DATA PROCESSING ADDENDUM
My-DO

Last updated: 06/05/2026

This Data Processing Addendum, including its Exhibits, (the “Data Processing Addendum” or “DPA”) forms part of and supplements the agreement, terms of service, order form or other written agreement entered into by and between Digita SRL and the Customer governing the provision and use of My-DO (the “Agreement”).

This DPA applies only where Digita SRL processes Personal Data on behalf of a Customer in connection with the provision of My-DO and the related SaaS services, including where My-DO is used by a business, professional, institutional or public-sector customer.

Where My-DO is provided directly to an individual consumer for personal, household or non-professional purposes, Digita SRL may act as an independent data controller for the personal data processed to provide and manage that consumer service. In such case, this DPA does not apply, and the processing is governed by Digita SRL’s Privacy Policy and the applicable Consumer Terms of Service.

1. Definitions

For the purposes of this DPA:

(a) “Agreement” means the service agreement, terms and conditions, order form, quotation, subscription plan or other written agreement entered into by and between the Parties, governing the provision of My-DO by Digita SRL to the Customer. This DPA is incorporated into the Agreement by reference.

(b) “Applicable Data Protection Laws” means any applicable privacy, data protection, data security or electronic communications law or regulation, including, to the extent applicable, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, applicable since 25 May 2018 (the “GDPR”), any applicable national implementing laws, and any other privacy or data protection laws applicable to the Processing.

(c) “Customer Data” has the meaning given in the Agreement and includes data, documents, files, prompts, queries, knowledge base content, system instructions, user interactions, configurations and other materials provided, uploaded, submitted, configured or made available by or on behalf of the Customer through My-DO.

(d) “Description of Processing” means the description of the Processing set out in Exhibit 1 of this DPA.

(e) “International Data Transfer” means any transfer of Personal Data to a country outside the European Economic Area or another jurisdiction subject to data transfer restrictions, where such country does not benefit from an adequacy decision or equivalent lawful transfer mechanism under Applicable Data Protection Laws.

(f) “My-DO” means the AI-powered knowledge management platform and related SaaS services provided by Digita SRL to the Customer under the Agreement.

(g) “Personal Data” means any Customer Data that constitutes “personal data”, “personal information” or an equivalent term under Applicable Data Protection Laws and that Digita SRL processes on behalf of the Customer as Processor.

(h) “Processing” or “Process” means any operation or set of operations performed on Personal Data, whether or not by automated means, as further described in Exhibit 1.

(i) “Restricted Country” means any country outside the European Economic Area that does not benefit from an adequacy decision from the European Commission or another competent authority, where applicable.

(j) “SCCs” means the standard contractual clauses adopted by the European Commission for the transfer of personal data to third countries, including the clauses annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as amended, replaced or supplemented from time to time. The European Commission issued modernised SCCs for transfers from controllers or processors in the EU/EEA to recipients in third countries.

(k) “Subprocessor” means any processor appointed by Digita SRL to carry out all or part of the Processing on behalf of the Customer.

(l) “Services” means My-DO and the related SaaS, support, hosting, storage, backup, API, technical and operational services provided by Digita SRL under the Agreement.

The terms “Controller”, “Processor”, “Data Subject”, “Personal Data Breach”, “Subprocessor” and “Supervisory Authority” shall have the meanings given to them under Applicable Data Protection Laws. Capitalised terms not defined in this DPA shall have the meaning given to them in the Agreement.

2. Role of the Parties and Description of the Processing

2.1 Role of the Parties

For the Processing of Personal Data under this DPA, the Customer is the Controller and Digita SRL processes Personal Data on behalf of the Customer as Processor.

This DPA applies only where a Customer determines the purposes and means of the Processing and instructs Digita SRL to process Personal Data on its behalf.

Where My-DO is provided directly by Digita SRL to an individual consumer for personal, household or non-professional purposes, Digita SRL may determine the purposes and means of the processing and may therefore act as an independent Controller. Such consumer processing is not governed by this DPA and is instead governed by Digita SRL’s Privacy Policy and the applicable Consumer Terms of Service.

Where the Customer acts as Processor on behalf of another Controller, Digita SRL shall act as Subprocessor, and the Customer represents and warrants that it has all necessary rights, authorisations and instructions from the relevant Controller to appoint Digita SRL as

Subprocessor and to instruct Digita SRL to Process Personal Data in accordance with this DPA and the Agreement.

