

PRIVACY POLICY

My-DO

Last updated: 05/05/2026

Welcome to My-DO.

This Privacy Policy explains how Digita SRL collects, uses, stores, shares and protects personal data when you visit the My-DO website, use the My-DO web application or mobile applications, create or access an account, contact us, request information, receive support, or otherwise interact with My-DO.

My-DO is primarily designed for business, professional, institutional and public-sector use. However, certain My-DO features, subscription plans or private solutions may also be made available to consumers for personal, household or non-professional use.

This Privacy Policy applies where Digita SRL acts as an independent data controller, including in relation to website visitors, account users, authorised users, consumer users, support contacts, billing contacts, app users and individuals who interact with My-DO.

This Privacy Policy does not apply to personal data that Digita SRL processes on behalf of a customer organisation within Customer Data, knowledge base content, prompts, uploaded documents, user queries, system instructions or outputs. In those cases, the customer organisation is generally the data controller and Digita SRL acts as processor under the applicable Data Processing Addendum.

My-DO does not currently use third-party analytics SDKs such as Firebase Analytics, Mixpanel, Amplitude or similar tools, based on the current technical configuration of the Service.

My-DO may, however, collect and process internal operational analytics, usage metrics, token consumption data, feedback trends, API call logs, activity logs and last activity timestamps for the purposes of service administration, monitoring, security, support, billing, performance analysis and improvement of the Service.

1. Who Collects Your Data?

The data controller is:

Digita SRL
Via Verdi 3
24121 Bergamo, Italy
VAT / Tax Code: 04334180165
Company identification number: IT04334180165
Share capital fully paid in: €10,000.00
PEC: pec.digita@legalmail.it
Email: info@digita.work

For privacy-related questions or to exercise your data protection rights, you may contact us at:

info@digita.work

or by writing to:

Digita SRL
Via Verdi 3
24121 Bergamo, Italy
Attention: Privacy

2. Scope of This Privacy Policy

This Privacy Policy applies to personal data processed by Digita SRL as controller in connection with:

- (a) the My-DO website;
- (b) the My-DO web application;
- (c) the My-DO mobile applications for iOS and Android;
- (d) account administration;
- (e) demo requests, contact forms and commercial enquiries;
- (f) customer support and technical assistance;
- (g) billing, contracts and administrative activities;
- (h) security, abuse prevention and service integrity;
- (i) communications, including service communications and marketing where applicable;
- (j) legal compliance and dispute management.

Where you use My-DO as an authorised user of a customer organisation, that organisation may separately process your personal data as an independent controller. You should refer to that organisation's privacy notice for information about how it processes your personal data.

3. What Personal Data We Collect

3.1 Data You Provide Directly to Us

We may collect the following categories of personal data directly from you:

- (a) Identity data, such as first name, last name, role, job title, organisation or department;
- (b) Contact data, such as business email address, phone number, postal address or PEC address;
- (c) Account data, such as username, account ID, login credentials, authentication information, role and permissions;
- (d) Contract and customer data, such as organisation name, subscription plan, order information, contract details, customer type and authorised user status;
- (e) Billing and administrative data, such as billing address, VAT number, tax information, invoice data, payment status and transaction references;

(f) Support data, such as messages, requests, tickets, bug reports, screenshots, technical descriptions and communications with our support team;

(g) Marketing and communication data, such as newsletter preferences, contact preferences and responses to communications;

(h) Feedback data, such as comments, suggestions, ratings, corrections, feature requests or other feedback about My-DO.

3.2 Data Generated When You Use My-DO

When you use the website, web application or mobile applications, we may collect certain technical, operational and usage data, including:

(a) Technical data, such as IP address, device type, operating system, browser type, app version, language settings, session identifiers, access times, network information and error or crash information;

(b) Usage data, such as features used, actions performed, assistant interactions, session activity, token consumption, API call activity, feedback trends and other operational metrics generated through the use of My-DO;

(c) Security and activity data, such as authentication events, access logs, failed login attempts, valid API calls, activity logs, last activity timestamps, suspicious activity signals and audit logs;

(d) Account and organisation activity data, such as information relating to when a user is added to an organisation, assigned to an assistant, removed from an organisation or otherwise granted or modified access.

