the Cloud Services;

2.8 "Third Party Subprocessor" means a third party subcontractor, other than an Arcserve Affiliate, engaged by Arcserve and which may Process Personal Data as set forth in Section 3.3.

Other capitalized terms have the definitions provided for them in the Cloud Services Agreement or as otherwise specified below.

3. Controller and Processor of Personal Data and Purpose of Processing

3.1. You are and will at all times remain the Controller of the Personal Data Processed by Arcserve under the Cloud Services Agreement. You are responsible for compliance with Your obligations as a Controller under Applicable Data Protection Law, in particular for justification of any transmission of Personal Data to Arcserve (including providing any required notices and obtaining any required consents and/or authorizations, or otherwise securing an appropriate legal basis under Applicable Data Protection Law), and for Your decisions and actions concerning the Processing of such Personal Data.

3.2. Arcserve is and will at all times remain a Processor with regard to the Personal Data provided by You to Arcserve under the Cloud Services Agreement. Arcserve is responsible for compliance with its obligations under this Data Protection Agreement and for compliance with its obligations as a Processor under Applicable Data Protections Law.

3.3 Arcserve and any persons acting under the authority of Arcserve, including any Arcserve Affiliates and Third Party Subprocessors as set forth in Section 8, will Process Personal Data solely for the purpose of (i) providing the Cloud Services in accordance with the Cloud Services Agreement and this Data Protection Agreement (ii) complying with Your documented written instructions in accordance with Section 5, or (iii) complying with Arcserve's regulatory obligations in accordance with Section 13.

4. Categories of Personal Data and Data Subjects

4.1. In order to perform the Cloud Services and depending on the Cloud Services You have ordered, Arcserve may Process some or all of the following categories of Personal Data: personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords; information concerning family, lifestyle and social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children; employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, social security details and business contact details; financial details; goods and services provided; unique IDs collected from mobile devices, network carriers or data providers, IP addresses, and online behavior and interest data.

4.2. Categories of Data Subjects whose Personal Data may be Processed in order to perform the Cloud Services may include, among others, Your representatives and end users, such as Your employees, job applicants, contractors, collaborators, partners, suppliers, customers and clients.

4.3 Additional categories of Personal Data and/or Data Subjects may be described in the Cloud Services Agreement. Unless otherwise specified in Your order (including in the Service Specifications), Your Content may not include any sensitive or special personal data that imposes specific data security or data protection obligations on Arcserve in addition to or different from those specified in the Service Specifications.

5. Your Instructions

5.1. Arcserve will Process Personal Data on Your written instructions as specified in the Cloud Services Agreement and this Data Protection Agreement, including instructions regarding data transfers as set forth in Section 7.

5.2. You may provide additional instructions in writing to Arcserve with regard to Processing of Personal Data in accordance with Applicable Data Protection Law. Arcserve will comply with all such instructions to the extent necessary for Arcserve to (i) comply with its Processor obligations under Applicable Data Protection Law; or (ii) assist You to comply with Your Controller obligations under Applicable Data Protection Law relevant to Your use of the Cloud Services, including assistance with notifying Personal Data breaches as set forth in Section 11, Data Subject requests as set forth in Section 6, and Data Protection Impact Assessments (DPIAs).

5.3. To the extent required by Applicable Data Protection Law, Arcserve will immediately inform You if, in its opinion, Your instruction infringes Applicable Data Protection Law. You acknowledge and agree that Arcserve is not responsible for performing legal research and/or for providing legal advice to You.

5.4. Without prejudice to Arcserve's obligations under this Section 5, the parties will negotiate in good faith with respect to any charges or fees that may be incurred by Arcserve to comply with instructions with regard to the Processing of Personal Data that require the use of resources different from or in addition to those required for the provision of the Cloud Services.

6. Rights of Data Subjects

6.1. Arcserve will grant You electronic access to Your Cloud Services environment that holds Personal Data to enable You to respond to requests from Data Subjects to exercise their rights under Applicable Data Protection Law, including requests to access, delete or erase, restrict, rectify, receive and transmit, block access to or object to Processing of specific Personal Data or sets of Personal Data.