2.2 Description of the Processing

The subject matter, duration, nature and purpose of the Processing, the categories of Data Subjects and the categories of Personal Data are described in Exhibit 1.

Digita SRL may update the Description of Processing from time to time to reflect new My-DO features, functionalities, subscription plans, subprocessors or technical configurations, provided that such updates do not materially reduce the level of protection afforded to Personal Data under this DPA.

2.3 Digita SRL as Independent Controller

Digita SRL may process certain personal data as an independent Controller for its own purposes, including account administration, customer relationship management, contracts, invoicing, tax and accounting obligations, support, security, fraud prevention, abuse prevention, website forms, demo requests, commercial communications, service communications, legal compliance and establishment, exercise or defence of legal claims. Such processing is not governed by this DPA and is governed by Digita SRL's applicable privacy policy.
For clarity, Digita SRL does not use Customer Data or Outputs to train, fine-tune or improve general-purpose AI models by default, unless expressly agreed in writing with the Customer or otherwise set out in the Agreement or an applicable Order Form.

This also includes cases where Digita SRL provides My-DO directly to an individual consumer for personal, household or non-professional purposes, including private or consumer solutions expressly made available by Digita SRL. In such cases, Digita SRL may act as an independent Controller for the personal data processed to provide, administer, secure, support and bill the consumer service, and such processing is governed by Digita SRL's Privacy Policy and the applicable Consumer Terms of Service.

3. General Obligations of the Parties

3.1 Obligations of Digita SRL

Digita SRL shall:
(a) Process Personal Data only on documented lawful instructions from the Customer, including the Agreement, this DPA, the applicable Order Form, Customer configurations and lawful instructions provided through My-DO, unless required to do otherwise by applicable law;
(b) promptly inform the Customer if, in Digita SRL's opinion, an instruction infringes Applicable Data Protection Laws, in which case Digita SRL may suspend or refuse to perform the relevant Processing to the extent permitted or required by applicable law;
(c) ensure that persons authorised to Process Personal Data, including employees, contractors and Subprocessors, are subject to appropriate confidentiality obligations;
(d) implement and maintain appropriate technical and organisational measures designed to protect Personal Data in accordance with Section 5 and Exhibit 2;
(e) assist the Customer, taking into account the nature of the Processing and the information available to Digita SRL, in complying with the Customer's obligations under Applicable Data Protection Laws, including obligations relating to security, Personal Data

Breaches, data protection impact assessments, prior consultations and Data Subject requests;
(f) make available to the Customer information reasonably necessary to demonstrate compliance with this DPA, subject to confidentiality, security and trade secret limitations;
(g) notify the Customer without undue delay if Digita SRL determines that it can no longer meet its obligations under this DPA;
(h) comply with the obligations applicable to Digita SRL as Processor under Applicable Data Protection Laws.

3.2 Obligations of the Customer

The Customer shall:

(a) comply with all obligations applicable to it under Applicable Data Protection Laws;
(b) ensure that all instructions given to Digita SRL are lawful, documented, complete and consistent with Applicable Data Protection Laws;
(c) have and maintain all rights, legal bases, notices, consents, authorisations and permissions required for Digita SRL to Process Personal Data in accordance with this DPA and the Agreement;
(d) ensure that Personal Data included in Customer Data, knowledge base content, prompts, system instructions, documents and Outputs is accurate, relevant, limited to what is necessary and lawfully processed;
(e) configure access rights, user permissions, knowledge base governance, retention settings and security controls appropriately;
(f) not upload or process special categories of Personal Data, criminal conviction data, highly sensitive data, classified information, export-controlled data or other restricted data through My-DO unless expressly permitted by the Agreement or an Order Form and unless appropriate legal bases and safeguards are in place;
(g) be responsible for responding to Data Subject requests and Supervisory Authority requests, except to the extent Digita SRL is legally required to respond directly.

4. Data Subjects

4.1 Customer Responsibility
The Customer is responsible for providing Data Subjects with all information required by Applicable Data Protection Laws and for responding to requests from Data Subjects exercising their rights in relation to the Processing.