As of the date of this Privacy Policy, My-DO does not currently use third-party analytics SDKs such as Firebase Analytics, Mixpanel, Amplitude or similar tools. Usage analytics are generated and managed internally for operational, administrative, security, support and service improvement purposes.

3.3 Data Processed Through My-DO as Part of the Service

Depending on how a customer organisation configures and uses My-DO, the Service may process prompts, queries, documents, knowledge base content, system instructions, outputs and interaction logs.

Where such data is processed by Digita SRL on behalf of a customer organisation, it is governed by the applicable customer agreement and Data Processing Addendum, not by this Privacy Policy, except where Digita SRL also processes certain related data as controller for security, account administration, support, legal compliance or service integrity.

4. Why We Use Your Personal Data and Legal Bases

We process personal data for the purposes and legal bases described below.

4.1 To Provide and Maintain My-DO

We use identity data, account data, technical data, usage data, support data and security data to provide, operate, maintain and make available My-DO.

Legal basis:

Performance of a contract or steps prior to entering into a contract; legitimate interest in providing and maintaining a secure and functional service.

4.2 To Create and Manage Accounts

We use identity data, contact data, account data and organisation data to create accounts, authenticate users, manage access permissions and administer user roles.

Legal basis:

Performance of a contract; legitimate interest in account administration and access control.

4.3 To Provide Customer Support

We use identity data, contact data, account data, support data, technical data and, where necessary, limited service data to respond to support requests, investigate issues, debug problems and improve service reliability.

Legal basis:

Performance of a contract; legitimate interest in providing support and improving the Service.

4.4 To Manage Security, Abuse Prevention and Service Integrity

We use account data, technical data, usage data, security data and logs to protect My-DO, prevent fraud, detect unauthorised access, investigate abuse, enforce terms and maintain service integrity.

Legal basis:

Legitimate interest in protecting My-DO, customers, users, systems and data; legal obligation where applicable.

4.5 To Manage Contracts, Billing and Administration

We use identity data, contact data, contract data, billing data, payment status and administrative information to manage contracts, subscriptions, invoices, accounting, tax obligations and payment-related activities.

Legal basis:

Performance of a contract; compliance with legal obligations; legitimate interest in business administration.

4.6 To Communicate With You

We use contact data, account data and organisation-related information to send operational, administrative and service-related communications.

These communications may include, by way of example:

- (a) account creation or invitation emails;
- (b) notifications that you have been added to an organisation;
- (c) notifications that you have been added to or removed from an assistant;
- (d) access, role or permission-related communications;
- (e) service, security or support communications;
- (f) important notices relating to changes to My-DO, these Terms, the Privacy Policy or other legal documents.

Legal basis:

Performance of a contract; legitimate interest in administering the Service and communicating operational information; legal obligation where applicable.

My-DO does not currently send marketing or promotional emails to users.

4.7 Marketing Communications

My-DO does not currently send marketing or promotional communications to users.

If Digita SRL decides to send marketing communications in the future, such communications will be sent only where permitted by applicable law and, where required, with the user's prior consent. Users will be able to unsubscribe or object to marketing communications at any time.

4.8 To Monitor, Analyse and Improve My-DO

We may use technical data, operational data, usage data, token consumption data, feedback trends, API call logs, activity logs, performance data and aggregated or anonymised statistics to:

- (a) monitor the use, performance and availability of My-DO;
- (b) analyse token consumption and usage trends;
- (c) provide internal analytics dashboards to authorised administrators;
- (d) identify bugs, errors, misuse, abuse or abnormal activity;
- (e) improve the reliability, security, performance and functionality of My-DO;
- (f) develop, test and improve features and user experience.

Legal basis:

Legitimate interest in monitoring, securing, maintaining and improving My-DO; performance of a contract where such processing is necessary to provide the Service.

