

## Data Processing Addendum

This Data Processing Addendum (the “**DPA**”) shall be supplemental to any valid licensing, subscription, support or service agreement (together hereinafter “**Agreement**”) between the applicable AvePoint entity as identified in the Agreement (hereinafter referred to as “**AvePoint**”) and your company or entity (“**Customer**”). This DPA is entered into between AvePoint and Customer as of the effective date of the Agreement (the “**Effective Date**”) and shall only apply if and to the extent that AvePoint Processes Personal Data as a Processor on behalf of the Customer or a Customer Affiliate as a Controller as defined below and in the Agreement.

The purpose of this DPA is to ensure such Processing is conducted in accordance with applicable laws, including Data Protection Legislation (as defined below). This DPA shall not be applicable to further aspects of the parties’ business relationship.

### 1 Definitions

For purposes of this DPA,

- 1.1 “**Affiliate**” has the same meaning ascribed to it in the Agreement and, if not defined in the Agreement, means, with respect to any Person, any other Person that controls or is Controlled by or under common Control with such Person; provided, that a Person shall be deemed to be an Affiliate only so long as such Control exists. For the purposes of this definition, “**Person**” means any individual, corporation, partnership, or limited liability company; and “**Control**”, when used with respect to any Person, means ownership of at least fifty percent (50%) of the voting stock, shares or other equity interest in the Controlled Person and possession of the power to direct or cause the direction of the management and policies of the controlled Person.
- 1.2 “**CCPA**” means the California Consumer Privacy Act.
- 1.3 “**Controller**” means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- 1.4 “**Customer Data**” means any data, information or material originated by Customer that Customer submits to AvePoint, collects through its use of the Services or provides to AvePoint in the course of using the Services.
- 1.5 “**EEA**” means the European Economic Area, which constitutes the member states of the European Union and Norway, Iceland and Liechtenstein, as well as, for the purposes of this DPA, the United Kingdom.
- 1.6 “**EU Data Protection Legislation**” means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (“**General Data Protection Regulation**” or “**GDPR**”), as amended, replaced or superseded, and (ii) the applicable data protection laws of Switzerland and the United Kingdom.
- 1.7 “**IDTA**” means the United Kingdom’s International Data Transfer Addendum to the EU Standard Contractual Clauses, Version B1.0, in force 21 March 2022 (as amended from time to time).
- 1.8 “**Personal Data**” means any Customer Data relating to an identified or identifiable natural person (“**Data Subject**”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- 1.9 “**Processor**” means an entity which Processes Personal Data on behalf of the Controller.
- 1.10 “**Processing**” means any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- 1.11 “**Services**” means any services provided by AvePoint under the Agreement.
- 1.12 “**Standard Contractual Clauses**” means the standard data protection clauses (processor-to-processor module) that have been entered into by and between AvePoint Deutschland GmbH and all its Affiliates for the transfer of Personal Data from Processors in the EEA to Processors established in third countries which do not ensure an adequate level of data protection, as described in Art. 46 GDPR and approved by the EU Commission in decision 2021/914/EC, dated

June 4, 2021 as amended or superseded; or any alternative data transfer solutions permitted by and under EU Data Protection Laws for the Processing or Transfer of Personal Data to third countries.

- 1.13 **“Supervisory Authority”** means an independent public authority which is established by an EU member state pursuant to EU Data Protection Legislation.
- 1.14 Capitalized terms not defined in this DPA shall have the same meaning as set out in the Agreement. Capitalized terms not defined in the Agreement but defined in the GDPR shall have that meaning.

## 2 Specification of the Customer Data Processing

- 2.1 **Categories of Personal Data Processed.** The categories of Personal Data are determined by the Customer in its sole discretion and may include but are not limited to: first and last name; employer; business role; professional title; contact information (e.g., e-mail, phone, physical address); business network; business experience; business interests; localization data; and device identification data.
- 2.2 **Special Categories of Personal Data.** Special categories of Personal Data, if any, are determined by Customer in its sole discretion and may include, but are not limited to, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
- 2.3 **Categories of Data Subjects.** The categories of Data Subjects whose Personal Data may be Processed in connection with the Services are determined and controlled by Customer in its sole discretion and may include but are not limited to customers and prospects of Customer, employees or contractors of Customer's prospects and customers, and employees and contractors of Customer.
- 2.4 **Nature of Processing Operations.** AvePoint will Process Personal Data as necessary to perform the Services pursuant to the Agreement. The Processing operations performed on the Personal Data will depend on the scope of the Services agreed between AvePoint and the Customer. Such Processing operations of Personal Data as necessary for AvePoint to provide the Services may include the following: collecting, recording, organizing, storage, use, alteration, disclosure, transmission, combining, retrieval, consultation, archiving and/or destruction.

