*Here you can see the data processing agreement, which describes how we process your personal data, when you are a Yodiwocustomer.*

# Personal Data Processing Agreement (DPA)

YOU SHOULD READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE ACCESSING AND/OR USING ANY SERVICES SPECIFIED IN THE AGREEMENT OF WHICH THESE CLICKWRAP DATA PROCESSING TERMS AND CONDITIONS FORM A PART ("SERVICES"). THE ACCESS AND/OR USE BY YOU OF ANY SERVICES WILL INDICATE YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS AND YOUR CONSENT TO BE BOUND BY THEM TOGETHER WITH YOUR ACKNOWLEDGEMENT OF YOUR AUTHORITY TO DO SO IN YOUR OWN RIGHT OR ON BEHALF OF YOUR COMPANY ("DATA CONTROLLER" OR "CONTROLLER") AND WILL CREATE A LEGALLY BINDING CONTRACT BETWEEN THE DATA CONTROLLER AND YODIWO ACTING IN ITS OWN NAME AND ACTING IN THE NAME AND ON BEHALF OF THE PROCESSORS LISTED IN APPENDIX 3 (EACH A "DATA PROCESSOR" OR "PROCESSOR"). IF YOU DO NOT AGREE WITH THESE YODIWO CLICK WRAP DATA PROCESSING TERMS AND CONDITIONS, YOU SHOULD NOT PROCEED WITH THE ACCESS AND/OR USE OF THE SERVICES.

## 1. General requirements

**1.1** The Data Processor may process the Personal Data only in compliance with the Data Controller's documented written instructions. The data processing tasks performed by the Data Processor on behalf of the Data Controller under this Agreement are set out inAPPENDIX 1.

**1.2** The Data Processor is entitled to process the Personal Data only for the purpose of providing the Services, and only to such an extent and in such a manner as is necessary in order to provide the Services.

**1.3** As the Data Processor is a legal person, the provisions of this Agreement apply to every employee of the Data Processor. The Data Processor guarantees that its employees comply with this Agreement.

## 2. Disclosure of Personal Data

**2.1** The Data Processor may not in any way modify, amend or alter the contents of the PersonalData or disclose the Personal Data to any third party, unless

a) explicitly provided for in this Agreement
b) the Data Controller has otherwise authorised and/or instructed the Data Processor in writing to do so; and/or
c) such disclosure is required by applicable legislation to which the Data Processor is subject.

**2.2** If the disclosure falls within clause 2.1, the Data Processor must notify the Data Controller thereof before commencing the processing of the Personal Data, unless notification of the Data Controller is prohibited under Union law or the Member State law to which the Data Processor is subject.

## 3. Security

**3.1** The Data Processor must implement appropriate technical and organisational security measures to protect the Personal Data against unauthorised or unlawful processing and against accidental or unlawful loss, destruction, damage, alteration or disclosure.

**3.2** When determining the appropriate technical and organisational security measures, the Data Processor must take account of the current available technology and technological developments; the costs of implementation; the nature, scope, context and purposes of the processing; and the risks of varying likelihood and severity for rights and freedoms of natural persons.

**3.3** The Data Processor must comply with and ensure compliance by its employees with the special data security requirements applying to the Data Processor, including without limitation (i) all security measure requirements notified in writing to the Data Processor; (ii) the Data Processor's own internal security standards, and (iii) the national security measure requirements of the country in which the Data Processor is established or the country where the data processing takes place.

**3.4** The Data Processor must keep the Personal Data confidential. The Data Processor must take reasonable steps to ensure that every employee, agent or contractor who has access to the Personal Data is reliable and trustworthy, and that all such persons are subject to confidentiality undertakings, professional secrecy or statutory non-disclosure obligations. The Data Processor must also ensure in each case that access to the Personal Data is strictly limited to those persons who need to access the relevant Personal Data to carry out the duties assigned to them by the Data Processor, and that this is strictly necessary for the provision of the Services.

**3.5** The physical location of the Data Processor's servers, service centre, etc., used in connection with the data processing appears from APPENDIX 1 to this Agreement. The Data Processor is entitled without prior notice to change the physical location of the Data Processor's servers, service centre, etc.

## 4. Transfer of Personal Data to third countries

**4.1** The Data Processor may access the Personal Data from or transfer the Personal Data to any third country without the prior written consent of the Data Controller.