6.2. To the extent such electronic access is not available to You, You can submit a "service request" via https://support.arcserve.com or other applicable primary support tool provided for the Services), and provide detailed written instructions to Arcserve (including the Personal Data necessary to identify the Data Subject) on how to assist with such Data Subject requests in relation to Personal Data held in Your Cloud Services environment. Arcserve will promptly follow such instructions. If applicable, the parties will negotiate in good faith with respect to any charges or fees that may be incurred by Arcserve to comply with instructions that require the use of resources

different from or in addition to those required for the provision of the Cloud Services.

6.3. If Arcserve directly receives any Data Subject requests regarding Personal Data, it will promptly pass on such requests to You without responding to the Data Subject if the Data Subject identifies You as the Data Controller. If the Data Subject does not identify You, Arcserve will instruct the Data Subject to contact the entity responsible for collecting their Personal Data.

7. Personal Data Transfers

7.1. Personal Data held in Your Cloud Services environment will be hosted in the data center region specified in the Cloud Services Agreement or otherwise selected by You. Arcserve will not migrate Your Cloud Services environment to a different data center region without Your prior written authorization.

7.2. Without prejudice to Section 7.1, Arcserve may access and Process Personal Data on a global basis as necessary to perform the Cloud Services, including for IT security purposes, maintenance and performance of the Cloud Services and related infrastructure, Cloud Services technical support and Cloud Service change management.

7.3. To the extent such global access involves a transfer of Personal Data originating from the European Economic Area ("EEA") or Switzerland to Arcserve Affiliates or Third Party Subprocessors located in countries outside the EEA or Switzerland that have not received a binding adequacy decision by the European Commission or by a competent national EEA data protection authority, such transfers are subject to (i) the terms of the EU Model Clauses incorporated into this Data Protection Agreement by reference; or (ii) other binding and appropriate transfer mechanisms that provide an adequate level of protection in compliance with Applicable Data Protection Law, such as approved Binding Corporate Rules for Processors. For the purposes of the EU Model Clauses, You and Arcserve agree that (i) You will act as the data exporter on Your own behalf and on behalf of any of Your entities, (ii) Arcserve will act on its own behalf and/or on behalf of the relevant Arcserve Affiliates as the data importers, (iii) any Third Party Subprocessors will act as 'subcontractors' pursuant to Clause 11 of the EU Model Clauses.

7.4. To the extent such global access involves a transfer of Personal Data originating from Argentina to Arcserve Affiliates or Third Party Subprocessors located in countries outside Argentina that have not received a binding adequacy decision by the National Directorate for Personal Data Protection, such transfers are subject to (i) the terms of the Argentinean Model Clauses incorporated into this Data Protection Agreement by reference; or (ii) other binding and appropriate transfer mechanisms that provide an adequate level of protection in compliance with Applicable Data Protection Law.

7.5. Transfers of Personal Data originating from locations outside of the EEA, Switzerland or Argentina to Arcserve Affiliates or Third Party Subprocessors are subject to the terms of the Arcserve Privacy Policy https://www.arcserve.com/about/privacy/, which requires all transfers of Personal Data to be made in compliance with all applicable Arcserve security and data privacy policies and standards; and (ii) for Third Party Subprocessors, the terms of the relevant Arcserve Third Party Subprocessor agreement incorporating security and data privacy requirements consistent with the relevant requirements of this Data Protection Agreement.

7.6. The terms of this Data Protection Agreement shall be read in conjunction with the EU Model Clauses, and other applicable transfer mechanisms pursuant to this Section 7.

8. Arcserve Affiliates and Third Party Subprocessors

8.1. Subject to the terms and restrictions specified in Sections 3.3, 7 and 8, You agree that Arcserve may engage Arcserve Affiliates and Third Party Subprocessors to assist in the performance of the Cloud Services.

8.2. Arcserve will, in response to Your request, advise you as to Third Party Subprocessors or Arcserve Affiliates that may Process Personal Data.

