Data Processing Agreement

> *This English version is a translation provided for convenience. The Dutch version is the leading text; in the event of any discrepancy, the Dutch version prevails.*

This data processing agreement (the "**Data Processing Agreement**" or "**DPA**") applies to every processing of personal data that DOENio VOF (the "**Processor**") performs on behalf of the customer (the "**Controller**") in the context of using the DOENio platform and the subscriptions concluded under it (the "**Main Agreement**").

DOENio VOF Chamber of Commerce (KvK): 42052522 VAT: NL869488818B01 Email: legal@doenio.nl

By accepting DOENio's General Terms, the Controller also accepts this Data Processing Agreement.

1. Definitions

Terms defined in the GDPR have the same meaning in this agreement. In addition:

- **GDPR**: Regulation (EU) 2016/679 (General Data Protection Regulation).
- **Platform**: the software-as-a-service solution "DOENio" offered by the Processor, including the associated web application, AI agents, AI squads, workflows, connectors, management functions and APIs.
- **Main Agreement**: the agreement between the parties (including the General Terms and the chosen subscription) under which the Processor makes the Platform available to the Controller.
- **Controller**: the customer that determines the purposes and means of the processing of Personal Data (Article 4(7) GDPR).
- **Processor**: DOENio VOF, which processes Personal Data on behalf of the Controller (Article 4(8) GDPR).
- **Personal Data**: any data relating to an identified or identifiable natural person ("**Data Subject**") that the Processor processes on behalf of the Controller.
- **Customer Data**: all data, including Personal Data, that is entered, uploaded, generated or otherwise processed in the Platform by or on behalf of the Controller, including messages, documents, knowledge base content, agent configurations, workflow settings and outputs.
- **Data Subject**: the natural person to whom a Personal Data item relates.
- **Sub-processor**: a third party engaged by the Processor that actually processes Personal Data on behalf of the Processor in the context of the Main Agreement. This includes two distinct categories:

- **(a) Core sub-processors**: sub-processors engaged for every Controller because they are necessary for the basic operation of the Platform (such as hosting, authentication and payment processing). See Annex 2, Table A.
- **(b) AI/LLM providers**: providers of the language model that processes the content the Controller or its agents send to the model. See Annex 2, Table B.

External services activated by the Controller (Connectors) are not Sub-processors of the Processor; see the definition of "Customer-activated external service" and article 6.2.

- **Infrastructure supplier**: a supplier of general infrastructure or supporting technology that, by the nature of the service, does not access or take cognisance of Personal Data in intelligible form. An Infrastructure supplier that does actually process Personal Data qualifies as a Sub-processor and falls under Annex 2.
- **Connector**: a link to an external service (such as email, calendar, chat or ticketing) that the Controller can activate in the Platform, enabling the Platform to exchange data with that service on behalf of the Controller.
- **Customer-activated external service**: an external service that processes Personal Data only after the Controller has activated a Connector, integration or AI functionality for that purpose.
- **AI service / LLM provider**: the provider of the large language model and associated processing services used by or on behalf of the Controller to run AI agents and automated functionalities.
- **Security Incident**: any breach of, or threat to, the security of processing systems or data, regardless of whether Personal Data is involved.
- **Personal Data Breach**: a Security Incident that, accidentally or unlawfully, leads to the destruction, loss, alteration, or unauthorised disclosure of, or access to, Personal Data (Article 4(12) GDPR). A Personal Data Breach is a particular category of Security Incident.
- **Written instruction**: any instruction from the Controller to the Processor regarding the processing of Personal Data. This includes: (i) the provisions of the Main Agreement and this Data Processing Agreement; (ii) the configuration and settings that an authorised administrator (tenant admin) of the Controller makes within the Platform, including activating Connectors, integrations and AI functionalities; and (iii) instructions given through a verified support channel or support ticket by an authorised representative. Oral instructions are confirmed by the Processor in writing or electronically as soon as possible.

2. Subject matter, nature, duration and scope of the processing

2.1. The Processor provides the Controller with a SaaS platform enabling the Controller to set up and run AI agents and workflows and, to the extent activated by the Controller, to connect to external services. The Processor processes Personal Data solely in the context of performing the Main Agreement.