4.2 Assistance by Digita SRL
Taking into account the nature of the Processing and upon the Customer’s written request, Digita SRL shall provide commercially reasonable assistance to enable the Customer to respond to Data Subject requests under Applicable Data Protection Laws.

4.3 Requests Sent Directly to Digita SRL
If a Data Subject request relating to Personal Data processed on behalf of the Customer is made directly to Digita SRL, Digita SRL shall not respond to such request directly unless authorised by the Customer or required by applicable law.

Where appropriate, Digita SRL may redirect the request to the Customer. If Digita SRL is legally required to respond directly, Digita SRL shall notify the Customer unless prohibited by applicable law.

5. Security

5.1 Security Measures

Taking into account the state of the art, implementation costs, the nature, scope, context and purposes of the Processing, and the risk of varying likelihood and severity for the rights and freedoms of natural persons, Digita SRL shall implement and maintain appropriate technical and organisational measures designed to protect Personal Data against unauthorised access, accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

The security measures implemented by Digita SRL are described in Exhibit 2.

The Customer acknowledges that security measures may be updated from time to time to reflect technical progress, operational changes, security developments and changes to My-DO, provided that such updates do not materially decrease the overall security of the Processing.

5.2 Customer Security Responsibilities

The Customer is responsible for the security of its own systems, devices, networks, credentials, user accounts, access permissions, endpoint protection, internal authorisations and use of My-DO by authorised users.

6. Personal Data Breach

6.1 Notification

Digita SRL shall notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Personal Data processed on behalf of the Customer.

Notification of or response to a Personal Data Breach shall not be construed as an admission of fault or liability by Digita SRL.

6.2 Notification Content

To the extent available, the notification shall include:
(a) the name and contact details of Digita SRL’s point of contact;
(b) a description of the nature of the Personal Data Breach;
(c) the categories and approximate number of Data Subjects concerned, where known;
(d) the categories and approximate number of Personal Data records concerned, where known;
(e) the likely consequences of the Personal Data Breach, where known;
(f) the measures taken or proposed by Digita SRL to address the Personal Data Breach;
(g) measures that the Customer may take to mitigate possible adverse effects.

Where not all information is available at the time of the initial notification, Digita SRL may provide information in phases as it becomes available.

6.3 Assistance

Upon the Customer's written request, and taking into account the nature of the Processing and the information available to Digita SRL, Digita SRL shall provide commercially reasonable assistance to support the Customer's assessment, notification, mitigation and remediation obligations in relation to the Personal Data Breach.

7. Subprocessing

7.1 General Authorisation

The Customer grants Digita SRL a general written authorisation to engage Subprocessors to assist in the provision, maintenance, security and support of My-DO and the Processing of Personal Data.

Digita SRL shall:
(a) maintain an up-to-date list of Subprocessors in Exhibit 3 of this DPA or otherwise make such list available to the Customer upon request;
(b) enter into a written agreement with each Subprocessor imposing data protection obligations substantially equivalent to those set out in this DPA, to the extent applicable to the services provided by the Subprocessor;
(c) remain liable to the Customer for the performance of its Subprocessors' data protection obligations in relation to the Processing, subject to the limitations of liability set out in the Agreement.

7.2 Current Subprocessors

As of the date of this DPA, the Customer authorises the use of the Subprocessors listed in Exhibit 3, including the following:

(a) GitLab, for website management, code repository management, development workflow, project management and technical operations related to My-DO. GitLab may rely on the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, Standard Contractual Clauses or other lawful transfer mechanisms, as applicable.
(b) Amazon Web Services (AWS), for cloud infrastructure, storage, hosting, backup, vector database storage, security, availability and disaster recovery. AWS may rely on Standard Contractual Clauses, adequacy decisions or other lawful transfer mechanisms, as applicable.
(c) OpenAI, for API calls, AI model processing and generation of Outputs in connection with My-DO. OpenAI may rely on Standard Contractual Clauses, adequacy decisions, the UK Addendum or other lawful transfer mechanisms, as applicable.
(d) Stripe, in the future, for payment processing, subscription billing, invoicing support, payment authentication, payment fraud prevention and related financial operations. Stripe may rely on Standard Contractual Clauses, adequacy decisions or other lawful transfer mechanisms, as applicable. Stripe shall become an active Subprocessor only once payment processing or subscription billing through Stripe is enabled for My-DO.