For clarity, Digita SRL does not use Customer Data, uploaded documents, knowledge base content, prompts, queries or outputs to train general-purpose AI models by default, unless expressly agreed in writing or clearly disclosed in a specific feature or agreement.

4.9 To Comply With Legal Obligations

We may process personal data to comply with tax, accounting, regulatory, legal, data protection, court or authority obligations.

Legal basis:

Compliance with legal obligations.

4.10 To Establish, Exercise or Defend Legal Claims

We may process personal data where necessary to prevent, investigate or manage disputes, enforce agreements, recover unpaid amounts, protect rights or defend legal claims.

Legal basis:

Legitimate interest in protecting our legal rights; legal obligation where applicable.

5. Cookies and Similar Technologies

When you visit the My-DO website or use the Service, we may use cookies or similar technologies that are necessary for the functioning, security, authentication, session management and accessibility of the website or Service.

As of the date of this Privacy Policy, My-DO does not currently use third-party analytics SDKs such as Firebase Analytics, Mixpanel, Amplitude or similar tools.

If Digita SRL introduces non-essential cookies, third-party analytics tools, marketing cookies or similar tracking technologies in the future, such tools will be used only where permitted by applicable law and, where required, with your prior consent.

For more information, please see our Cookie Policy, where applicable.

6. How Long We Keep Your Personal Data

We keep personal data only for as long as necessary for the purposes described in this Privacy Policy, unless a longer retention period is required or permitted by law.

Technical, security, usage and activity logs, including API call logs, token consumption data, last activity timestamps and internal operational analytics: for up to 12 months, unless a longer retention period is necessary for security, abuse prevention, billing verification, legal compliance, dispute management or service integrity.

Indicative retention periods are:

- (a) Account data: for the duration of the account and for up to 1 year after account deletion, unless longer retention is required for security, legal or dispute purposes;
- (b) Contract and customer relationship data: for the duration of the contractual relationship and for up to 10 years where required for accounting, tax or legal purposes;
- (c) Invoices and accounting records: for 10 years from the relevant financial year, where required by applicable law;
- (d) Support requests: for the time necessary to handle the request and for up to 5 years for record-keeping, service improvement and dispute management;

- (e) Technical, security, usage and activity logs, including API call logs, token consumption data, last activity timestamps and internal operational analytics: for up to 12 months, unless a longer retention period is necessary for security, abuse prevention, billing verification, legal compliance, dispute management or service integrity;
- (f) Demo and sales lead data: for up to 3 years from the last meaningful interaction, unless a contractual relationship is established or you object earlier;
- (g) Privacy rights requests: for the time necessary to respond and for up to 5 years to demonstrate compliance;
- (h) Dispute-related data: for the duration of the dispute and until the expiry of applicable limitation periods.

Where Digita SRL processes personal data on behalf of a customer organisation, retention is governed by the applicable customer agreement, Data Processing Addendum, customer configuration, deletion policy and backup retention rules.

7. Who We Share Personal Data With

We may share personal data on a need-to-know basis with the following categories of recipients:

- (a) authorised Digita SRL personnel and contractors;
- (b) hosting, infrastructure, storage and backup providers;
- (c) AI model and API providers;
- (d) code repository, development workflow, website management and technical operations providers;
- (e) payment and billing providers, if and when enabled;
- (f) professional advisers, such as lawyers, accountants, auditors and consultants;
- (g) banks and financial institutions, where necessary;
- (h) public authorities, courts, regulators or law enforcement bodies where required by law;
- (i) business partners or successors in the context of mergers, acquisitions, reorganisations or business transfers, where applicable.

Our current main service providers and subprocessors include:

- (a) GitLab, for website management, code repository management, development workflow, project management and technical operations related to My-DO;
- (b) Amazon Web Services, for cloud infrastructure, storage, hosting, backup, S3 bucket storage, vector database storage, security, availability and disaster recovery;
- (c) OpenAI, for API calls, AI model processing and generation of outputs in connection with My-DO;
- (d) Stripe, in the future, for payment processing, subscription billing, invoicing support, payment authentication, fraud prevention and related financial operations, once enabled.