2.2. A distinction is made between:

- **standard processing operations** that take place for every Controller, namely hosting the Platform, user and account management, authentication, logging and monitoring, support, and backup and recovery; and
- **processing operations that take place only after the Controller activates a function for that purpose**, such as running specific AI agents, setting up workflows and connecting Connectors to external services.

2.3. The Processor processes Personal Data only for the following purposes:

- (a) providing and operating the Platform and the services obtained within it;
- (b) securing the Platform and the data stored within it;
- (c) providing support at the request of or on behalf of the Controller;
- (d) carrying out maintenance, management and (further) development of the Platform;
- (e) making backups and performing recovery operations;
- (f) complying with legal obligations incumbent on the Processor.

The Processor does not use Personal Data for its own, differing purposes.

2.4. This Data Processing Agreement applies for the duration of the Main Agreement. The processing runs concurrently with the duration of the Main Agreement, plus a limited wind-down period needed for deletion or return (article 11), rotating backups according to the retention schedule, and complying with statutory retention obligations. Provisions that by their nature continue to apply after the end (such as confidentiality and liability) remain in force.

2.5. The subject matter, nature, purpose, categories of data subjects, types of Personal Data, sources, recipients and retention periods are further described per processing activity in **Annex 1**.

3. Processing on instruction

3.1. The Processor processes Personal Data solely on the basis of Written instructions from the Controller, save for diverging legal obligations incumbent on the Processor. In the latter case, the Processor informs the Controller of that legal requirement prior to the processing, unless that law prohibits such notification.

3.2. Only instructions originating from an authorised representative or an administrator (tenant admin) designated by the Controller qualify as instructions of the Controller. The Controller is responsible for managing and ensuring the accuracy of the rights granted to administrators.

3.3. The activation of Connectors, integrations or AI functionalities by an administrator of the Controller, and the configuration choices made in doing so, qualify as a Written instruction of the Controller to carry out the associated processing operations.

3.4. If the Processor, in its reasonable judgement, considers that an instruction infringes the GDPR or other privacy law, or entails an unacceptable security risk, it informs the Controller in writing without delay. In that case the Processor is entitled to suspend execution of the relevant instruction until the Controller confirms or amends it.

3.5. The Processor does not use Personal Data for its own purposes and does not share it with third parties, other than as expressly permitted by this agreement or required by law.

3.6. The Processor is not responsible or liable for:

- (a) the lawfulness and accuracy of the Customer Data entered by or on behalf of the Controller, nor for the existence of an adequate legal basis for it;
- (b) erroneous configurations, settings or activation choices made by the Controller or its administrators;
- (c) the use of Platform functionalities in breach of the Controller's privacy policy, internal guidelines or legal obligations.

3.7. To the extent the Controller gives additional instructions that fall outside the standard service and that reasonably require additional effort from the Processor, the Processor may charge the reasonable costs involved, after giving prior indication of these to the Controller.

4. Confidentiality

4.1. The Processor ensures that persons who have access to Personal Data (employees, hired staff, temporary staff, contractors and support personnel, as well as persons working for Sub-processors) have committed themselves to confidentiality, either contractually or under a statutory obligation.

4.2. This confidentiality obligation continues to apply after the end of the work or the employment or contractual relationship.

4.3. Access is granted on a "least privilege" basis: only to persons for whom access is strictly necessary to perform their task.

4.4. The Processor ensures that persons who have access to Personal Data periodically receive privacy and information security awareness and training measures.

5. Security

5.1. The Processor implements appropriate technical and organisational measures to secure Personal Data, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks to the rights and freedoms of Data Subjects. The measures are described in more detail and in a verifiable manner in **Annex 3** and include at least:

- (a) role-based access control on a "least privilege" basis;
- (b) multi-factor authentication (MFA) for administrator access to production systems;
- (c) encryption of Personal Data in transit;
- (d) encryption of sensitive data at rest where appropriate;
- (e) logging of administrator and security-relevant actions;
- (f) patch and update management and vulnerability management;

- (g) regular backups and periodic recovery tests;
- (h) a process for incident response and handling Personal Data Breaches;
- (i) logical separation and isolation of the data of different Controllers (tenant isolation);
- (j) secure software development (secure SDLC) with separation between development, test and production environments.