7.3 Notification of New Subprocessors

Digita SRL shall provide reasonable notice of any intended addition or replacement of a Subprocessor. Notice may be provided by email, Customer Account notification, publication of an updated Subprocessor list, update to this DPA or another reasonable communication method.

The Customer may object in writing to the appointment of a new Subprocessor within ten (10) days of receiving notice, by contacting Digita SRL at info@digita.work, provided that the objection is based on reasonable grounds relating to Applicable Data Protection Laws.

If the Customer objects within the ten (10) day period, the Parties shall consult in good faith to find a commercially reasonable solution. If no reasonable solution is available, Digita SRL may terminate the affected Services or the Agreement to the extent the Subprocessor is necessary for the provision of My-DO.

If the Customer does not object within the ten (10) day period, the new Subprocessor shall be deemed authorised.

8. International Data Transfers

8.1 General Authorisation

The Customer authorises Digita SRL and its Subprocessors to transfer Personal Data to countries that have been recognised as providing an adequate level of protection under Applicable Data Protection Laws.

The Customer also authorises Digita SRL and its Subprocessors to perform International Data Transfers where appropriate safeguards are implemented in accordance with Applicable Data Protection Laws, including, as applicable, adequacy decisions, Standard Contractual Clauses, the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, supplementary measures, or any other lawful transfer mechanism recognised under Applicable Data Protection Laws.

8.2 Transfers Involving OpenAI

Where Digita SRL uses OpenAI as a Subprocessor for API calls, AI model processing and generation of Outputs in connection with My-DO, Personal Data may be transferred to or accessed by OpenAI entities or subprocessors outside the European Economic Area, Switzerland or the United Kingdom.

For Personal Data originating from the European Economic Area or Switzerland, OpenAI states that OpenAI Ireland Limited processes such data and, where transfers outside the European Economic Area or Switzerland are required to provide the services, such transfers are based on agreements containing Standard Contractual Clauses or on an adequacy decision issued by the European Commission under Article 45 GDPR.

For Personal Data originating from the United Kingdom, OpenAI states that the relevant processing is subject to the applicable UK data protection transfer mechanisms, including the UK Addendum to the Standard Contractual Clauses where applicable.

Digita SRL shall rely on the applicable data processing terms, transfer mechanisms and safeguards made available by OpenAI for such processing, to the extent OpenAI is used as a Subprocessor for My-DO.

8.3 Transfers Involving GitLab

Where Digita SRL uses GitLab as a Subprocessor for website management, code repository management, development workflow, project management or technical operations related to My-DO, Personal Data may be transferred to or accessed by GitLab entities or subprocessors outside the European Economic Area, Switzerland or the United Kingdom.

GitLab states in its data processing terms that transfers of Personal Data from customers in the EEA, the United Kingdom or Switzerland to GitLab, Inc. in the United States may take place under the Data Privacy Framework, and that where the Data Privacy Framework is suspended, invalidated, unavailable, not relied upon or where a restricted transfer occurs, the Standard Contractual Clauses apply. GitLab also provides jurisdiction-specific terms for UK and Swiss transfers.

Digita SRL shall rely on the applicable data processing terms, transfer mechanisms and safeguards made available by GitLab for such processing, to the extent GitLab is used as a Subprocessor for My-DO.

Where Digita SRL uses Amazon Web Services as a Subprocessor for cloud infrastructure, storage, hosting, backup, S3 bucket storage, vector database storage, disaster recovery, security or related service components, Personal Data may be processed within the AWS region selected by Digita SRL for the relevant service component.

As of the date of this DPA, Customer documents uploaded to My-DO and stored in the S3 bucket are hosted in AWS Europe (Stockholm). Other AWS regions, including AWS Europe (Milan), may be enabled in Digita SRL's AWS account but are not used for the storage of Customer-uploaded documents unless expressly configured or agreed.

Depending on AWS support, maintenance, security, subprocessors and service configuration, Personal Data may be accessed from or transferred to jurisdictions outside the European Economic Area, Switzerland or the United Kingdom. Digita SRL shall rely on the applicable data processing terms, transfer mechanisms and safeguards made available by AWS, including Standard Contractual Clauses, adequacy decisions or other lawful transfer mechanisms where applicable.