8.3. Within fourteen (14) calendar days of Arcserve providing such notice to You, You may object to the intended involvement of a Third Party Subprocessor or Arcserve Affiliate in the performance of the Cloud Services, providing objective justifiable grounds related to the ability of such Third Party Subprocessor or Arcserve Affiliate to adequately protect Personal Data in accordance with this Data Protection Agreement or Applicable Data Protection Law in writing by submitting a "service request" via My Arcserve Support, or other applicable primary support tool provided for the Services. In the event Your objection is justified, You and Arcserve will work together in good faith to find a mutually acceptable resolution to address such objection, including but not limited to reviewing additional documentation supporting the Third Party Subprocessors' or Arcserve Affiliate's compliance with this Data Protection Agreement or Applicable Data Protection Law, or delivering the Cloud Services without the involvement of such Third Party Subprocessor. To the extent You and Arcserve do not reach a mutually acceptable resolution within a reasonable timeframe, You shall have the right to terminate the relevant Cloud Services (i) upon serving prior notice in accordance with the terms of the Cloud Services Agreement; (ii) without liability to You and Arcserve and (iii) without relieving You from Your payment obligations under the Cloud Services Agreement up to the date of termination. If the termination in accordance with this Section 8.3 only pertains to a portion of Cloud Services under an order, You will enter into an amendment or replacement order to reflect such partial termination.

8.4. The Arcserve Affiliates and Third Party Subprocessors are required to abide by the same level of data protection and security as Arcserve under this Data Protection Agreement as applicable to their Processing of Personal Data. You may request that Arcserve audit a Third Party Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist customer in obtaining a third-party audit report concerning the Third Party Subprocessor's operations) to verify compliance with such obligations. You will also be entitled, upon written request, to receive copies of the relevant privacy and security terms of Arcserve's agreement with any Third Party Subprocessors and Arcserve Affiliates that may Process Personal Data.

8.5. Arcserve remains responsible at all times for the performance of the Arcserve Affiliates' and Third Party Subprocessors' obligations in compliance with the terms of this Data Protection Agreement and Applicable Data Protection Law.

9. Technical and Organizational Measures, and Confidentiality of Processing

9.1. Arcserve has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Data. These measures take into account the nature, scope and purposes of Processing as specified in this Data Protection Agreement, and are intended to protect Personal Data against the risks inherent to the Processing of Personal Data in the performance of the Cloud Services, in particular risks from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

9.2. In particular, Arcserve has implemented the physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures specified in the Service Specifications. You are advised to carefully review the applicable Service Specifications to understand which specific security measures and practices apply to the particular Cloud Services ordered by You, and to ensure that these measures and practices are appropriate for the Processing of Personal Data pursuant to this Data Protection Agreement.

9.3. All Arcserve and Arcserve Affiliate staff, as well as any Third Party Subprocessors that may have access to Personal Data are subject to appropriate confidentiality arrangements.

10. Audit Rights and Cooperation with You and Your Supervisory Authorities

10.1. You may audit Arcserve's compliance with its obligations under this Data Protection Agreement up to once per year. In addition, to the extent required by Applicable Data Protection Law, including where mandated by Your Supervisory Authority, You or Your Supervisory Authority may perform more frequent audits, including inspections of the Cloud Service data center facility that Processes Personal Data. Arcserve will contribute to such audits by providing You or Your Supervisory Authority with the information and assistance reasonably necessary to conduct the audit, including any relevant records of Processing activities applicable to the Cloud Services ordered by You.

10.2. If a third party is to conduct the audit, the third party must be mutually agreed to by You and Arcserve (except if such Third Party is a competent Supervisory Authority). Arcserve will not unreasonably withhold its consent to a third party auditor requested by You. The third party must execute a written confidentiality agreement acceptable to Arcserve or otherwise be bound by a statutory confidentiality obligation before conducting the audit.

10.3. To request an audit, You must submit a detailed proposed audit plan to Arcserve at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Arcserve will review the proposed audit plan and provide You with any concerns or questions (for example, any request for information that could compromise Arcserve security, privacy, employment or other relevant policies). Arcserve will work cooperatively with You to agree on a final audit plan.

10.4. If the requested audit scope is addressed in a SSAE 16/ISAE 3402 Type 2, ISO, NIST, PCI DSS, HIPAA or similar audit report issued by a qualified third party auditor within the prior twelve months and Arcserve provides such report to You confirming there are no known material changes

in the controls audited, You agree to accept the findings presented in the third party audit report in lieu of requesting an audit of the same controls covered by the report.

10.5. The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Arcserve's health and safety or other relevant policies and may not unreasonably interfere with Arcserve business activities.

