

Applixure Data Processing Agreement

Updated: April 2018

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 “Agreement”). This DPA is an amendment to the Agreement and will form a part of the Agreement. The details of the processing are described in Appendix 1.

The Customer and the Supplier 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 the Supplier to the Customer.

Furthermore, the parties recognize and agree that proper data protection is required by both national legislation and the directives 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 the Supplier 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 the Supplier is processing Personal Data on behalf of the Customer, the Supplier shall, and shall procure that any subcontractors shall, process Personal Data solely to the extent necessary for fulfilling their obligations under the Agreement and in accordance with the procedures conforming to the Customer's requirements and/or instructions expressly provided in the Agreement or this DPA or as otherwise provided by the Customer in writing. The Supplier 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 the Supplier for the incurred costs.

The Supplier shall not process the Personal Data for any other purposes than those specified in the Agreement and this DPA, including any exhibits thereto. The Supplier undertakes to, at the choice of the Customer, after the end of provisioning Service, 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

Unless otherwise agreed, the Supplier will not process Personal Data in a country outside the Adequately Legislated Countries. Should the provision of services be located in a country that is outside Adequately Legislated Country, the Supplier shall ensure compliance with the Data Protection Laws in connection with all such transfers of Personal Data and, in the absence of any applicable framework for exchanges of personal data like the EU-US Privacy Shield, enter into the appropriate contractual arrangements on the transfer of Data to third countries as approved by the applicable data protection regulatory authority (Model Clauses), as in force from time to time.

6. CONFIDENTIALITY

Except to the extent necessary for the Supplier to perform its obligations towards the Customer under the Agreement, the Supplier 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. Supplier 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

The Supplier 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 the Supplier.

The Supplier shall inform the Customer of any intended changes of subcontractors.

8. SAFEGUARDS

The Supplier 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. The Supplier 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.

The Supplier shall keep accurate records of all processing of Personal Data under the Agreement 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.

The Supplier 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 the Supplier to address Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

9. RIGHT TO AUDIT

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

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 Supplier and prior to commencement of any auditing activities, the auditor must sign a confidentiality agreement with Supplier that is substantially similar to the confidentiality provisions contained in the Agreement.

The audit timetable, method and scope will be agreed beforehand between the parties and the audit may not burden Supplier or endanger Supplier or Supplier'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, the Supplier must cooperate with Customer in answering the request.

10. ACCESS TO PERSONAL DATA AND RIGHTS OF DATA SUBJECTS

If requested by the Customer or by authorities, to comply with the Data Protection Laws, the Supplier 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 Agreement, 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.

Otherwise provided by the 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, device software version numbers and identifiers of the end-users, and the name, user name, email address and contact phone number for the main users of the Service.

(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 Service.

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

(d) Duration of the processing

During the Subscription term of the Customer to the Service + 2 months as set forth in Applixure Privacy Policy as retain time for Personal Data.