Applixure Data Processing Agreement

Updated: November 2026

1 INTRODUCTION

This Data Processing Agreement ("DPA") sets forth the parties' obligations regarding data protection and compliance with Data Protection Laws, and the parties (including their representatives) are required to comply with this DPA in connection with the performance of their obligations related the agreed Services.

This DPA reflects the parties' agreement with respect to the terms governing the Processing of Personal Data under the Applixure Terms of Service (the "Terms"). This DPA will form a part of the Terms. The details of the processing are described in Appendix 1.

The Customer and Applixure acknowledge that relevant Data Protection Laws must be observed during the provision of the Services under the Agreement.

2 SUBJECT AND PURPOSE OF THIS APPENDIX

The purpose of this DPA is to ensure the implementation of consistent privacy and data protection practices to be applied in the provision of Services by Applixure to the Customer.

Furthermore, the parties recognize and agree that proper data protection is required by both national legislation and the regulations of the European Union, our own personnel, customers and other stakeholders.

3 DEFINITIONS

"Adequately Legislated Countries" shall mean the countries outside the EU/EEA with laws considered by the European Commission to provide an adequate level of protection of personal data.

"Personal Data" shall mean personal data as defined in the Data Protection Laws.

"Data Breach" shall mean a data breach, as defined in the Data Protection Laws.

"Data Subject" shall mean a person, as defined in the Data Protection Laws, whose Personal Data Applixure processes under this DPA.

"Data Protection Laws" shall mean, without limitation and as applicable, all directly applicable EU legislative acts related to protection of personal data as in force from time to time (collectively the "EU Legislation"), and all other applicable data protection legislation.

4 COMPLIANCE WITH LAWS AND THE CUSTOMER'S INSTRUCTIONS

The parties agree to comply with the Data Protection Laws, including without limitation, to observe the requirements derived therefrom in all its such activities, such as 'privacy by design' and 'privacy by default'.

To the extent that Applixure is processing Personal Data on behalf of the Customer, Applixure shall, and shall procure that any subcontractors shall, process Personal Data solely to the extent necessary for fulfilling their obligations under the Terms and in accordance with the procedures conforming to the Customer's requirements and/or instructions expressly provided in the Terms or this DPA or as otherwise provided by the Customer in writing. Applixure shall ensure that its subcontractors comply with the same requirements concerning any Personal Data. Should any future written instructions of the Customer go beyond the legally necessary, Customer will compensate Applixure for the incurred costs.

Applixure shall not process the Personal Data for any other purposes than those specified in the Terms and this DPA, including any exhibits thereto. Applixure undertakes to, at the choice of the Customer, after the end of provisioning Services, either return or delete the personal data processed on behalf of the Customer, unless EU or national legislation requires storage such personal data.

5 TRANSFER OF PERSONAL DATA

If and to the extent that the Customer is located in the EU/EEA, unless otherwise agreed, Applixure will not process Personal Data in a country outside the EU/EEA or the Adequately Legislated Countries. Should the provision of Services be located in a country that is outside Adequately Legislated Country, Applixure shall ensure compliance with the Data Protection Laws in connection with all such transfers of Personal Data and enter into the appropriate contractual arrangements on the transfer of Personal Data to third countries as approved by the applicable data protection regulatory authority (Standard Contractual Clauses "SCCs"), as in force from time to time.

If and to the extent that the Customer is located outside the EU/EEA, the Customer hereby acknowledges that Applixure will transfer Personal Data outside of the EU/EEA (as "data exporter") to the Customer (as "data importer") in connection with the Services. In effecting any such international transfer, the Parties shall ensure that:

(i) to the extent that such a transfer is pursuant to the SCCs, such transfer is subject to Module 4 of the SCCs, where Applixure acts as a processor of Personal Data for the purposes of the Services. Module 4 shall be completed as set out in Appendix 2 to this DPA; or

(ii) the transfer otherwise complies with Data Protection Laws (for example, transfer is carried out to the Adequately Legislated Countries or under any EU-US transatlantic data privacy framework).