5.2. The Processor periodically evaluates these measures and adjusts them based on the state of the art, identified threats and changes in the nature of the processing.

5.3. **Administrator access.** Access by the Processor's personnel to production systems and Customer Data takes place only to the extent necessary for delivery, support, security or maintenance, is logged, is limited to authorised persons, and runs via internal authorisation procedures.

5.4. **Security of AI functionalities.** To the extent the Controller uses AI functionalities:

- (a) prompts, context data and outputs within the Platform are protected with the same access and encryption measures as other Customer Data;
- (b) Customer Data is not used to train general or third-party models, unless expressly agreed otherwise in writing (see article 14);
- (c) logs of AI processing are secured and accessible on a least-privilege basis.

5.5. The Controller acknowledges that the measures described in Annex 3 are appropriate for the processing described in Annex 1, and is responsible for correctly configuring the security settings available on the Controller's side (such as enforcing MFA for end users).

6. Sub-processors

6.1. The Controller grants the Processor general prior authorisation to engage the Sub-processors listed in **Annex 2**. A distinction is made between Core sub-processors (Table A) and AI/LLM providers (Table B).

6.2. **Connectors and customer-activated integrations.** By activating a Connector or integration in the Platform, the Controller links an external service used by the Controller itself to the Platform. The Controller determines which data is exchanged via that Connector and where it is stored with the external service, and remains responsible for its own relationship with, and legal basis for, that external service. The Processor does not engage this external service as its own Sub-processor and has no control over the storage of data with that service. The Processor acts solely as a processor for the processing of data within the Platform itself (as described in Annex 1). An overview of the Connectors available in the Platform is included for transparency in Annex 2, Table C.

6.3. **AI/LLM provider.** The AI/LLM provider configured by the Controller, or offered by the Processor and chosen by the Controller, processes the content the Controller or its agents send to the language model. The Controller is informed about the AI sub-processor(s) involved via Annex 2, Table B.

6.4. **Change of Sub-processors.** Where the Processor wishes to add or replace a Sub-processor, it notifies the Controller at least thirty (30) days in advance, via the contact details referred to in article 13 and/or the publication location referred to in Annex 2. The Controller may object on reasonable grounds in writing within that period.

6.5. **Consequences of objection.** In the event of a timely and reasoned objection, the parties will consult to find a reasonable solution. Possible outcomes are, in order of preference: (a) offering an alternative Sub-processor or setup; (b) disabling the relevant function or Connector for the Controller; or, as a last resort, (c) full or partial termination of the relevant part of the Main Agreement by either party, without this constituting a breach.

6.6. The Processor imposes on each Sub-processor, by way of a written agreement, data protection obligations equivalent to those incumbent on the Processor under this agreement, in particular as regards security and transfers.

6.7. The Processor remains fully liable to the Controller for the performance of the Sub-processor's obligations (Article 28(4) GDPR).

6.8. A current list of Sub-processors is maintained by the Processor and is available at https://www.doenio.nl/en/legal/data-processing-agreement and on request via legal@doenio.nl.

7. Assistance with data subject rights

7.1. The Processor does not handle requests from Data Subjects on the merits independently, unless the Controller so requests or it is required by law. Requests that reach the Processor directly are forwarded without delay to, or referred to, the Controller.

7.2. Taking into account the nature of the processing and the means available to it, the Processor provides reasonable assistance to the Controller in responding to requests from Data Subjects exercising their rights under the GDPR. This assistance may include:

- locating Personal Data (access);
- exporting Personal Data (data portability);
- correcting Personal Data (rectification);
- erasing Personal Data;
- restricting processing;
- providing relevant log data, to the extent applicable.

7.3. To the extent a request for assistance is excessive or exceeds the standard support that may reasonably be expected of the Processor, the Processor may charge the reasonable costs involved separately, after giving prior indication of these.

8. Personal Data Breaches and other assistance

8.1. The Processor informs the Controller without delay and without undue delay after becoming aware of a Personal Data Breach affecting the Personal Data it processes for the Controller. The initial notification is made as soon as the Processor has sufficient basic information, and in any event in time for the Controller to comply with its own 72-hour notification obligation under Article 33 GDPR.

