

Data processing agreement (DPA) for myPlane service platform

Last updated: 9th of February 2022

1. GENERAL

- 1.1 This Data Processing Agreement for myPlane Service Platform ("**DPA**") is a legal agreement between myPlane Ltd ("**Service Provider**") and the user company duly accepting this DPA by its authorized representative ("**User**"). This DPA applies strictly to myPlane Service Platform ("**Service**") only, and does not govern or apply to issues beyond Service.
- 1.2 This DPA shall bind User upon its acceptance. This DPA shall become an integral part of Terms of Use Agreement for Service ("**TOU**"). This DPA will be applied as between Parties primarily in matters concerning data processing.
- 1.3 For the purpose of this DPA, Service Provider shall be regarded as processor and User shall be regarded as controller. Controller and processor are hereinafter referred to as "**Controller**" and "**Processor**". Controller and Processor may also be referred hereinafter individually as a "**Party**" and jointly as "**Parties**".
- 1.4 Processor will process Personal Data in accordance with this DPA. Legal ground for the processing of Personal Data is the provision of Services under TOU. This DPA will remain in force as long as Services are being provided and TOU, under which Personal Data is being processed, are valid.

2. DEFINITIONS

- 2.1 "**Data Breach**" means an event leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data processed by Service Provider or any other such event that in Service Provider's point of view has or may have compromised the data security of Personal Data.
- 2.2 "**Data Protection Legislation**" means Data Protection Act (1050/2018, as amended), General Data Protection Regulation of the European Union (EU 2016/679, as amended, "**GDPR**"), Data Protection Act (1050/2018) and any other applicable national or EU-wide data protection legislation as well as any instructions and decisions given by the competent data protection authorities.
- 2.3 "**Data Subject**" shall mean a natural person whose Personal Data will be processed under this DPA.
- 2.4 "**Personal Data**" means any information relating to an identified or identifiable natural person, or other personal data as defined in Data Protection Legislation.

3. PROCESSING OF PERSONAL DATA

- 3.1 Parties undertake to comply with applicable Data Protection Legislation.
- 3.2 Controller is a controller of Personal Data and Processor is a processor of Personal Data, who acts on behalf of Controller.
- 3.3 The purpose and nature of the processing, the types of Personal Data and the groups of Data Subjects, the applicable data security measures, and the duration of the processing are described by Parties in more detail in [Appendix 1](#), which Service Provider may amend.
- 3.4 Personal Data will be stored in Services database and maintained either in Processor's or its sub-processor's environment, subject to respective due agreement between Processor and its sub-processor.

4. GENERAL OBLIGATIONS

- 4.1 Service Provider shall process Personal Data in compliance with this DPA, Data Protection Legislation and good data industry practice.
- 4.2 In case Service Provider considers that written instructions given by User, if any, are in breach of Data Protection Legislation, Service Provider shall inform User thereof without undue delay.

- 4.3 Service Provider shall ensure that its personnel providing Services to User with access to Personal Data have committed themselves to due confidentiality obligations or are under an appropriate statutory obligation of confidentiality.
- 4.4 Service Provider shall assist User in ensuring compliance with its obligations set out in Data Protection Legislation, including but not limited to data security measures, Data Breaches, data protection impact assessments and prior consulting obligations.
- 4.5 Service Provider shall assist User in ensuring compliance with User's obligations pursuant to Articles 32-36 of GDPR.
- 4.6 Service Provider shall make available to User all reasonable information necessary to demonstrate compliance with obligations set out in this DPA and in Data Protection Legislation.
- 4.7 Service Provider shall be entitled to invoice User of its assistance to User under this Section 4 subject to Service Provider's then current price list for Service Provider's hourly work.

5. SUBCONTRACTORS

- 5.1 Service Provider shall have the right to use subcontractors in the processing of Personal Data without a separate prior written consent of User.
- 5.2 Service Provider is responsible for ensuring that its subcontractors commit to terms corresponding at least to the terms agreed in this DPA. Service Provider shall without delay notify User in case it notices that a subcontractor is not fulfilling its contractual obligations.
- 5.3 Service Provider is responsible for any acts and omissions by its subcontractors as for its own.
- 5.4 Upon User's written request, Service Provider shall provide User with a current list of those subcontractors that Service Provider uses for the provision of Services. In case User objects to any of such subcontractor listed, User shall inform Service Provider thereof in written form and Parties shall in good faith try to resolve the subject matter.

