

Data processing agreement



 **Workspace365**
Everything Simplified.

Workspace 365 Processing Agreement

This is our standard processing agreement. It governs how we act as a processor of certain categories of your personal data. We are New Day At Work B.V. Berencamperweg 6D, 3861 MC Nijkerk ("we", "us" or "our" and the legal entity or business which is identified below ("you")). You can accept this agreement by (1) downloading a signed .pdf copy from <https://www.workspace365.net> (our "website") and (2) returning a fully signed electronic copy by email 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. The types of personal data which are processed by us on your behalf, and for which we act as your processor, are set out in Appendix 1. This agreement governs our duties as your processor.
- B. We have designed Workspace 365 in such a manner that you should be able to provide us with your instructions by means of the Workspace 365 admin dashboard. If by any chance you need to provide us with an instruction that is not accommodated by the dashboard, please send an email to privacy@workspace365.net. If any instruction in our reasonable opinion infringes applicable law, we will inform you immediately.
- C. You accept that: (i) any personal data processed by Microsoft or by a provider of an app for which we provide an integration in Workspace 365, is subject to the applicable Microsoft or app provider privacy policy and data processing agreement, and that (ii) Microsoft nor the app provider are a sub-processor of us.

3. Our obligations as a Processor

- A. As a processor we:
1. shall conduct the processing in accordance with applicable law, this agreement and all 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 authorised by you;
 3. shall only allow our personnel access to your personal data to the extent that this is strictly required to provide you with Workspace 365 and to enable us to meet our obligations pursuant to this agreement, and require such personnel to protect and maintain the confidentiality and the security of the personal data to which they have access to;
 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. except as specifically provided for in this agreement, shall not disclose personal data without your prior written approval;
 6. shall cooperate with you to address and resolve any complaints, requests or inquiries from users in connection with the exercise of their data subject rights, as well as to address any investigations, inspections or audits by any public authority into your practices with respect to the 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 or access to personal data 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 regarding 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 auditor 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 email. This email shall include the complete breach notification information that we have received from our hosting provider. If you require so, we are happy to provide you with a copy of the data 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. When your subscription for Workspace 365 ends all your personal data shall be deleted 24 November 2022 3 by or on behalf of us within 30 days of the last day of your subscription term. This may be different only for personal data which we need to retain under applicable law.
- F. Subject to the provisions of this article, you hereby authorise us to disclose personal data if we are legally obliged to do so, provided that we use reasonable legal resources to validate our obligation. We will always try to inform you prior to our disclosure taking place. It may be however that we are prohibited by applicable law to do so.
- G. We currently use the sub-processors identified in Appendix 1. We have done our best to enter into subprocessing agreements with these sub-processors that are in substance comparable to this agreement. You hereby approve our use of these sub-processors. When we start using other sub-processors or discontinue a current sub-processor, we will tell you by email 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 licence for Workspace 365.

4. Your obligations as a Controller

- A. As a controller you shall:
 1. provide us with specific and documented instructions regarding the security and confidentiality of personal data in accordance with applicable data protection legislation;
 2. inform us of any legitimate inspection or audit of the processing by any competent authority which relates to our processing;
 3. 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 that you may have received from user; and
 4. make sure that all 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 value in EURO of your subscription, provided you fully paid for your subscription. We shall not be held liable for any damages resulting from the processing of personal data by Microsoft and by any providers of apps for which we provide an integration in Workspace 365.

6. Term and Termination

- A. This agreement shall run for the duration of your subscription for Workspace 365.
- B. Upon termination of this agreement, we shall as soon as reasonably possible, act in accordance with article 3E above.

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 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 auditor access to: (i) our hosting facilities, (ii) our personnel and (iii) our written policies, procedures, processes, and controls.
- B. Our obligation to cooperate with your audit is limited to applying our commercially reasonable effort and is subject to compliance by your auditor with the access policies of our hosting provider.
- C. You shall give at least 14 days' notice of an audit.
- D. Any audit shall not 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 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 subject to the laws of the Netherlands.
- B. Disputes shall be settled by the competent courts in the legal district of Midden-Nederland.

9. Miscellaneous

- A. Listing of Appendices
Appendix 1 and Appendix 2 are 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 Appendices, 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.	[controller]
By:	By:
Name:	Name:
Position:	Position:
Date:	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

Provide the functionality of Workspace 365 including access to Micro Apps to your users.

3. The types of Personal Data to be Processed

Data category	Types of data
Authentication data	User principal name (Email) <i>[required]</i>
	Given name <i>[required]</i>
	Family name <i>[required]</i>
	Integration Username of user <i>[optional]</i> (CRDP-WebDAV)
Personal data	Language <i>[required]</i>
	Phone number of user <i>[optional]</i>
	Profile picture of user <i>[optional]</i>
	Job title of user <i>[optional]</i>
	Birthday of user <i>[optional]</i>
	Department of user <i>[optional]</i>
	Location of Company <i>[optional]</i>
	Secondary email of user <i>[optional]</i>
	About me <i>[optional]</i>
Working Days <i>[optional]</i>	

	Projects <i>[optional]</i>
	Skills and Expertise <i>[optional]</i>
	Schools and Education <i>[optional]</i>
	Interest and Hobbies <i>[optional]</i>
Mobile App	Platform
	Device Model Name
	Device Model Manufacturer
Hub	Depending on data inserted by a Workspace 365 administrator or author; for example, a birthday announcement or announcement related to a change in position.
Micro Apps API data	We ingest a live data feed through the API of a Micro App and relay it to the user. This live feed may include personal data.
Activity Feed data	This is interaction data of the user with a Micro App through an API connection. This activity feed is stored in a database within the Workspace 365 platform.
Customer API data	Depending on data inserted by a Workspace 365 administrator; for example, company news, data is stored in a database within the Workspace 365 platform.

4. *The categories of individuals to whom the personal data relates to*

Your Workspace 365 users. These are generally employees or consultants of our customers.

5. *Our hosting provider and other sub-processors*

Microsoft (Microsoft Azure platform), Pendo (Analytics), Dynatrace (Monitoring), Coralogix (Logging)

Appendix 2

Technical and Organisational 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 unauthorised 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