8.5 Transfers Involving Stripe

Where Digita SRL enables Stripe as a Subprocessor for payment processing, subscription billing, invoicing support, payment authentication, fraud prevention and related financial operations, Personal Data may be transferred to or accessed from jurisdictions outside the

European Economic Area, Switzerland or the United Kingdom depending on Stripe's service configuration, entities and subprocessors.

Digita SRL shall rely on the applicable data processing terms, transfer mechanisms and safeguards made available by Stripe, including Standard Contractual Clauses, adequacy decisions or other lawful transfer mechanisms where applicable.

Stripe shall become an active Subprocessor only once payment processing or subscription billing through Stripe is enabled for My-DO.

8.6 Customer Located in a Restricted Country

Where the Customer is located in a Restricted Country and Digita SRL transfers Personal Data back to the Customer or makes Personal Data available to the Customer from the European Economic Area, Switzerland, the United Kingdom or another jurisdiction subject to data transfer restrictions, the Parties shall implement the appropriate Standard Contractual Clauses module, UK Addendum, Swiss transfer terms or other lawful transfer mechanism, where required by Applicable Data Protection Laws.

Where applicable, the Standard Contractual Clauses shall be completed as follows unless otherwise agreed by the Parties:

(a) the data exporter and data importer shall be identified according to the roles of the Parties in the relevant transfer;
(b) the optional docking clause in Clause 7 shall apply, unless otherwise required by the applicable transfer mechanism;
(c) the optional redress clause in Clause 11(a) shall not apply, unless required by applicable law;
(d) the governing law shall be the law of Italy, where permitted by the Standard Contractual Clauses;
(e) the competent courts shall be the courts of Italy, where permitted by the Standard Contractual Clauses;
(f) Annexes I and II to the Standard Contractual Clauses shall be deemed completed by Exhibits 1 and 2 of this DPA;
(g) Annex III to the Standard Contractual Clauses shall be deemed completed by Exhibit 3 of this DPA, where applicable.

8.7 Conflict with Transfer Clauses

In the event of any conflict or inconsistency between this DPA and the applicable Standard Contractual Clauses, UK Addendum, Swiss transfer terms or other mandatory data transfer mechanism, the applicable transfer mechanism shall prevail to the extent of such conflict or inconsistency.

9. Audit and Compliance

9.1 Documentation Audit

Upon the Customer's written request, Digita SRL shall make available information reasonably necessary to demonstrate compliance with this DPA, to the extent commercially reasonable and required by Applicable Data Protection Laws, subject to confidentiality, security, intellectual property and trade secret limitations.

Such information may include summaries of security measures, relevant policies, certifications, audit summaries, subprocessors information, data flow information or other documentation reasonably available to Digita SRL.

9.2 On-Site Audit

Only to the extent the Customer cannot reasonably verify Digita SRL's compliance with this DPA through the documentation audit described in Section 9.1, and where required by Applicable Data Protection Laws, the Customer may request an on-site audit no more than once per calendar year, subject to the following conditions:

(a) the Customer must provide at least ninety (90) days' prior written notice;
(b) the audit shall be conducted by an independent auditor jointly selected by the Parties, with appropriate expertise, independence and impartiality, and who is not a direct or indirect competitor of Digita SRL;
(c) the auditor shall be bound by confidentiality obligations acceptable to Digita SRL;
(d) the audit shall be conducted during Digita SRL's regular business hours;
(e) the audit shall be limited to information, systems and Processing activities relevant to the Customer's Personal Data;
(f) the audit shall not unreasonably interfere with Digita SRL's business operations, security, confidentiality, service availability or obligations to other customers;
(g) the audit shall not require Digita SRL to disclose trade secrets, confidential information of other customers, information that would compromise security, or information protected by legal privilege;
(h) the audit costs shall be borne by the Customer;
(i) an identical copy of the audit report shall be provided to both Parties and shall be treated as Digita SRL's Confidential Information.

10. Return or Deletion of Personal Data

10.1 Return or Deletion

Following termination or expiration of the Agreement, Digita SRL shall delete or return Personal Data processed on behalf of the Customer in accordance with the Agreement, this DPA, the applicable Order Form, deletion policies, backup retention policies and Applicable Data Protection Laws.

Unless otherwise agreed in writing, the Customer must export any Customer Data, knowledge base content, Outputs or other Personal Data it wishes to retain before the termination or expiration of its access to My-DO, where export functionality is available.