**4.2** If the Data Processor transfers Personal Data to a third country, the Data Processor must ensure that the transfer is effected on a legal basis, e.g. the European Commission model contracts for the transfer of personal data to third countries, before such transfer may be made by the Data Processor.

## 5. Assistance

**5.1** Taking into account the nature of the processing, the Data Processor must to the extent possible assist the Data Controller in dealing with requests from data subjects in connection with the data subject's exercise of his/her rights under the Data Protection Legislation, including without limitation requests for access, rectification, restriction of processing, deletion or data portability.

**5.2** Without undue delay after becoming aware thereof, the Data Processor must inform the Data Controller in writing of any request from a data subject for the exercise of his/her rights received directly from the data subject or from a third party.

**5.3** Taking into account the nature of the processing and the information available to the Data Processor, the Data Processor must implement adequate technical and organisational measures to assist the Data Controller in the performance of its obligation to respond to such data subject requests. The Data Processor must provide all information requested by the Data Controller within a reasonable time.

**5.4** Immediately upon becoming aware thereof, the Data Processor must inform the Data Controller in writing of any suspected or confirmed (i) data security breach; (ii) accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data processed by the Data Processor under this Agreement. The Data Processor must cooperate with and provide assistance to the Data Controller in connection with the management of the data security breach.

**5.5** Taking into account the nature of the processing and the information available to the Data Processor, the Data Processor must assist the Data Controller in complying with any other obligations imposed on the Data Controller under the Data Protection Legislation, including without limitation, upon request, to provide the Data Controller with all necessary information required to make a data protection impact assessment.

**5.6** The services rendered by the Data Processor under clause 5 herein are payable at the Data Processor's hourly rates applicable at any given time.

## 6. Sub-processing

**6.1** The Data Processor is entitled to appoint a third-party as data processor to process Personal Data on behalf of the Data Processor ("Sub-Processor") without the prior written consent of the Data Controller.

**6.2** The Data Processor's appointment of Sub-Processors under clause 6.1 is conditional upon the Data Processor

i. carrying out adequate due diligence on each Sub-Processor to ensure that the Sub-Processor is capable of providing the level of protection for the processing of Personal Data as is required by this Agreement and the Data Protection Legislation;

ii. Including terms in the contract between the Data Processor and each Sub-Processor which, at a minimum, impose the same obligations on the Sub-Processor as those imposed on the Data Processor under this Agreement; and

iii. remaining fully liable to the Data Controller for any failure by any Sub-Processor to perform its obligations in relation to the processing of Personal Data.

**6.3** The Data Processor must inform the Data Controller of any planned changes concerning the addition or replacement of Sub-Processors.

**6.4** The Data Controller is entitled, upon demand, to receive a copy of those parts of the Data Processor's contract with the Sub-Processor which concern the Sub-Processor's obligations relating to the processing of Personal Data.

## 7. Compliance with legislation, damages etc.

**7.1** The Data Controller must ensure that there is a legal basis for the personal data processing activities covered by the instruction given to the Data Processor, cf. APPENDIX 1.

**7.2** The Data Controller acknowledges that the Data Processor is reliant on the Data Controller for direction as to the extent to which the Data Processor is entitled to use and process the Personal Data on behalf of the Data Controller. Consequently, the Data Processor will not be liable for any claim arising from any action or omission on the part of the Data Processor, to the extent that such action or omission are a direct result of the performance of the personal data processing activities in compliance with the Data Controller's instructions.

**7.3** Under no circumstances can the Data Processor's liability towards to the Data Controller exceed the lower amount of either 1) EUR 25,000 or 2) an amount equal to the total amount paid by the Data Controller under the Contract during the last 12 months from the occurrence of the loss. Any other limitations of the Data Processor's liability in damages under the Contract also apply to this Agreement.

## 8. Compliance audits and statements

**8.1** At the request of the Data Controller, the Data Processor must within reasonable time provide all information necessary for the Data Controller, a third party auditor mandated by the Data Controller, or a public authority to verify compliance with the Data Protection Legislation.

**8.2** The Processor is once a year and upon reasonable written notice obliged to cooperate in such compliance audit, inspection and/or review carried out by the Controller, a third party auditor mandated by the Controller, or by a public authority concerning the processing of Personal Data under this Agreement undertaken by the Processor and any Sub-Processors.

