Workspace365

Processing Agreement

Content

Workspace 365 | Processing Agreement

As per article 5A of the Workspace 365 EULA we agreed with you that we shall provide you with a standard processing agreement which shall govern how we process personal data on your behalf. Below you shall find this agreement. It is entered into by New Day At Work B.V. Berencamperweg 6D, 3861MC Nijkerk ("we", "us" or "our" and the legal entity or business which is identified below ("you"). You can accept it by (i) downloading a signed .pdf copy from https://www.workspace365.net (our "website") and (ii) returning a fully signed electronic copy by e-mail to us.

1. Definitions

A. "**Agreement**" means this Workspace 365 Processing Agreement. "**Applicable Law**" means any legislation applicable to the processing, protection, confidentiality or the privacy of Personal Data, including but not limited to the GDPR. "**Disclosure**" means any form of disclosure of the Data or any copies thereof to a third party, including, but not limited to, the transfer of data to a third party and the (remote) access to the data by a third party (hereinafter also referred to "**Disclose**"). "**GDPR**" means the EU General Data Protection Regulation (EU Regulation 2016/679). "**Party**" means you or we. "**Parties**" means you and we together. **"Controller", "Processor", "Personal Data", Personal Data Breach"** and "**Processing**" all have the meaning that is assigned to these terms in article 4 of the GDPR. "**Third Party**" means any party other than the parties to this agreement. "**Transfer**" of Personal Data means forwarding, copying and providing remote access to Personal Data (hereinafter also referred to as a verb "**Transfers**"). "**User**" means the individual Workspace 365 user whose personal data is processed by us in connection with his use of Workspace 365.

2. Scope

A. Our provision of Workspace 365 to you may involve that we process personal data relating to your users. You agree that we only process personal data: (i) that is created and stored by you as part of your use of a Workspace 365 App (like a time sheet) or (ii) subscription information that is displayed in your Workspace 365 dashboard. Our obligations as a processor to you are limited to the personal data we have described in this article 2A and in further detail in **Appendix 1.**

B. You accept that any personal data that is included in documents which your users create in Workspace 365, are processed solely by Microsoft and shall be subject to the applicable Microsoft privacy policy and Microsoft processing agreement. We shall consequently not be bound to observe any instruction you may have in relation to the processing of personal data in Microsoft Office 365 or related official Microsoft Application Programming Interfaces (APIs).

3. Our obligations as a Processor

A. As a processor we:

1. shall conduct the processing in accordance with the applicable law, this agreement and all further reasonable commercial instructions you provide to us with regard to the processing;
2. shall perform the processing appropriately and accurately and only insofar as needed to provide you with Workspace 365; and shall not process personal data for purposes not authorized by you;
3. shall ensure that only our personnel (including the personnel of our Dutch hosting provider) to the extent required to provide you with Workspace 365 and enabling us to meet our obligations pursuant to this agreement shall have access to Personal Data and shall require such personnel to protect and maintain the confidentiality and the security of personal data;
4. shall implement the technical and organisational security measures, as specified in **Appendix 2**, to protect personal data against unauthorised or unlawful processing, accidental or unlawful destruction or accidental loss, alteration, damage, unauthorised disclosure or unauthorised access by any person;
5. shall not disclose personal data to any third party without your prior written approval except if this is our current hosting provider or if our disclosure is obligated by applicable mandatory law, for example after having been issued with a warrant from a competent law enforcement agency;
6. shall cooperate with you to address and resolve any complaints, requests or inquiries from users, as well as to address any investigations, inspections or audits by any public authority into your practices with respect to processing;
7. shall not transfer personal data outside of the territory of the EU without your prior approval.

B. We shall maintain in place procedures to enable you to comply with requests for information by users. All your requests for information shall be answered within four (4) weeks or as may be required by local law after receipt of the request. We shall not respond directly to users ourselves.

C. If you require so and provided you notify us well in advance we shall cooperate with you to perform any data protection risk assessments, perform prior consultations with competent data protection or privacy authorities or perform audits with regard to the processing, and shall in particular:

- ☑ provide you with access to any information which may be reasonably necessary to review our hosting facilities, procedures and documentation relating to the processing; and
- ☑ enable you to have a registered EDP audit us in accordance with article 7 below.