10.2 Backup Copies

The Customer acknowledges that residual copies of Personal Data may remain in backups, logs or disaster recovery systems for a limited period after deletion from production systems.

Such backup copies shall remain protected in accordance with this DPA and shall be deleted or overwritten in accordance with Digita SRL's backup retention cycle, unless retention is required by applicable law, legal obligation, dispute management or security purposes.

10.3 Legal Retention

Digita SRL may retain Personal Data to the extent required by applicable law, regulatory obligation, accounting obligation, legal process, dispute resolution, security investigation or establishment, exercise or defence of legal claims.

Any retained Personal Data shall remain subject to the protections of this DPA for as long as it is retained.

11. General

11.1 Term

This DPA shall commence on the earlier of:

(a) the effective date of the Agreement; or
(b) the date on which Digita SRL first Processes Personal Data on behalf of the Customer.

This DPA shall remain in force for the duration of the Agreement and for as long as Digita SRL processes Personal Data on behalf of the Customer.

11.2 Incorporation and Conflict

This DPA is incorporated into the Agreement by reference and forms an integral part of the Agreement.
In the event of conflict between this DPA and the Agreement with respect to the Processing of Personal Data on behalf of the Customer, this DPA shall prevail to the extent of the conflict.
In the event of conflict between this DPA and the SCCs, the SCCs shall prevail to the extent required by Applicable Data Protection Laws.

11.3 Liability

The liability of each Party and its affiliates under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement, except to the extent such exclusions or limitations are prohibited by Applicable Data Protection Laws.

11.4 Changes to this DPA

Digita SRL may update this DPA from time to time to reflect changes in Applicable Data Protection Laws, My-DO features, security measures, Subprocessors, technical architecture, data flows or business operations.

Where an update materially affects the Processing of Personal Data or the Customer's rights under this DPA, Digita SRL shall provide reasonable notice to the Customer.

12. Specific Privacy Laws

12.1 Applicability

The terms in this Section apply only where the corresponding privacy law applies to the Processing of Personal Data.

12.2 CCPA / CPRA

To the extent the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and its implementing regulations (collectively, "CCPA") apply to the Processing of Personal Data, Digita SRL shall act as a "service provider" or "contractor", as applicable, and shall not:

(a) sell or share Personal Data, as those terms are defined under the CCPA;
(b) retain, use or disclose Personal Data for any purpose other than for the business purposes specified in the Agreement and this DPA;
(c) retain, use or disclose Personal Data outside the direct business relationship between Digita SRL and the Customer, except as permitted by the CCPA;
(d) combine Personal Data with personal data received from or on behalf of another person, or collected from Digita SRL's own interaction with Data Subjects, except as permitted by the CCPA.

Digita SRL certifies that it understands and will comply with the restrictions set out in this Section where the CCPA applies.

EXHIBIT 1
Description of the Processing

1. List of Parties

Controller:
The Customer, as identified in the Agreement or applicable Order Form.

Processor:
Digita SRL, Via Verdi 3, 24121 Bergamo, Italy.
VAT / Tax Code: 04334180165.
Company identification number: IT04334180165.
PEC: pec.digita@legalmail.it.
Contact email: info@digita.work.

2. Subject Matter of the Processing

The Processing of Personal Data by Digita SRL on behalf of the Customer in connection with the provision, maintenance, support, security and operation of My-DO, an AI-powered knowledge management platform designed to create specialised digital assistants for companies, public institutions and complex organisations.

3. Duration and Frequency of the Processing

The Processing is carried out on a continuous basis for the duration of the Agreement and for any additional period required for deletion, return, backup retention, legal compliance, dispute resolution or security purposes.

4. Nature of the Processing

The Processing may include collection, recording, organisation, structuring, storage, hosting, retrieval, consultation, indexing, vectorisation, transmission, access, display, generation, analysis, logging, backup, deletion, anonymisation, support, debugging, security monitoring and other operations necessary to provide My-DO.

