Data processing agreement

Workspace365

Everything Simplified.

Workspace 365 Processing Agreement

This Data Processing Agreement (DPA) outlines how we process Personal Data on your behalf as part of our services. We are New Day At Work B.V., located at Berencamperweg 6D, 3861 MC Nijkerk, the Netherlands ("we," "us," or "our"). By signing the main agreement for Workspace 365, you ("you" or "the customer") also agree to the terms of this DPA, which forms an integral part of that agreement.

1. Definitions

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

2. Scope

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.

We have designed Workspace 365 in such a manner that you should be able to provide us with your instructions additional to this DPA by means of the Workspace 365 admin dashboard, only in writing. 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.

You understand 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 1 calendar month 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 we become aware of a Personal Data Breach involving your Personal Data, whether directly or via our hosting provider, we will notify you without undue delay
The notification will include:
    - a description of the breach,
    - the type of data affected,
    - number of impacted individuals (if known),
    - likely consequences, and
    - any mitigation actions taken.

    We will assist you with any necessary notifications to supervisory authorities or data subjects under Article 33 or 34 of the GDPR, as applicable.

E. We will not retain Personal Data longer than necessary to provide Workspace 365. Retention periods are as follows:
    - User account data: deleted within 30 days after subscription ends.
    - Platform logs and metadata (e.g. login, activity logs): retained for 90 days.
    - Backups: retained for 35 days, then permanently deleted.
    - Analytics/telemetry data: retained for a maximum of 13 months, then aggregated or anonymised.

    You may request earlier deletion of any data categories during your active subscription via written request.

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 also maintain a live list of active sub-Processors at our support portal, which you may reference at any time. You agree that we may engage new sub-processors at our discretion without obtaining your prior approval, provided that we notify you via our support portal with such additions or changes within fourteen (14) days after they take effect

H. We support your data protection obligations by design. Upon written request, we will:
    - Provide DPIA-related information including architecture diagrams, data flow summaries, and technical controls;
    - Describe how Workspace 365 enforces role-based access, audit trails, and data minimisation.

    We aim to respond to such requests within 10 business days unless otherwise agreed

I. Workspace 365 is developed and operated under an ISO 27001 certified Information Security Management System (ISMS). Certification reports and Statements of Applicability (SoA) can be shared under NDA upon request. Security measures implemented under this framework are described in Appendix 2 and/or our Security Summary.

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. Notwithstanding anything to the contrary in this Agreement, our aggregate liability for any and all claims arising out of or relating to this DPA shall be limited to the total fees paid by you under the applicable subscription during the twelve (12) months preceding the event giving rise to liability; provided, however, that this limitation shall not apply to (a) any fines or penalties imposed under applicable data protection laws (including the GDPR), or (b) any damages resulting from our own gross negligence or wilful misconduct. 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, since this is an direct relationship between customer and vendor following their DPA's.

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 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 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.

Appendix 1

Details of processing of Personal Data

This appendix outlines the categories of Personal Data we process on your behalf through Workspace 365, the purposes of processing, and the systems involved. All data is hosted in our Azure-based environment, which is fully controlled and maintained by us. Subject matter and duration of the processing

1. Subject matter and duration
The subject matter of processing is the provision of the Workspace 365 platform to you and your users. This processing continues for the duration of your active subscription and is governed by the main agreement and this DPA.

2. Nature and purpose of processing
We process Personal Data to:

- Provide users with access to Workspace 365 and its features;
- Support collaboration, customization, and personalization across the product e.g. Live Tiles, Communities, the Hub, AI;
- Enable admin functionality and integration with third-party systems;
- Monitor product usage, diagnose issues, and improve performance;
- Secure the environment and investigate security incidents where necessary.
- We may process limited user metadata (such as job title) for the purpose of usage analytics and UX optimisation via Pendo, a sub-Processor.