10.6. You will provide Arcserve any audit reports generated in connection with any audit under this Section 10, unless prohibited by Applicable Data Protection Law or otherwise instructed by a Supervisory Authority. You may use the audit reports only for the purposes of meeting Your regulatory audit requirements and/or confirming compliance with the requirements of this Data Protection Agreement. The audit reports are Confidential Information of the parties under the terms of the Cloud Services Agreement.

10.7. Any audits are at Your expense. The parties will negotiate in good faith with respect to any charges or fees that may be incurred by Arcserve to provide assistance with an audit that requires the use of resources different from or in addition to those required for the provision of the Cloud Services.

11. Incident Management and Personal Data Breach Notification

11.1. Arcserve promptly evaluates and responds to incidents that create suspicion of or indicate unauthorized access to or Processing of Personal Data ("Incident"). All Arcserve and Arcserve Affiliates staff that have access to or Process Personal Data are instructed on responding to Incidents, including prompt internal reporting, escalation procedures, and chain of custody practices to secure relevant evidence. Arcserve's agreements with Third Party Subprocessors, contain similar Incident reporting obligations.

11.2. In order to address an Incident, Arcserve defines escalation paths and response teams involving internal functions such as Information Security and Legal. The goal of Arcserve's Incident response will be to restore the confidentiality, integrity, and availability of the Cloud Services environment and the Personal Data that may be contained therein, and to establish root causes and remediation steps. Depending on the nature and scope of the Incident, Arcserve may also involve and work with You and outside law enforcement to respond to the Incident.

11.3. To the extent Arcserve becomes aware and determines that an Incident qualifies as a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed on Arcserve systems or the Cloud Services environment that compromises the security, confidentiality or integrity of such Personal Data ("Personal Data Breach"), Arcserve will inform You of such Personal Data Breach without undue delay but at the latest within 72 hours.

11.4. Arcserve will take reasonable measures designed to identify the root cause(s) of the Personal Data Breach, mitigate any possible adverse effects and prevent a recurrence. As information regarding the Personal Data Breach is collected or otherwise reasonably becomes available to Arcserve and to the extent permitted by law, Arcserve will provide You with (i) a

description of the nature and reasonably anticipated consequences of the Personal Data Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; (iii) where possible, the categories of Personal Data and Data Subjects including an approximate number of Personal Data records and Data Subjects that were the subject of the Personal Data Breach; and (iv) other information concerning the Personal Data Breach reasonably known or available to Arcserve that You may be required to disclose to a Supervisory Authority or affected Data Subject(s).

11.5. Unless otherwise required under Applicable Data Protection Law, the parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected Data Subjects and/or notices to the relevant Supervisory Authorities.

12. Return and Deletion of Personal Data upon Termination of Cloud Services

12.1. Following termination of the Cloud Services, Arcserve will return or otherwise make available for retrieval Your Personal Data then available in Your Cloud Services environment, unless otherwise expressly stated in the Service Specifications. For Cloud Services for which no data retrieval functionality is provided by Arcserve as part of the Cloud Services, You are advised to take appropriate action to back up or otherwise store separately any Personal Data while the production Cloud Services environment is still active prior totermination.

12.2. Upon termination of the Cloud Services or upon expiry of the retrieval period following termination of the Cloud Services (if available), Arcserve will promptly delete all copies of Personal Data from the Cloud Services environment by rendering such Personal Data unrecoverable, except as may be required by law. Data deletion capabilities of the parties are described in more detail in the Service Specifications.

13. Legally Required Disclosure Requests

13.1. If Arcserve receives any subpoena, judicial, administrative or arbitral order of an executive or administrative agency, regulatory agency, or other governmental authority which relates to the Processing of Personal Data ("Disclosure Request"), it will promptly pass on such Disclosure Request to You without responding to it, unless otherwise required by applicable law (including to provide an acknowledgement of receipt to the authority that made the Disclosure Request).

13.2. At Your request, Arcserve will provide You with reasonable information in its possession that may be responsive to the Disclosure Request and any assistance reasonably required for You to respond to the Disclosure Request in a timely manner.

14. Compliance Team

14.1. Arcserve has created a compliance team which can be contacted at gdpr@arcserve.com.

14.2. If You have appointed a Data Protection Officer, You may request Arcserve to include the contact details of Your Data Protection Officer in the order, or may subsequently communicate the relevant contact details to Arcserve at gdpr@arcserve.com