## 3 Roles and Responsibilities

- 3.1 **Parties' Roles.** Customer, as Controller, appoints AvePoint as a Processor to Process the Personal Data on Customer's behalf. In some circumstances Customer may be a Processor, in which case Customer appoints AvePoint as Customer's sub-processor, which shall not change the obligations of either Customer or AvePoint under this DPA, as AvePoint will remain a Processor with respect to the Customer in such event.
- 3.2 **Purpose Limitation.** AvePoint shall Process Personal Data for the purposes set forth in the Agreement and only in accordance with the lawful, documented instructions of Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by applicable law; in such a case, AvePoint shall inform the Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. The Agreement and this DPA set out Customer's complete instructions to AvePoint in relation to the Processing of Personal Data and any Processing required outside of the scope of these instructions (inclusive of the rights and obligations set forth under the Agreement) will require prior written agreement of the parties.
- 3.3 **Training.** AvePoint shall ensure that its relevant employees, agents and contractors receive appropriate training regarding their responsibilities and obligations with respect to the Processing, protection and confidentiality of Personal Data.
- 3.4 **Compliance.** AvePoint, as Processor, has complied and will continue to comply with all applicable privacy and data protection laws including, but not limited to, EU Data Protection Legislation. Customer, as Controller, shall be responsible for ensuring that, in connection with Customer Data and the Services:
  - a) it has complied, and will continue to comply, with all applicable privacy and data protection laws including, but not limited to, EU Data Protection Legislation; and
  - b) it has, and will continue to have, the right to transfer, or provide access to, the Personal Data to AvePoint for Processing in accordance with the terms of the Agreement and this DPA.

#### 4 Technical and Organisational Measures and Security

- 4.1 AvePoint shall establish the security in accordance with Art. 28.3 (c), 32 GDPR, in particular in conjunction with Art. 5.1, 5.2 GDPR. Taking into account the state of the art, 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, AvePoint shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk ("**Technical and Organisational Measures**"). These measures shall specifically be designed to ensure appropriate security of the Personal Data against risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed (each a "**Security Incident**"). The Technical and Organisational Measures that AvePoint has currently implemented are described in AvePoint's Data Protection and Information Security Policy, available under <https://www.avepoint.com/agreements/dataprotection>, as amended from time to time. Any changes to this policy may not materially deteriorate the level of security it provides.
- 4.2 AvePoint may not on its own authority rectify, erase or restrict the Processing of Personal Data that is being Processed on behalf of the Customer, but only on documented instructions from the Customer. Insofar as a Data Subject contacts AvePoint directly concerning a rectification, erasure, or restriction of Processing, AvePoint will immediately forward the Data Subject's request to the Customer and shall, where reasonably possible, provide commercially reasonable assistance, including appropriate Technical and Organisational Measures, to enable Customer to respond to such request.
- 4.3 Insofar as it is included in the scope of Services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by AvePoint in accordance with documented instructions from the Customer without undue delay.
- 4.4 Upon becoming aware of a Security Incident, AvePoint shall notify Customer without undue delay and pursuant to the terms of the Agreement, but within no more than seventy-two (72) hours and shall provide such timely information as Customer may reasonably require to enable Customer to fulfil any data breach reporting obligations under EU Data Protection Legislation. AvePoint will take steps to immediately identify and remediate the cause of such a Security Incident. If and insofar as it is not possible for AvePoint to simultaneously provide all of the relevant information, the information may be provided to the Customer step-by-step without unreasonable delay and no later than within 72 hours after the discovery. AvePoint will take steps to immediately identify and remediate the cause of such a Security Incident.