8.2. The initial notification contains at least, to the extent known at that time:

- (a) the nature of the incident;
- (b) the likely consequences and impact;
- (c) the systems and categories of Personal Data and Data Subjects involved;
- (d) the measures already taken or proposed to address the incident and limit its consequences;
- (e) a point of contact for further information.

8.3. The Processor provides follow-up updates as more information becomes available, and cooperates with the Controller in the investigation, containment, remediation and documentation of the incident.

8.4. The Processor does not independently notify a Personal Data Breach to Data Subjects or to a supervisory authority, unless required to do so by law. The assessment of whether and how a notification is made to the supervisory authority or Data Subjects rests with the Controller.

8.5. **Incidents involving AI and integrations.** Personal Data Breaches and Security Incidents include, where applicable, incidents such as an incorrect transfer of data via a Connector, the leakage of prompt or context data (prompt leakage), and the display of output to an incorrect Controller or tenant.

8.6. The Processor provides reasonable assistance to the Controller in complying with its obligations under Articles 32 to 36 GDPR, including in the context of Security Incidents, data protection impact assessments (DPIAs) and prior consultations.

9. Audit and provision of information

9.1. On the Controller's request, the Processor makes available all information necessary to demonstrate compliance with Article 28 GDPR. The provision of documentation and, to the extent available, certifications or assurance reports is the primary way in which the audit right is exercised.

9.2. If documentation and certifications are reasonably insufficient to demonstrate compliance, or in the event of a serious and concrete suspicion of a breach, the Controller may carry out (or have carried out) an on-site audit at most once per calendar year. Such an audit:

- (a) is announced at least four (4) weeks in advance;
- (b) takes place during office hours;
- (c) is conducted in a manner that minimises disruption to the Processor's operations;
- (d) takes place under a non-disclosure agreement (NDA).

9.3. An audit may not lead to access to:

- (a) data of other Controllers or customers;
- (b) confidential security details to the extent not necessary for the assessment;
- (c) source code, unless justified and necessary in a particular case.

9.4. Where the Processor holds current independent certifications or audit reports, the Controller may accept these as adequate fulfilment of its audit right, to the extent they cover the relevant subject matter.

9.5. **Costs.** A regular audit is at the Controller's expense, including the Processor's reasonable costs for support. If an audit reveals a demonstrable and material breach by the Processor, the reasonable costs of that audit may be borne by the Processor.

10. Transfers outside the EEA

10.1. The Processor will not transfer Personal Data to a country outside the European Economic Area (EEA) or to an international organisation without implementing an appropriate transfer mechanism under the GDPR, such as an adequacy decision or the European Commission's Standard Contractual Clauses (SCCs), supplemented where necessary by appropriate additional measures.

10.2. Transfers outside the EEA generally take place via certain Sub-processors (in particular providers of hosting services, authentication and bot protection established or processing in the United States). For each Sub-processor, the processing region and the applicable transfer scenario and mechanism are stated in **Annex 2**.

10.3. **AI processing within the EU.** The AI/LLM providers engaged by the Processor (Annex 2, Table B) process prompts, context data, outputs, metadata and logs solely within the European Union. No transfer of this data outside the EEA takes place via these AI providers.

10.4. The Processor informs the Controller of relevant changes in international data flows resulting from a change of Sub-processors, in accordance with the procedure in article 6.4.

11. Return, deletion and exit

11.1. After the end of the Main Agreement, or earlier on the Controller's request, the Processor deletes the Customer Data (including Personal Data) or returns it to the Controller, at the Controller's choice.

11.2. **Return.** Return takes place in CSV format, within thirty (30) days of the request, via an export provided by the Processor.

11.3. **Deletion from active systems.** The Processor deletes the Customer Data from the active production systems no later than within thirty (30) days of the end of the Main Agreement (or after an earlier deletion request).