5. Purposes of the Processing

The purposes of the Processing include:

(a) providing, operating, maintaining and supporting My-DO;
(b) creating, configuring and managing customer-specific AI assistants;
(c) processing system instructions, prompts, queries and knowledge base content;
(d) indexing, retrieving and processing documents and knowledge base materials;
(e) generating and displaying Outputs;
(f) managing user access, authentication, permissions and account administration;
(g) providing customer support and technical assistance;
(h) monitoring security, preventing abuse, detecting unauthorised access and maintaining service integrity;
(i) debugging, troubleshooting, testing and improving the Customer's own My-DO environment;
(j) performing backup, disaster recovery and business continuity operations;
(k) complying with legal obligations and enforcing the Agreement.

6. Categories of Data Subjects

The categories of Data Subjects may include:
(a) Customer's authorised users, administrators, employees, contractors and representatives;
(b) Customer's clients, customers, citizens, partners, suppliers or end users, where their Personal Data is included in Customer Data;
(c) individuals identified or identifiable in documents, manuals, procedures, policies, files, datasets, knowledge base content, prompts, queries or Outputs uploaded, configured or generated by or on behalf of the Customer;
(d) support contacts, billing contacts and technical contacts, to the extent processed on behalf of the Customer.

7. Categories of Personal Data

The categories of Personal Data may include:

(a) identification data, such as name, surname, username, user ID or role;
(b) professional contact data, such as business email address, business phone number, company, department, job title or office location;
(c) account and authentication data, such as login identifiers, access rights, roles and permission settings;
(d) technical and usage data, such as logs, timestamps, IP addresses, device information, browser information, session information and activity records;
(e) prompt, query and interaction data submitted by authorised users;
(f) document content and knowledge base content uploaded or configured by the Customer;
(g) Personal Data contained in policies, manuals, procedures, reports, files, technical documentation, public service information, HR materials, compliance materials or other Customer Data;
(h) Outputs generated through My-DO that may contain or refer to Personal Data;
(i) billing and subscription data, where processed on behalf of the Customer.

8. Special Categories of Personal Data

My-DO is not intended for the processing of special categories of Personal Data, criminal conviction data or other highly sensitive data unless expressly agreed in writing in the applicable Order Form and subject to appropriate legal bases and safeguards.

However, special categories of Personal Data may be included in Customer Data if the Customer uploads or configures such data. In such case, the Customer remains responsible for ensuring that the Processing is lawful and that appropriate safeguards are in place.

9. Retention Period

Personal Data shall be retained for the duration of the Agreement, unless otherwise specified in the applicable Order Form, customer configuration, deletion policy or Applicable Data Protection Laws.

After termination or expiration, Personal Data shall be deleted, returned or anonymised in accordance with Section 10 of this DPA and Digita SRL’s applicable backup and retention policies.

10. Transfers to Subprocessors

Transfers to Subprocessors are described in Exhibit 3. The subject matter, nature and duration of such Processing shall be limited to the services provided by each Subprocessor and shall continue for the duration necessary to provide My-DO and comply with the Agreement.

EXHIBIT 2

Technical and Organisational Security Measures

Digita SRL shall implement and maintain appropriate technical and organisational measures designed to protect Personal Data processed through My-DO. Such measures may include, as applicable:

1. Access Control

(a) user authentication and account-based access;
(b) role-based access controls and permission management;
(c) restriction of access to Personal Data to authorised personnel with a need to know;
(d) administrative access controls;
(e) procedures for granting, modifying and revoking access.

2. Confidentiality

(a) confidentiality obligations for personnel and contractors;
(b) confidentiality provisions in agreements with Subprocessors and service providers;
(c) internal policies limiting access to Customer Data and Personal Data.

3. Encryption and Transmission Security

(a) encryption of Personal Data in transit where technically appropriate;
(b) secure communication protocols for access to My-DO and related services;
(c) protection of API communications with appropriate technical safeguards.

4. Storage and Backup Security

(a) secure storage of Personal Data using authorised infrastructure providers;
(b) backup procedures for relevant service components, including vector database backups;
(c) access controls for backup environments;
(d) retention and deletion procedures for backups.

5. System Security

(a) monitoring of systems for security, performance and availability;
(b) vulnerability management and security patching where applicable;
(c) logging and monitoring of relevant access and system events;
(d) protection against unauthorised access, misuse and abuse.

6. Availability and Resilience

(a) backup and recovery procedures;
(b) business continuity and disaster recovery measures appropriate to the nature of the Service;
(c) infrastructure resilience measures provided by hosting and cloud providers.