#### 5 Quality Assurance and Other Duties of AvePoint

- 5.1 In addition to complying with the rules set out in this DPA, AvePoint shall comply with its statutory requirements referred to in the EU Data Protection Legislation; accordingly, AvePoint ensures, in particular, compliance with the following requirements:
  - a) AvePoint will entrust only such employees with the data Processing outlined in this DPA who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. AvePoint and any person acting under its authority who has access to Personal Data, shall not Process that data unless on instructions from the Customer, which includes the powers granted in this DPA, unless required to do so by law.
  - b) AvePoint shall inform the Customer immediately if it reasonably believes an instruction violates EU Data Protection Legislations or other applicable data protection provisions. AvePoint shall then be entitled to suspend the execution of the relevant instructions until the Customer confirms or changes them.
  - c) The Customer and AvePoint shall cooperate, on request, with the Supervisory Authority in performance of its tasks.
  - d) The Customer shall be informed without undue delay of any inspections and measures conducted by the Supervisory Authority, insofar as they relate to this DPA. This also applies insofar as AvePoint is under investigation or is party to an investigation by a competent authority in connection with infringements to any civil or criminal law, or administrative rule or regulation regarding the Processing of Personal Data in connection with this DPA.
  - e) Insofar as the Customer is subject to an inspection by a Supervisory Authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Data Processing by AvePoint under this DPA, AvePoint shall make every effort to support the Customer.

- 5.2 AvePoint shall, to the extent required by EU Data Protection Legislation, provide Customer with reasonable assistance with data protection impact assessments and/or prior consultations with Supervisory Authorities that Customer is required to carry out under EU Data Protection Legislation and, taking into account the nature of processing and the information available to AvePoint, with Customer's other obligations under EU Data Protection Legislation, by providing the information and documents as per sec. 7.1.
- a) AvePoint shall, taking into account the nature of the processing, assist the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights under applicable data protection laws.
  - b) AvePoint shall periodically monitor the internal processes and the Technical and Organisational Measures to ensure that Processing within its area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the Data Subject.

## 6 Sub-Processing

- 6.1 **Sub-processors.** Customer provides general authorization to AvePoint's use of AvePoint Affiliates and third-party sub-processors (collectively, "Sub-processors") to Process the Personal Data on AvePoint's behalf. The Sub-Processors currently engaged by AvePoint and authorized by Customer are listed on AvePoint's website (currently at <https://www.avepoint.com/company/sub-processors>). Customer hereby expressly consents to AvePoint's use of these Sub-processors. AvePoint shall make appropriate and legally binding contractual arrangements with such Sub-processors, shall impose on such Sub-processors data protection terms that protect the Personal Data to the same standard provided for by this DPA and shall remain liable for any breach of the DPA caused by a Sub-processor.
- 6.2 **Changes to Sub-processors.** At least 30 days before AvePoint engages a new Sub-processor, AvePoint will update the applicable webpage and provide Customer with a mechanism to obtain notice of that update. Customer may object to the appointment of an additional Sub-processor within fourteen (14) calendar days of such notice on reasonable grounds relating to the protection of the Personal Data, in which case AvePoint shall have the right to cure the objection through one of the following options (to be selected at AvePoint's sole discretion): (i) AvePoint will offer an alternative to provide the Services without such Sub-processor; or (ii) AvePoint will take the corrective steps requested by Customer in its objection (which remove Customer's objection) and proceed to use the Sub-processor with regard to Personal Data, or (iii) AvePoint may cease to provide or Customer may agree not to use (temporarily or permanently) the particular aspect of the Services that would involve the use of such Sub-processor with regard to Personal Data, subject to a mutual agreement of the parties to adjust the remuneration for the Services considering the reduced scope of the Services. Objections to a Sub-processor shall be submitted to AvePoint via e-mail to [legal@avepoint.com](mailto:legal@avepoint.com). If none of the above options are reasonably available and the objection has not been resolved to the mutual satisfaction of the parties within 30 days after AvePoint's receipt of Customer's objection, either party may terminate the Agreement and Customer will be entitled to a pro-rata refund for prepaid fees for Services not performed as of the date of termination.
- 6.3 **Emergency Replacement.** AvePoint may replace a Sub-processor if the need for the change is urgent and necessary to provide the Services and the reason for the change is beyond AvePoint's reasonable control. In such instance, AvePoint shall notify Customer of the replacement as soon as reasonably practicable, and Customer shall retain the right to object to the replacement Sub-processor pursuant to sec. 6.2 above.
- 6.4 **Data Processing outside the EU/EEA.** If the Sub-processor provides the agreed Services outside the EU/EEA, AvePoint will ensure compliance with EU Data Protection Legislation by appropriate measures. All transfers of Personal Data out of the EU/EEA, United Kingdom, and Switzerland to provide the Services shall be governed by the Standard Contractual Clauses implemented by AvePoint. In addition, transfers from the United Kingdom shall be governed by the IDTA implemented by AvePoint. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Art. 46 GDPR and such transfers and safeguards will be documented according to Art. 30.2 GDPR.
- 6.5 **Outsourcing by the Sub-processor.** Further outsourcing by the Sub-processor requires the express consent of AvePoint in writing and shall be communicated to Customer in accordance with sec. 6.2 above.