11.4. The following applies to the other forms in which Customer Data appears:

- (a) **backups**: are rotated according to the fixed retention schedule and overwritten or deleted no later than within seven (7) days of deletion from the active systems;
- (b) **logs**: are retained in accordance with the retention periods in Annex 1 and deleted thereafter;
- (c) **support data**: is anonymised in accordance with Annex 1 no later than one (1) year after the relevant support request and contains no Personal Data thereafter;
- (d) **test environments**: contain no production Customer Data; to the extent Customer Data is nevertheless present, it is included in the deletion;
- (e) **cache files**: are deleted or overwritten according to the regular cycle.

11.5. Deletion may be postponed to the extent and for as long as a statutory retention obligation requires; in that case the Customer Data is retained solely for that purpose and the obligations under this agreement continue to apply to it.

11.6. **Exit assistance.** On request, the Processor provides the Controller with reasonable support in migrating Customer Data to the Controller or a party designated by it. The Processor may charge the reasonable costs for this, after giving prior indication of these.

11.7. **Scope for SaaS/AI.** The exit and deletion obligations also include, where applicable, the Controller's workflow configurations, agent settings, knowledge bases and output history.

11.8. The Processor confirms the deletion in writing to the Controller on request.

12. Liability

12.1. The liability regime of the Main Agreement applies to liability arising under this Data Processing Agreement. This provision must always be read in conjunction with the Main Agreement. This is without prejudice to liability that may arise directly between the parties or towards Data Subjects under Article 82 GDPR.

12.2. **Indemnification by the Controller.** The Controller indemnifies the Processor against claims of third parties (including Data Subjects and supervisory authorities) arising from:

- (a) unlawful or incorrect instructions of the Controller;
- (b) the absence of an adequate legal basis for the processing on the Controller's side;
- (c) unlawful or prohibited content that the Controller enters into the Platform or has processed.

13. Final provisions

13.1. In the event of a conflict between the Main Agreement and this Data Processing Agreement, this Data Processing Agreement prevails for matters concerning the processing of Personal Data and the protection of Data Subjects.

13.2. Amendments to this Data Processing Agreement may be agreed between the parties in writing or electronically. Amendments resulting solely from changed legislation or guidance from supervisory authorities may be implemented by the Processor with prior notice to the Controller.

13.3. **Partial invalidity.** If a provision of this Data Processing Agreement is void or voidable, the remaining provisions remain in full force. The parties will consult to replace the void or voided provision with a valid provision that approximates its intent as closely as possible.

13.4. **Contact points.** The following contact points apply for matters under this agreement:

- Privacy and general matters: legal@doenio.nl
- Security and Security Incidents: security@doenio.nl
- Reporting Personal Data Breaches: security@doenio.nl

13.5. This Data Processing Agreement is governed by Dutch law. Disputes are submitted to the competent court in Arnhem, the Netherlands.

14. AI and automated functionalities

14.1. The Controller is responsible for the choice to activate and use AI functionalities in the Platform, and for the manner in which these are deployed.

14.2. The Processor does not use Customer Data to train general or third-party models, unless this is expressly agreed with the Controller in writing.

14.3. The Controller is informed about the Sub-processors involved in the AI functionalities (AI/LLM providers) via Annex 2, Table B.

14.4. Prompts, context data, outputs and logs processed in the context of AI functionalities fall within the scope of this Data Processing Agreement.

14.5. The Controller does not enter prohibited data or special categories of personal data as input for AI functionalities without having its own legal basis for doing so and making prior written additional arrangements with the Processor about it (see also Annex 1).

14.6. Outputs of AI functionalities may contain inaccuracies. The Controller is responsible for validating outputs before they are used for decision-making, communication or other purposes with consequences for Data Subjects.

Annex 1: Description of the processing

General subject matter and nature: hosting and processing Personal Data for the purpose of operating the DOENio platform, including user management, running AI agents and related workflows, integrations with external services designated by the Controller, and storing results and logs.

Purpose (overarching): performing the Main Agreement and providing the services described in it, within the purposes referred to in article 2.3.

Duration: for the term of the Main Agreement, followed by the deletion and retention periods referred to in article 11.