Use of AI Assistant
Workspace 365 includes an AI-powered assistant that helps users interact with the platform more efficiently. It can generate responses or summaries based on:

- Workspace 365 content (e.g. Knowledgebase, Communities, activity logs),
- Data made available through customer-configured integrations via the Workspace 365 Integration Framework.

The assistant only accesses external systems that have been explicitly connected and authorised by Workspace 365 administrators.

The assistant uses a model hosted within our own Azure environment via Azure OpenAI EU . UK / US / AU region – and more depending on customer location. All inference happens in this environment, and no customer data is used for model training or shared outside the customer region.

3. Types of Personal Data processed

A. Authentication and profile data

Category	Fields
Authentication	User principal name (email) [required], given name [required], family name [required], integration username (e.g. CRDP/WebDAV) [optional]
Personal Info	Language [required], phone number, profile picture, job title, birthday, department, location, secondary email, "about me", time zone, working days, projects, skills, education, interests, hobbies (all optional)

B. Mobile app device Info

Category	Description
Platform	Details used for troubleshooting and interface adaptation
Model	Name, manufacturer, OS/platform

C. Content within Workspace 365

Area	Description
Hub	Articles, announcements, and change notifications. Includes titles, body text, optional author names, timestamps.
Communities	User-generated posts, comments, usernames, optional avatars, and optional file attachments. May include any content entered by users.
Customer API Content	Admin-inserted content such as company news or updates, stored in the Workspace 365 database.

D. Environment analytics

Metric	Scope
Feature usage	Toggle events, click paths, page views, UI behaviour

Note: These metrics are collected anonymously or pseudonymously where possible. Analytics via Pendo (a hosted service) is anonymized.

4. Logging and observability

We use Elasticsearch (self-hosted in Azure) for logging application and system-level events, which may contain:

- IP addresses
- Request metadata (URLs, user agent)
- User IDs (internal platform references)

These logs are used for platform monitoring, diagnostics, and security auditing. We also store Hub and Communities content in indexed form to enable fast in-app search.

Logs are retained for a maximum of 90 days and access is strictly limited to authorized personnel under role-based access control.

5. Ecosystem - Integration framework data

Workspace 365 includes an integration framework allowing administrators to connect external systems (e.g., HR platforms, ticketing tools, reporting tools).

We store:

- Configuration metadata (e.g., integration name, target system)
- API credentials (e.g., OAuth2 tokens, API keys) entered by the customer
- Connection logs or health check results

Credentials are stored encrypted at rest. The customer is responsible for entering and maintaining secure secrets.

6. Categories of Data Subjects

- End-users of Workspace 365 (e.g. employees, contractors, partners)
- Workspace administrators (managing settings, integrations, and content)
- Use of the AI assistant is optional and subject to the permissions and content scope set by Workspace 365 administrators. Customers are responsible for controlling which content (e.g. Knowledgebase, Communities) is available to the assistant.

7. Hosting and AI infrastructure

Workspace 365 is hosted in Microsoft Azure (user region) under our full administrative control. In addition, we use the following components for analytics, observability, and AI functionality:

Component	Purpose	Location	Notes
Microsoft Azure	Primary hosting and storage (all data types)	EU / UK / US / AU region and more - depending on customer location	Primary Processor environment under our control
Pendo	Product usage analytics and persona insights	EU / U.S. (depending on customer location)	Used in anonymised form; Used to segment user behaviour by role/persona. Job title is passed via configuration by admin. No message content or sensitive data is processed.
Elasticsearch (self-hosted)	Logging, search indexing (e.g. Hub, Communities)	EU / UK / US / AU region and more - depending on customer location	No external sub-Processor involved
Azure OpenAI	AI assistant responses (inference only)	EU / UK / US / AU region and more - depending on customer location	Data processed via GPT-4+ model hosted in our Azure subscription; no training or fine-tuning occurs

Appendix 2

Security Measures (aligned with ISO 27001)

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 Data 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