## 7 Certifications and Audits

- 7.1 **Certification Documentation.** Upon Customer's written request and subject to an NDA or equivalent contractual confidentiality provisions in place between the Parties, AvePoint will provide Customer with additional documents and information pertaining to its security- and privacy-related certifications. This may in particular include (i) ISO

certificates (e.g., for ISO 27001, 27017, 27701 and/or other ISO standards), (ii) Statements of Applicability (SoA) for such ISO certifications, (iii) System and Organization Controls (SOC) reports, and/or other.

- 7.2 **AvePoint Audits.** AvePoint commissions third parties to review and verify the adequacy of AvePoint's security measures (collectively "**AvePoint Audit**"). Such AvePoint Audits will be performed (i) at least annually or in such other frequency as required to comply with applicable standards; and (ii) according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; and (iii) by independent qualified third parties at AvePoint's selection and expense. Any audit report generated as a result of an AvePoint Audit ("**Audit Report**") will be AvePoint's Confidential Information. Upon Customer's written request and subject to an NDA or equivalent contractual confidentiality provisions in place between the Parties, AvePoint will provide Customer with a copy of the Audit Report so that Customer can reasonably verify AvePoint's compliance with its obligations under this DPA.
- 7.3 **Customer Audits.** If Customer chooses to conduct any audit, including any inspection of AvePoint, under Applicable Data Protection Law or the Standard Contractual Clauses (collectively "**Customer Audit**"), Customer has the right to request or mandate such Customer Audit on its own behalf, and on behalf of its Controllers when Customer is acting as a Processor to a third party, by instructing AvePoint to carry out the audit described in sec. 7.2. If Customer wishes to change this instruction regarding the Customer Audit, then Customer has the right to request a change to this instruction by sending AvePoint written notice as provided for in the Agreement. If AvePoint declines to follow any instruction requested by Customer regarding Customer Audits, Customer is entitled to terminate the Agreement in accordance with its terms.

## 8 Deletion and Return of Personal Data

- 8.1 Copies or duplicates of the data shall never be created without the knowledge of the Customer, with the exception of (i) copies or duplicates that AvePoint needs to create in order to fulfil its contractual obligations towards Customer; (ii) back-up copies as far as they are necessary to ensure orderly data Processing; and (iii) data required to meet regulatory requirements to retain data.
- 8.2 After the end of the Processing by AvePoint, AvePoint shall upon written request and at the choice of the Customer within 60 (sixty) days after the request delete or make available to Customer for retrieval all relevant Personal Data (including copies) in AvePoint's possession, in a structured, commonly used, and machine-readable format. The log of the destruction or deletion shall be provided on request.
- 8.3 Notwithstanding the provisions of sec. 8.2 above, AvePoint shall be entitled to retain documentation which is used to demonstrate orderly data Processing in accordance with the Agreement and this DPA as well as Personal Data that AvePoint is required by any applicable law to retain. Such documentation and Personal Data shall be stored beyond the contract duration by AvePoint in accordance with the respective retention periods and AvePoint shall limit its further Processing to only those limited purposes that require the retention, for so long as AvePoint maintains such documentation and Personal Data.

## 9 CCPA and Similar Laws

- 9.1 If AvePoint is processing Personal Data within the scope of the CCPA or any laws that rely on, are similar to or based on the CCPA, including without limitation, the respective laws of Virginia and Colorado ("**Similar Laws**"), AvePoint makes the following additional commitments to the Customer:
- AvePoint shall not "sell" (as defined in the CCPA or such Similar Law, as applicable) such Personal Data;
  - AvePoint shall not Process Personal Data for any purpose other than to perform the Services or as otherwise permitted by the CCPA or such Similar Law, as applicable; and
  - AvePoint shall not Process Personal Data outside of the business purpose (as defined in the CCPA or such Similar Law, as applicable) between the Parties.
- 9.2 The terms under this sec. 9 do not limit or reduce any data protection commitments AvePoint makes to Customer in this DPA, the Agreement, or any other agreement between AvePoint and Customer.

## 10 Miscellaneous

- 10.1 Except as amended by this DPA, all provisions of the Agreement shall remain in full force and effect, in particular regarding legal venue, applicable law and liability.
- 10.2 If there is a conflict between the Agreement and this DPA, the terms of this DPA shall prevail. Nothing in this document varies or modifies the Standard Contractual Clauses other than the choices or options expressly permitted therein.