6. LOCATION OF PERSONAL DATA

- 6.1 Service Provider or its subcontractors may transfer Personal Data, including giving access to the Personal Data, to countries outside the European Union or the European Economic Area.
- 6.2 If Service Provider transfers Personal Data outside the European Union or the European Economic Area, it will ensure compliance with Data Protection Legislation before the transfer of data by committing to conclude standard contractual clauses for the transfer of personal data approved by the European Commission ("**Model Clauses**") or to ensure otherwise that the transfer meets the requirements of Data Protection Legislation.

7. DATA SECURITY MEASURES

- 7.1 Service Provider shall carry out necessary technical and organizational measures in order to ensure the security of processed Personal Data, and especially to prevent and protect Personal Data from unintentional loss, alteration, destruction, or damage. When assessing the appropriate level of such data security measures, Service Provider shall take in account the risks included in the processing of Personal Data, the state of the art and the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons. Service Provider shall at least commit to:
 - 7.1.1 pseudonymise and encrypt Personal Data if necessary to maintain the confidentiality thereof;
 - 7.1.2 ensure the ongoing confidentiality, integrity, availability, and resilience of the processing systems and services;
 - 7.1.3 ensure the ability to restore the availability of and access to Personal Data in a timely manner in the event of a physical or technical incident;
 - 7.1.4 implement a process to regularly test, assess and evaluate the effectiveness of the implemented technical and organizational measures to ensure the security of data processing; and

7.1.5 carry out security inspections to its processing operations of Personal Data.

7.2 Service Provider understands that Personal Data is confidential information which shall be treated accordingly. Service Provider shall ensure that Personal Data is processed only by persons who need such information to provide Services agreed in TOU. Service Provider shall ensure that these persons process Personal Data have committed themselves to confidentiality obligations or are under an appropriate statutory confidentiality obligation.

8. DATA BREACHES

8.1 Service Provider shall notify User of any Data Breaches concerning Personal Data without undue delay. The written notification of the Service Provider shall include at least the following information:

8.1.1 description of the nature of Data Breach;

8.1.2 description of the categories of the Data Subjects concerned, types of Personal Data concerned, and of their estimated amounts;

8.1.3 description of the likely or already occurred consequences of Data Breach, and of the actions taken by Service Provider to minimize the adverse effects of Data Breach; and

8.1.4 description of the remedial actions which Service Provider has taken or shall take due to the Data Breach.

8.2 Service Provider shall document all Data Breaches, including the facts relating to each Data Breach, its effects and the remedial actions taken.

8.3 Service Provider shall upon User's written request assist User in notifying about Data Breach to the supervisory authority and data subjects.

9. AUDIT

9.1 User or an independent auditor authorised by User has the right to audit that Service Provider processes Personal Data in accordance with this DPA and applicable Data Protection Legislation.

9.2 Each Party is responsible for its own costs in relation to the audit.

9.3 User shall give at least sixty (60) days prior written notice to Service Provider upon its intention to use its audit right.

9.4 Audit shall be carried out in a way that it does not interfere with Service Provider's ordinary business.

10. LIMITATION OF LIABILITIES

10.1 Limitation of liability of Service Provider agreed in TOU shall apply to this DPA.

11. ERASURE AND RETURN OF PERSONAL DATA

11.1 Service Provider is not entitled to erase any Personal Data processed on behalf of User without User's explicit request. Service Provider is obliged to deliver within reasonable time Personal Data processed by it or a copy or extract thereof to User upon User's written request to email address support@myplane.io.

11.2 Service Provider shall, in accordance with User's election, erase or return all Personal Data to User upon its written request or at the latest when TOU is no longer in force or when the processing of Personal Data is no longer necessary to provide Services. After Personal Data has been successfully erased or returned to User, Service Provider shall destroy Personal Data. Service Provider shall have the right to charge for the erasure or return of Personal Data to User.

APPENDIX 1: DESCRIPTION OF PROCESSING PERSONAL DATA

This appendix 1 describes in more detail Personal Data processed by Service Provider on behalf of User. In this Appendix 1 of DPA, Parties shall describe in more detail the nature and purpose of the processing, the types of Personal Data and categories of Data Subjects, applicable data security measures, and the duration of the processing of Personal Data.

a) Nature and purpose of the processing of Personal Data:

- The provision of Service.
- The facilitation of Service and all related customer service and product features.

b) Types of Personal Data and categories of Data Subjects:

Service Provider processes the following categories of Data Subjects:

- customers, partners, platform users, employees, service providers.

Service Provider processes the following types of Personal Data:

- Name, email, phone number, address, date of birth, passport details and/or any other personal details needed to provide the service.

c) Applicable data security measures:

- Service Provider follows its own data security measures.

d) Duration of the processing of Personal Data:

- For the term of TOU or any necessary term required for the Service or required by any applicable law.

***** end of document *****