**8.3** The Data Processor must notify the Data Controller immediately of any instruction given under clause 8.1 and/or clause 8.2 of this Agreement which the Data Processor believes to be contrary to the Data Protection Legislation.

**8.4** The Data Controller is entitled, at its own expense, to appoint an independent expert who is to have access to the physical facilities of the Data Processor where the Personal Data are processed and to receive the necessary information required to verify whether the Data Processor complies with its obligations under this Agreement. At the request of the Data Processor, the independent expert must sign a standard confidentiality undertaking.

**8.5** The services rendered by the Data Processor under clause 8 herein are payable at the Data Processor's hourly rates applicable at any given time.

## 9. Duration and termination

**9.1** This Agreement takes effect immediately.

**9.2** Each Party are entitled to terminate this Agreement for convenience with a written notice sent by email to the counter-party.

**9.3** This Agreement is to apply as between the Parties for as long as the Data Processor processes Personal Data on behalf of the Data Controller.

**9.4** Upon termination of this Agreement, for whatever reason, the Data Processor must

a) with the exception of paragraph c) below, cease processing the Personal Data;

b) at the Data Controller's request, (i) return to the Data Controller all Personal Data which is in its possession orcontrol and all copies thereof, or (ii) destroy all copies of the same and certify to the Data Controller that it has done so, unless the Data Processor is prevented by applicable law or any public authority from destroying or returning all or part of the

Personal Data, in which case the Data Processor must keep such data confidential, continue to process them in accordance with the terms of this Agreement and must not perform any processing other than what is necessary in order to comply with the requirements of such applicable law or the relevant public authority; and

c) at the Data Controller's request, for an additional charge, provide the necessary transitional services to the Data Controller, including cooperating in good faith and as quickly as possible to facilitate the transfer of the performance of the data processing to a new data processor or back to the Data Controller.

**9.5** If the Data Controller fails to issue an instruction regarding the return or deletion of the Personal Data within three (3) months after termination of this Agreement, the Data Processor is entitled to delete the Personal Data without prior notice.

## 10. Assignment

**10.1** In the event of an assignment of its rights or obligations under this Agreement to a third party, the Data Processor must notify the Data Controller of such assignment without any undue delay.

## 11. Entire agreement

**11.1** The Parties agree that this Agreement constitutes the entire agreement and understanding between the Parties in respect of the subject matter hereof. The Agreement thus supersedes any previous agreement between the Parties relating to the subject matter hereof.

**11.2** In the event of discrepancy between the provisions of this Agreement and the provisions of the Contract or any other written or oral agreements between the Parties, the provisions of this Agreement will prevail. Notwithstanding the above, the provisions of this Agreement will not apply where the Data Processor is subject to stricter obligations, e.g. when using the European Commission model contracts for the transfer of personal data to third countries.

## 12. Amendments

**12.1** The terms, provisions, obligations or conditions of this Agreement may not be waived or amended except by a written instrument signed by both Parties.

**12.2** If any provision of this Agreement is or becomes illegal, void, invalid or unenforceable, such provision must be severed from the other terms and conditions, which will continue to be valid and enforceable to the fullest extent permitted by law.

## 13. Notices

**13.1** All notices required to be given under this Agreement must be in writing.

## 14. Governing Law

**14.1** This Agreement is governed by and will be construed in accordance with Swedish law, without regard to its conflict of laws rules.

**14.2** Any dispute between the Parties arising out of or in connection with this Agreement must be submitted to and be subject to the jurisdiction of the City Court of Stockholm.

# APPENDIX 1

## DESCRIPTION OF PERSONAL DATA PROCESSING ACTIVITIES

This appendix constitutes the Data Controller's instruction to the Data Processor.

***Subject-matter and duration of the processing***

The Data Controller hereby instructs the Data Processor to collect and process data for the purpose of time tracking/logging, analysing and further processing of the same and, if necessary, integration to the Data Controller's other systems.

On termination of this Agreement, the Data Controller and its representatives will no longer have access to the software of the Processor. The underlying database will be stored in the backup system for up to six (6) months, whereupon all copies of the Personal Data provided by the Data Controller will be deleted.
Any access to and restoring of backed-up data requires a written instruction from the Data Controller. A data backup will be provided to the Data Controller upon written request. The costs related thereto are payable at the Data Processor's hourly rates applicable at the time in question.