6 CONFIDENTIALITY

Except to the extent necessary for Applixure to perform its obligations towards the Customer under the Agreement, Applixure shall keep Personal Data confidential, shall have no rights to Personal Data, and, unless specifically agreed otherwise with the Customer in writing, shall not access, use, process, disclose, or transfer Personal Data, in part or in whole, to any third party during or after the term of the Agreement unless legally required. Applixure shall ensure that persons authorised to process personal data on behalf of the Customer have committed themselves to confidentiality or are under appropriate statutory obligation of confidentiality.

7 USE OF THIRD PARTIES IN DATA PROCESSING

Applixure may engage subcontractor(s) to process Personal Data provided that:

(i) such engagement will be under a written contract, and

(ii) the subcontract will require the subcontractor(s) to comply with the same obligations applicable to Applixure.

Applixure shall inform the Customer in writing of any intended addition or replacement of subcontractors sufficiently in advance to give the Customer an opportunity to object on reasonable grounds relating to the protection of Personal Data before the concerned subcontractor begins processing Personal Data. The parties shall discuss any such objection in good faith with a view to resolving it before the proposed change is implemented.

8 SAFEGUARDS

Applixure shall implement and use its reasonable efforts to maintain at all appropriate times, operational and technical measures to protect the Personal Data against accidental, unauthorized or unlawful destruction, loss, alteration, disclosure or access. Applixure shall implement the following measures as applicable:

(i) the pseudonymisation and encryption of Personal Data where so required by Data Protection Law;

(ii) ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services processing Personal Data;

(iii) restoring the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

(iv) regularly testing, assessment and evaluation of the effectiveness of technical and organisational measures for ensuring the security of the processing of Personal Data.

Applixure shall keep accurate records of all processing of Personal Data under the Terms and limit access of Personal Data to authorized and properly trained personnel with a well-defined "need-to-know" bases and who are bound by appropriate confidentiality obligations.

9 DATA BREACHES

Applixure shall provide the Customer with reasonably detailed written notice of its discovery of any Data Breach without delay.

The Data Breach notification shall contain at least the following:

(i) description of the nature of the Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

(ii) the name and contact details of the contact point where more information can be obtained;

(iii) description of the likely consequences of the Data Breach;

(iv) description of the measures taken or proposed to be taken by Applixure to address Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Applixure shall co-operate with the Customer and take reasonable commercial steps as are directed by the Customer to assist in the investigation, mitigation and remediation of each such Data Breach.

10 RIGHT TO AUDIT

Applixure shall make available to the Customer all information necessary to demonstrate compliance with its obligations under Article 28 of the GDPR and this DPA. This information shall be provided independently of any formal audit. Applixure may initially respond by providing relevant existing documentation, such as current certifications and their scope, descriptions of technical and organisational measures, and the subcontractor list, and shall provide additional explanations or supporting information where necessary. Requests shall relate to the processing of Personal Data on behalf of the Customer. Confidential information, security-sensitive details and information relating to other customers or third parties shall be protected through appropriate confidentiality arrangements, redaction, summaries or secure access, without preventing the Customer from obtaining the information necessary to demonstrate compliance. The audit procedure and audit cost provisions below do not apply merely because the Customer requests such information.

The Customer shall have the right to audit the processing activities of Applixure under this DPA to examine the level of protection and security provided for Personal Data processed under the Terms.

The parties agree that this right will be exercised by appointment of a recognized, independent third party auditor with proven experience in the field. Such third party shall not be a competitor of Applixure and prior to commencement of any auditing activities, the auditor must sign a confidentiality agreement with Applixure that is substantially similar to the confidentiality provisions contained in the Terms.