D. If our hosting provider notifies us of a suspected personal data breach involving your personal data, we shall inform you immediately after having received his notification by sending you an e-mail. This e-mail shall include the information that we have received from our hosting provider. If you require so we are happy to provide you with a copy of the processing agreement that we have with our hosting provider.

E. We shall not keep personal data any longer than necessary for the purpose of providing you with Workspace 365. Subject to our legal and regulatory obligations with regard to personal data we shall ensure that we and our hosting provider, when your subscription for Workspace 365 ends, shall return all personal data to you by providing you with a copy of the SQL Server table with your Workspace 365 App data. When we have done so we shall be responsible for destroying all personal data related to your users that it in our possession or in the possession of our hosting provider.

F. Subject to the provisions of this article, you hereby authorize and, where relevant, hereby instruct us to:

    1. to disclose personal data to our hosting provider; and

    2. to disclose personal data to a third party in order to comply with a legal obligation to which you, we or the user are subject, provided such disclosure is directly related to the provision of Workspace 365.

G. We currently use the sub-processors that are identified in **Appendix 1**. These sub-processors include our current hosting providers. You hereby approve our use of these sub-processors. When we start using other sub-processors or discontinue a sub-processor, we will tell you by e-mail no later than 30 days before the change becomes effective. If you do not agree with this change your only means of redress is to terminate the license for Workspace 365.

4. Your obligations as a Controller

A. As a controller you shall:

    a. Provide us with specific and documentated instructions with regard to the security and confidentiality of personal data in accordance with applicable data protection legislation;

    b. Inform us of any legitimate inspection or audit of the processing by any competent authority which relates to our processing;

    c. Inform us as soon as reasonably possible of any access request, request for correction or blocking of personal data or any objection related to our processing; and make sure that all of your instructions are in line with applicable law.

5. Liability

A. Parties to indemnify and hold each other, their representatives and employees harmless against any direct and substantiated losses, agreed fees, penalties, fines, direct claims, direct damages, direct, reasonable and substantiated costs and direct, reasonable out-of-pocket expenses (including external legal fees), and other direct and substantiated liabilities they have actually suffered as a result of the other party's material breach of any representations and warranties contained in this agreement, any data protection obligations or laws in any jurisdiction.

B. Our liability is limited to the maximum amount offered pursuant to the EULA that applies to your subscription.

6. Terms and Termination

A. This agreement shall be effective for the duration of your subscription for Workspace 365 unless terminated by either party in accordance with the terms and conditions of this agreement.

B. Upon termination or receipt of notice terminating this agreement, we shall as soon as reasonably possible act in accordance with article 3E above.

C. If a party has not remedied any material breach of this agreement notified to it by the other party within ten (10) days after receipt of such notice, the other party is entitled to terminate this agreement by notice to the failing party without prejudice to any other rights accruing under this agreement or in law.

D. This agreement may be terminated by the other party in the event that either party:

1. shall or can reasonably be expected to cease business in the ordinary course;
2. becomes insolvent;
3. makes a general assignment for the benefit of its creditors;
4. suffers or permits the appointment of a receiver or a manager for its business assets; or
5. avails itself or becomes subject to any proceeding under bankruptcy laws or any other statutes or laws relating to insolvency or protection of the rights of creditors.

7. Audit

A. For the duration of this agreement and with a maximum frequency of once per calendar year you shall be entitled to have a registered EDP auditor verify our compliance with the terms of this agreement and with any legislative, judicial and regulatory provision to which you and your organisation are subject to ("audit"). To enable an audit, we shall allow this EDP auditor access to: (i) our hosting facilities,

(ii) our personnel and (iii) our written policies, procedures, processes and controls. Our obligation to cooperate with your audit is limited to applying our commercially reasonable effort and is subject to compliance by you your EDP auditor with the access policies of our hosting provider.

B. Our obligation to cooperate with your audit is limited to applying our commercially reasonable effort and is subject to compliance by you your EDP auditor with the access policies of our hosting provider.

C. You shall give at least 30 days notice of an audit. Promptly after the issuance of any audit report or findings, you and we shall meet to review such audit report and findings. We shall consequently at our own expense, undertake reasonable all commercial reasonable remedial action to address and resolve any material deficiencies arising out of any audit.