As of the date of this Privacy Policy, My-DO does not currently use third-party analytics SDKs such as Firebase Analytics, Mixpanel, Amplitude or similar tools.

8. International Transfers

We aim to use providers and configurations that are appropriate for the protection of personal data, including providers located in or offering services within the European Union where possible.

Some providers may process or access personal data outside the European Economic Area, Switzerland or the United Kingdom.

Where personal data is transferred internationally, we rely on appropriate safeguards under applicable data protection laws, such as 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 other lawful transfer mechanisms.

For AWS, customer-uploaded documents 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.

For OpenAI, API calls may involve processing according to OpenAI's applicable data processing terms and transfer safeguards.

For GitLab, transfers may rely on the Data Privacy Framework, Standard Contractual Clauses or other applicable safeguards according to GitLab's data processing terms.

Stripe is not active as of the date of this Privacy Policy and will become relevant only if payment processing or subscription billing through Stripe is enabled.

9. Security

We implement appropriate technical and organisational measures designed to protect personal data against unauthorised access, accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

These measures may include access controls, authentication, encryption in transit where appropriate, role-based permissions, confidentiality obligations, backup procedures, logging, monitoring, incident response processes and subprocessor management.

No online service can be guaranteed to be completely secure. You are responsible for keeping your credentials confidential, using secure devices and promptly notifying us of any suspected unauthorised access.

10. Your Data Protection Rights

Depending on applicable law and the circumstances, you may have the following rights:

- (a) right of access: to obtain confirmation whether we process your personal data and receive a copy of it;
- (b) right to rectification: to request correction of inaccurate or incomplete data;
- (c) right to erasure: to request deletion of your personal data;

(d) right to restriction: to request restriction of processing;

(e) right to portability: to receive personal data you provided to us in a structured, commonly used and machine-readable format, where applicable;

(f) right to object: to object to processing based on legitimate interests or direct marketing;

(g) right to withdraw consent: where processing is based on consent;

(h) right not to be subject to solely automated decisions producing legal or similarly significant effects, where applicable;

(i) right to lodge a complaint with a supervisory authority.

To exercise your rights, contact us at:
info@digita.work

We may need to verify your identity before responding. If your request relates to personal data processed by us on behalf of a customer organisation, we may direct you to that organisation or cooperate with it in accordance with the applicable Data Processing Addendum.

You also have the right to lodge a complaint with the competent supervisory authority. In Italy, this is the Garante per la protezione dei dati personali.

11. Automated Decision-Making

Digita SRL does not use personal data covered by this Privacy Policy to make decisions based solely on automated processing that produce legal effects or similarly significant effects on individuals.

My-DO may generate AI-assisted outputs, but such outputs should be reviewed and evaluated by users and, where applicable, by the relevant customer organisation before being relied upon.

12. Children

My-DO is not intended for children.

My-DO is primarily intended for business, professional, institutional and public-sector use. We do not knowingly collect personal data from children for consumer use of My-DO.

If you believe that a child has provided personal data to us without appropriate authorisation, please contact us at info@digita.work.

13. Third-Party Websites and Services

The My-DO website, web application or mobile applications may contain links to third-party websites, app stores, services or resources.

We are not responsible for the privacy practices, content or security of third-party websites or services that we do not control. You should review the privacy notices of those third parties before using them.

14. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in My-DO, our processing activities, providers, legal requirements or business operations.

If we make material changes, we will provide notice where required by applicable law, for example by email, account notification, app notification or notice on our website.

The updated Privacy Policy will apply from the date indicated at the top of the document.

15. Contact Us

For questions, requests or complaints regarding this Privacy Policy or the processing of your personal data, contact:

Digita SRL
Via Verdi 3
24121 Bergamo, Italy
Email: info@digita.work
PEC: pec.digita@legalmail.it
Attention: Privacy