The audit timetable, method and scope will be agreed beforehand between the parties and the audit may not burden Applixure or endanger Applixure or Applixure's other clients' delivery, quality, security or confidentiality. The Customer will pay all costs related to the audit.

In the event of an audit request directly from a supervisory authority regarding processing of Personal Data, Applixure must cooperate with Customer in answering the request.

11 ACCESS TO PERSONAL DATA AND RIGHTS OF DATA SUBJECTS

If requested by the Customer or by authorities, to comply with the Data Protection Laws, Applixure shall, at the standard rates,

(i) provide the Customer with a copy of individuals' Personal Data in tangible form,

(ii) correct, block or delete individuals' Personal Data,

(iii) provide the Customer with such information and cooperation regarding the processing of Personal Data under the Agreement as the Customer may reasonably request, including assisting in facilitating the exercise of their rights by Data Subjects,

(iv) assist the Customer in providing individuals whose Personal Data is being processed with such information regarding the processing as the Customer may reasonably request.

Appendix 1

This appendix defines details of processing of Personal Data and shall be an integral part of and supplement the DPA, as further agreed below:

(a) Nature and purpose of the processing

Information provided by Customer and required for the provision of our products and services, including registration information and information entered into our system when using the Services. Information otherwise provided by the Users or End-Users.

(b) Type of Personal Data and categories of data subjects

Technically gathered online data, including name and user name, picture, and unique device identifiers, IP address (not by default), device software version numbers and identifiers of the end-users. With respect to Applixure Feedback Service, data generated

or entered by End-Users by filling out questionnaires or feedback forms, including possible Personal Data entered into open text fields.

(c) Applicable security measures

Applixure takes all reasonable measures to protect Personal Data as the data is transferred from end-user devices to Applixure, and during storage and processing in the backend. These measures include encryption of data and connections wherever applicable, protecting access to the Applixure infrastructure and databases using industry standard protection methods, including technical and organizational safety procedures, and access control and monitoring against the Services.

As the Services will be maintained on external service providers' servers, service providers providing this service will also ensure appropriate safeguards against physical threats against the Services, including access monitoring and control.

(d) Duration of the processing

During the Subscription term of the Customer to the Service + 2 months.

Appendix 2

This appendix defines details of Module 4 of the SCCs and shall be an integral part of and supplement the DPA.

Module 4 be completed as follows:

a) Clause 7, the optional docking clause will apply;

b) Clause 11(a), optional data subject redress mechanism, shall not apply;

c) Clause 17, the SCCs will be governed by the laws of Finland;

d) Clause 18, any disputes arising from the SCCs shall be resolved by the courts of Finland.

Annex I of the SCCs shall be deemed completed with the following information:

A. List of Parties

Data Exporter: Applixure Oy

Address: Arabiankatu 12, 00560 Helsinki, Finland

Contact Person's name, position and contact details: info@applixure.com

Activities relevant to the data transferred under the SCCs: See Part B below

Signature and date: This Annex shall automatically be deemed executed when the agreement between the parties is executed by Applixure

Role: Processor

Data Importer: "Customer" as detailed in the agreement

Address: As detailed in the agreement

Contact Person's name, position and contact details: As detailed in the agreement

Activities relevant to the data transferred under the SCCs: See Part B below

Signature and date: This Annex shall automatically be deemed executed when the agreement between the parties is executed by the Customer

Role: Controller

B. Description of Processing and, only to the extent applicable to the Customer, the transfer of Personal Data under the SCCs

Categories of data subjects whose personal data is transferred: As detailed in Appendix 1 to DPA

Categories of personal data transferred: As detailed in Appendix 1 to DPA

Sensitive data transferred: None

The frequency of the transfer: Incidental (processing occurs on an ad hoc basis depending on Customer's use of and interaction with the Services).

Nature of the processing: As detailed in Appendix 1 to DPA

Purpose(s) of the data transfer and further processing: As detailed in Appendix 1 to DPA

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: As detailed in Appendix 1 to DPA