D. Any audit shall not disrupt unreasonably disrupt our business operations.

E. Promptly after the issuance of any audit report or findings, you and we shall meet to review such audit report and findings. We shall consequently at our own expense, undertake reasonable all commercial reasonable remedial action to address and resolve any material deficiencies arising out of any audit.

F. You shall be responsible for the cost of the audit. If and to the extent the audit report identifies any material deficiencies we shall only be required to meet our obligations pursuant to article 7E. We shall not be required to pay you any related damages, including but not limited to the audit costs.

8. Governing Law

A. This agreement is governed by and construed in accordance with the laws of the Netherlands.

B. Any disputes arising out of, or in connection with this agreement shall be settled by the competent courts in the legal district of Midden-Nederland

9. Miscellaneous

A. Force Majeure

In the event of a Force Majeure situation (as defined hereinafter) the party being delayed shall inform the other party as soon as possible but in any event within three (3) days after the commencement of such Force Majeure situation specifying the nature of the Force Majeure situation as well as the estimated duration thereof. In the event the Force Majeure situation continues for a period of more than thirty (30) days, then either party is entitled to terminate this agreement together with the EULA for the subscription for Workspace 365 by simple notice in writing and without either party being liable for damages towards the other party. If the affected party does not wish to terminate this agreement in accordance with the

above, the respective parties' rights and obligations shall be suspended, and a new time schedule shall be agreed upon between the parties.

"Force Majeure" shall be understood to mean and include damage or delay caused by unavailability of telecommunications connections and underlying infrastructure, acts or regulations or decrees of any government (de facto or de jure) natural phenomena such as earthquakes and floods, fires, riots, wars, freight embargoes, lockouts or other causes whether similar or dissimilar to those enumerated above unforeseeable and beyond the reasonable control of the pertaining parties and which prevent the total or partial carrying out of any obligation pursuant to this Agreement.

Listing of Annexes

Annex 1 shall be deemed to form, be read and construed as an integral part of this agreement.

If any conflict appears between the terms and conditions of the body of this agreement and any of the above documents, the terms and conditions contained in the body of this agreement shall prevail.

As signed in duplicate on the dates identified below:

New Day at Work B.V.

By: New Day at Work
Name: Erik Nicolai
Position: CEO
Date:

Controller:

By:
Name:
Position:
Date:

Appendix 1 Details of processing of personal data

This Appendix 1 provides further details on the processing of personal data that we perform for you and our current hosting provider:

1. *Subject matter and duration of the processing*

The subject matter and duration of the processing of personal data are set out in the EULA for Workspace 365 and this Appendix 1.

2. *The nature and purpose of the processing*

Workspace 365 only collect user provided information.

3. *The types of Personal Data to be Processed*
   - Personal identifications data
     - Required: name, surname, business email, business phone
     - Optional: picture, title
   - In the business apps it is possible to store any data so also personal data. This depends how customers have configured the business apps in Workspace 365

4. *The categories of individuals to whom the personal data relates to*
   - Employee data of Workspace 365 end customers

5. *Our hosting provider*

Microsoft Azure.

Appendix 2 Technical and Organizational Measures

Pursuant to article 3.A.4. of this agreement, we shall:

1. adopt and implement policies and standards related to information security;
2. assign responsibility for information security management;
3. devote adequate personnel resources to information security;
4. perform background checks on permanent staff that shall have access to personal data (where practicable and lawful in each relevant jurisdiction);
5. require our employees, vendors and others to abide by our information security standards and other privacy policies (as such may be revised from time to time), which standards and policies may include confidentiality provisions;
6. conduct training to make employees aware of information security risks and to enhance compliance with our policies and standards relating to data protection;
7. have procedures in place in an attempt to prevent unauthorized access to personal data through the use, as appropriate, of physical and logical (password) entry controls, secure areas for processing and built in system audit trails;
8. protect personal maintained in online systems through the use, as appropriate, of secure passwords, network intrusion detection technology, encryption and authentication technology, secure log on procedures, and virus protection;
9. ensure compliance with our policies and standards related to data protection on an ongoing basis.