***Nature and purpose of the processing***

The Data Processor is permitted to collect and process the Personal Data for the following purpose(s):

(i) to provide the services for the use of the Data Processor's software;
(ii) any other purposes instructed by the Data Controller in writing.

***Categories of Personal Data***

The processing activities involve Personal Data of the following categories. The security measures put in place by the Data Processor and any Sub-Processors must provide a level of security appropriate to the risk represented by the sensitivity of the Personal Data.

***Ordinary Personal Data***

- Name
- Title
- Email
- Address
- Telephone
- Social media
- Birthday
- Expenditure records
- Travel data
- Records of hours worked and general absence

***Sensitive Personal Data***

- Health status data
- Records of sickness absence

***Categories of Data Subjects***

- The Data Controller's end users
- The Data Controller's employees
- The Data Controller's customers
- The Data Controller's customers' employees
- The Data Controller's customers' contact persons

# APPENDIX 2

## DESCRIPTION OF TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

This Appendix contains a description of the technical and organisational security measures which the Data Processor is obliged, under the Data Processing Agreement, to implement, comply with and ensure compliance with by its Sub-Processors.

The Data Processor must as a minimum implement the following technical and organisational security measures to ensure an adequate level of protection.

***General security measures***

The Data Processor must ensure the implementation of security measures which ensure a level of security appropriate to the risk presented by the relevant categories of Personal Data.

The Data Processor must implement strong encryption of any collected passwords or access keys, as well as anonymization of Personal Data as risk-reducing factors where deemed relevant by the Data Processor.

The Data Processor must restrict access to the Personal Data to the relevant persons in order to comply with the requirements and obligations set out in the Agreement.

The Data Processor must implement systems which can prevent, detect and restore incidents relating to Personal Data. Any identified incidents must be reported to affected DataController(s).

The Data Processor must ensure that Personal Data are transferred to Sub-Processors in an appropriate and transparent manner.

The Data Processor must constantly evaluate whether the technical and organisational security measures implemented ensure adequate protection of the Personal Data, including pursuant to GDPR Article 32 on security of processing and Article 25 on data protection by design and by default.

The Data Processor has ensured that all Personal Data from the Data Controller or its representatives are accessed via an encrypted SSL connection.

The Data Processor has established a hosting platform which ensures that all Personal Data are safely stored, prevents unauthorised access to data, and provides backup systems ensuring that all data are restorable in case of hosting platform incidents.

Personal Data are anonymized in databases when the Data Processor accesses the Data Controller's data in connection with support.

The Data Processor has implemented software and routines to ensure that the internal level of IT security remains high at all times. Further information about security is available on Yodiwo's website.

***Authorisations and access control***

Personal Data are accessed using authorisation with a personal user name and password in the internal systems established by the Data Processor to comply with its obligations under the Agreement.

The Data Processor has ensured that Sub-Processors use personal authorisation and access control in connection with their services.

***External communication links***
Personal Data can be accessed only using an encrypted SSL or VPN connection.

***Monitoring of denied access attempts***
Denied access attempts are monitored routinely to ensure that no attempts are made to gain unauthorised access to the Data Controller's data.

***Logging***
The date, reason and identity of the Data Processor's representative are logged when Personal Data are accessed in the course of performing the Data Processor's obligations under the Agreement.
The above log records are routinely spot checked to ensure that Personal Data are accessed solely in accordance with the instructions under which the employee works.
Routine spot checks are made to ensure that Sub-Processors and their representatives access Personal Data only where relevant to the service provided by them or under direct instruction from the Data Processor.

***Home and/or remote workplaces***
The Data Processor's processing of Personal Data is performed, in whole or in part, from home and/or remote workplaces.
Personal Data are accessed using a personal VPN connection to the Data Processor's network or using a SSL connection and personal login to Helpdesk Software.

***Encryption of the Personal Data***
The passwords of the Data Controller's representatives are protected by encryption.

## APPENDIX3

## LIST OF PROCESSORS

| # | Country | Name | Address | Data Processing Operation |
|---|---|---|---|---|
| 1 | Sweden | YODIWO AB | Dalsro 308, 31161 Ullared | Cloud Services and Support |
| 2 | Greece | YODIWO AE | Innohub 4 Kastritsiou Str, 26504 Patras | Cloud Services and Support |
| 3 | Cyprus | YODIWO CYPRUS Ltd | Dromos 105, 18,PanoPolemidia, 4130, Limassol | Cloud Services and Support |