7. Data Minimisation and Segregation

(a) logical separation of customer environments, where applicable;

(b) processing of Personal Data only to the extent necessary to provide the Service;
(c) configuration options to manage knowledge base content and user access.

8. Incident Management

(a) procedures for identifying, assessing and responding to security incidents;
(b) escalation processes for suspected Personal Data Breaches;
(c) customer notification procedures in accordance with this DPA.

9. Subprocessor Management

(a) due diligence and contractual controls for Subprocessors;
(b) written agreements imposing appropriate data protection and security obligations;
(c) maintenance of Subprocessor information.

10. Organisational Measures

(a) assignment of internal responsibilities for privacy and security;
(b) personnel awareness regarding confidentiality and data protection;
(c) review and updating of security measures as appropriate.

EXHIBIT 3

List of Subprocessors
The Customer authorises Digita SRL to use the following Subprocessors for the provision, maintenance, security and support of My-DO.

1. GitLab

Purpose:
Website management, code repository management, development workflow, project management and technical operations related to My-DO.

Categories of Personal Data:
Technical, operational and account-related data that may be processed in connection with website or project management; limited Customer Data only where necessary for support, debugging or technical operations.

Transfer Mechanism:
GitLab may rely on the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework, Standard Contractual Clauses or other lawful transfer mechanisms, as applicable.

Location:
United States and/or other locations according to the applicable GitLab service configuration, subprocessors and data hosting arrangements.

2. Amazon Web Services (AWS)

Purpose:

Cloud infrastructure, storage, hosting, backup, S3 bucket storage, vector database storage and backup, security, availability and disaster recovery.

Categories of Personal Data:
Customer Data, knowledge base content, documents uploaded by the Customer, vector database data, technical logs, account and usage data, prompts, queries and Outputs, to the extent stored or backed up within AWS infrastructure.

Transfer Mechanism:
Standard Contractual Clauses, adequacy decisions or other lawful transfer mechanisms, as applicable.

Location:
European Union. Customer documents uploaded to My-DO and stored in the S3 bucket are hosted in AWS Europe (Stockholm) region. Other AWS regions, including AWS Europe (Milan), may be enabled in Digita SRL's AWS account but are not used for the storage of Customer-uploaded documents unless expressly configured or agreed.

Notes:
Digita SRL shall use AWS services with due regard to data protection, security and data residency requirements applicable to My-DO. Any material change to the AWS region used for the storage of Customer-uploaded documents shall be communicated to the Customer in accordance with this DPA, where required by Applicable Data Protection Laws or the Agreement.
3. OpenAI

Purpose:
API calls, AI model processing and generation of Outputs in connection with My-DO.

Categories of Personal Data:
Prompts, user queries, relevant retrieved context, selected knowledge base excerpts, system instructions, metadata and Outputs, to the extent transmitted through API calls necessary to provide My-DO.

Transfer Mechanism:
Standard Contractual Clauses, adequacy decisions, UK Addendum or other lawful transfer mechanisms, as applicable. For EEA and Swiss Personal Data, OpenAI states that OpenAI Ireland Limited processes such data and that transfers outside the EEA or Switzerland, where required to provide the services, are based on agreements containing SCCs or on an adequacy decision under Article 45 GDPR.

Location:
European Economic Area, United States and/or other locations according to OpenAI's applicable data processing, hosting, support and subprocessor arrangements.

4. Stripe
Status:
Future / planned Subprocessor. Stripe is not active as of the date of this DPA.

Purpose:
Payment processing, subscription billing, invoicing support, payment authentication, payment fraud prevention and related financial operations, if and when enabled for My-DO.

Categories of Personal Data:
Billing contact data, payment-related data, subscription information, transaction data, tax information and customer account information.

Transfer Mechanism:
To be specified when Stripe is enabled. Stripe may rely on Standard Contractual Clauses, adequacy decisions or other lawful transfer mechanisms, as applicable.

Location:
To be specified when Stripe is enabled, according to Stripe's applicable data processing, hosting, support and subprocessor arrangements.

Notes:
Stripe shall become an active Subprocessor only once payment processing or subscription billing through Stripe is enabled for My-DO. Digita SRL shall update this DPA or the Subprocessor list before or when Stripe becomes active, where required by Applicable Data Protection Laws or the Agreement.

Digita SRL may update this list from time to time in accordance with Section 7 of this DPA.