Processing activities

#	Processing activity	Purpose	Categories of Personal Data	Categories of Data Subjects	Source of the data	Recipients / Sub-processors	Retention period
1	Hosting and storage	Making the Platform available and operating it	All Personal Data processed in the Platform	All categories below	Controller and connected services	Hosting providers (Annex 2, Table A)	Term of agreement + deletion art. 11
2	Account and user management	Managing users, roles and rights	Name, email, language preference, organisation, role	Users/administrators of the Controller	Controller	Hosting providers	Term of agreement + deletion art. 11
3	Authentication	Secure sign-in and session management	Account identifiers, email, authentication/session tokens (encrypted/hashed)	Users/administrators	Controller; identity provider	Authentication providers (Google/Microsoft, Table A)	Session duration; tokens max. 30 days
4	Support	Handling support requests	Contact details and the data shared in a request	Users/administrators	Controller	Processor (support team)	Anonymised after 1 year
5	Logging and monitoring	Security, debugging, auditing	Activity and audit logs, IP address, technical metadata	Users/administrators	Platform usage	Hosting providers	12 months
6	Email processing (Connector)	Processing email via an activated connector	Sender/recipient data, subject, content, headers	Senders/recipients of email	Email service connected by the customer	Email service connected by the customer (customer-activated integration, see Table C; not a sub-processor)	365 days

#	Processing activity	Purpose	Categories of Personal Data	Categories of Data Subjects	Source of the data	Recipients / Sub-processors	Retention period
7	Calendar synchronisation (Connector)	Synchronising calendar items	Title, participants, time, location, description	Participants in appointments	Calendar service connected by the customer	Calendar service connected by the customer (customer-activated integration, see Table C; not a sub-processor)	365 days
8	AI analysis / agent execution	Running AI agents on input supplied by the customer	Prompts, context data and outputs (may contain Personal Data)	Determined by the Controller	Controller and/or activated services	AI/LLM provider (Table B)	Run logs and results 365 days; generated artefacts 2 months
9	Workflow automation	Running configured workflows	Depends on the workflow	Determined by the Controller	Controller and/or activated services	Depends on the connected services	Run logs and results 365 days; generated artefacts 2 months
10	Export	Providing a data export to the Controller	All exported Personal Data	All categories	Platform	Controller	Not retained after delivery (except logging)
11	Backup and recovery	Continuity and recoverability	All Personal Data processed in the Platform	All categories	Platform	Hosting providers	7-day rotation
12	Payment processing and invoicing	Collecting subscription fees and invoicing	Name, contact/billing details, payment data	Billing contact of the Controller	Controller	Mollie (Table A)	Billing data 7 years (statutory tax retention)

Types of personal data (summary)

- contact and account data (name, email, language preference, organisation, role);
- content of messages and documents supplied or processed by or on behalf of the Controller;
- metadata about use of the Platform (for example activity and audit logs, IP addresses);
- credentials and session tokens (encrypted or hashed where applicable);
- prompts, context data and outputs of AI functionalities.

Special categories of personal data

The Controller does **not** enter special categories of personal data (such as data concerning health, race or ethnic origin, religion or belief, or criminal record data) into the Platform, unless it has its own legal basis for doing so **and** has made prior written additional arrangements with the Processor about it. The Platform is not configured by default for the processing of special categories of personal data.

Annex 2: Sub-processors

Table A: Core sub-processors (always active, essential for basic operation)

Sub-processor	Service / function	Processing location	Categories of personal data	International transfer	Transfer mechanism
Google Cloud EMEA Limited	Platform hosting	EU	All Personal Data processed in the Platform	No	n/a
Microsoft Ireland Operations Ltd.	Platform hosting and authentication (Entra ID sign-in)	EU	Hosting: all Personal Data; sign-in: account identifiers, email, tokens	Yes (transfer to US possible)	Standard Contractual Clauses (SCCs)
Google Ireland Limited	Authentication (sign-in via Google OAuth)	EU	Account identifiers, email, authentication tokens	Yes (transfer to US possible)	Standard Contractual Clauses (SCCs)
TransIP B.V.	Hosting	Netherlands (EU)	All Personal Data processed in the Platform	No	n/a
Mollie B.V.	Payment processing and invoicing	Netherlands (EU)	Name, contact/billing details, payment data	No	n/a
Cloudflare, Inc.	Bot protection on the public registration form	EU	IP address, technical request metadata of visitors	Yes (transfer to US possible)	Standard Contractual Clauses (SCCs)

Table B: AI/LLM providers (sub-processors that process prompts, context data and outputs)

Sub-processor	Service / function	Processing location	Categories of personal data	International transfer	Transfer mechanism
OpenAI	Running AI agents (language model)	EU	Prompts, context data and outputs (may contain Personal Data)	No	n/a
Google	Running AI agents (language model)	EU	Prompts, context data and outputs (may contain Personal Data)	No	n/a

> *To be verified per provider: the exact contracting entity (e.g. OpenAI Ireland Limited; Google Cloud EMEA Limited / Google Ireland Limited) and the EU processing region/data residency by which EU processing is ensured.*

Table C: Customer-activated integrations / connectors (not sub-processors of the Processor)

The external services below are connected only after the Controller activates a Connector. These are services used by the Controller itself; the Controller is itself responsible for them (including its own legal basis, its own agreement with the provider and any international transfer). The Processor does not engage these services as its own Sub-processor and has no control over the storage location. This overview is included for transparency.

Integration / provider	Connector / function	Storage location	Categories of personal data
Google	Gmail and Google Calendar connector	Determined by the Controller/end user	Email content/headers, calendar items, contacts
Microsoft	Outlook, Teams and Microsoft Calendar connector	Determined by the Controller/end user	Email content/headers, chat messages, calendar items
Meta	WhatsApp and Instagram connector	Determined by the Controller/end user	Message content, contact details, phone numbers
LinkedIn	LinkedIn connector	Determined by the Controller/end user	Profile/contact details, message content
Atlassian	Trello connector	Determined by the Controller/end user	Card/task content, names, contact details

A current list of Sub-processors is available at https://www.doenio.nl/en/legal/data-processing-agreement and on request via legal@doenio.nl.

Annex 3: Technical and organisational security measures

The Processor implements at least the following measures, to the extent applicable to the processing under this agreement. Where a frequency or standard is stated, it applies as a minimum framework.

Access management, authentication and authorisation

- role-based access control (RBAC) to production systems on a "least privilege" basis;
- an authorisation model in which rights are granted on the basis of function and necessity;
- mandatory strong passwords and multi-factor authentication (MFA) for administrator access by the Processor's personnel;
- support for multi-factor authentication for end users in the Platform;
- periodic review of access rights.

Encryption

- encryption of personal data in transit using TLS 1.2 or higher;
- encryption of all personal data at rest, including sensitive secrets such as OAuth tokens (AES-256-GCM).

Logging and monitoring

- central audit logs of security-relevant events, including administrator actions;
- monitoring of the Platform and alerting on anomalies;
- log retention period: 12 months.

Incident response

- a documented process for managing Security Incidents and Personal Data Breaches;
- defined roles, escalation paths and communication procedures.

Availability, backup and recovery

- regular backups of personal data: daily;
- backup retention: 7 days;
- periodic recovery tests: annually;
- recovery procedures for access and availability in the event of incidents.

Patch, vulnerability and change management

- patch and update management with timely installation of security updates: critical patches within 7 days;
- vulnerability management;
- change management with staged rollout and rollback capability.

Secure software development (secure SDLC)

- code review and automated tests;

- dependency management and periodic updates of components;
- separation of development, test and production environments.

Tenant isolation (multi-tenant SaaS)

- logical separation and isolation of the data of different Controllers;
- measures to prevent one Controller from gaining access to the data of another Controller.

Security of AI functionalities

- protection of prompts, context data and outputs in line with other Customer Data;
- exclusion of the use of Customer Data for training general models, unless expressly agreed (article 14);
- security of logs of AI processing on a least-privilege basis.

Network and endpoint security

- firewalls and network segmentation;
- security of workstations and endpoints of personnel.

Supplier management

- making equivalent data protection arrangements with Sub-processors (article 6.6);
- periodic assessment of relevant Sub-processors.

Physical security

- physical security of the processing environment is provided through the certified data centres of the hosting providers.

Organisational measures

- confidentiality obligations for personnel, including after termination;
- periodic privacy and information security awareness and training measures;
- process for managing Security Incidents and Personal Data Breaches.

The Processor periodically evaluates these measures and adjusts them based on the state of the art, identified threats and changes in the nature of the processing.