DATA PROCESSING AGREEMENT

FOR THE PROCESSING OF PERSONAL DATA BY VAN PASSE B.V.

Parties:

The client, being a natural person or legal entity that makes use of the services of Van Passe B.V. and, in that context, processes personal data (hereinafter: **Data Controller**);

And:

Van Passe B.V., located at Radarweg 29, 1043 NX Amsterdam, Netherlands, registered with the Chamber of Commerce under number 94604835 (hereinafter: **Processor**);

Hereinafter jointly referred to as the "Parties" and individually as a "Party".

Considering that:

- The Data Controller intends to have certain administrative and financial processing activities carried out by the Processor, whereby the Data Controller determines the purposes and means of this processing. This is within the framework of the agreement concluded between the Parties concerning administrative, accounting, and financial services (hereinafter referred to as the Main Agreement);
- The Processor is willing to comply with the obligations regarding security and other aspects of the General Data Protection Regulation (GDPR) to the extent that they apply to them;
- The Parties, given the requirement of Article 28, Paragraph 3 of the GDPR, wish to lay down their rights and obligations in writing through this Data Processing Agreement;
- The Processor is designated as a Processor in accordance with Article 4, Paragraph 8 of the GDPR in the execution of the Main Agreement;
- The Data Controller is designated as a Controller in accordance with Article 4, Paragraph 7 of the GDPR;
- Where this Data Processing Agreement refers to personal data, this means personal data as referred to in Article 4, Paragraph 1 of the GDPR;

Agree as follows:

Article 1. Purposes of Processing

1. The Processor commits to processing personal data on behalf of the Data Controller under the terms of this Data Processing Agreement. Processing shall only take place within the framework of this Data Processing Agreement and for the purposes defined in the Main Agreement. In Annex 1 of this Data Processing Agreement, the categories of data subjects and personal data covered by this agreement are specified. The Data Controller shall inform the Processor of processing purposes that are not already mentioned in this Data Processing Agreement.
2. The Data Controller determines the purposes for which and the means by which personal data are processed. The Processor has no authority over the purposes and means of processing the personal data.
3. The personal data processed by the Processor on behalf of the Data Controller remain the property of the Data Controller and/or the respective data subjects.

Article 2. Division of Responsibilities

1. The Parties shall ensure compliance with applicable privacy laws and regulations.
2. The processing of personal data by the Processor shall be carried out within a (semi-)automated environment unless otherwise agreed.
3. The Processor shall only process personal data under this Data Processing Agreement in accordance with the instructions of the Data Controller and under the ultimate responsibility of the Data Controller. For all other processing activities that are not reported by the Data Controller, processing performed by third parties and/or for other purposes is not the responsibility of the Processor. The responsibility for such processing lies solely with the Data Controller.
4. The Data Controller guarantees that the content, use, and assignment of processing personal data, as defined in this Data Processing Agreement, are not unlawful and do not infringe on any third-party rights.

Article 3. Obligations of the Processor

1. Regarding the processing activities mentioned in Article 1, the Processor shall ensure compliance with the conditions set by the GDPR for processing personal data in its role.
2. The Processor shall inform the Data Controller, upon request and within a reasonable timeframe, of the measures taken regarding its obligations under this Data Processing Agreement.
3. The Processor shall provide the necessary assistance to the Data Controller whenever required for conducting a data protection impact assessment or prior consultation with the supervisory authority if necessary.
4. The obligations of the Processor under this Data Processing Agreement also apply to individuals processing personal data under the authority of the Processor, including but not limited to employees and external contractors.

Article 4. Transfer of Personal Data

1. The Processor generally processes personal data within the European Economic Area (EEA). If personal data is processed outside the EEA, the Processor shall ensure that the transfer only takes place in compliance with the requirements of the General Data Protection Regulation (GDPR).
2. The transfer of personal data to countries outside the EEA is only permitted if:
   - The relevant country has been recognized by the European Commission as a country with an adequate level of protection (adequacy decision);
   - Standard Contractual Clauses (SCCs), as adopted by the European Commission, are used, with additional measures if required;
   - Other appropriate safeguards are applied, such as Binding Corporate Rules (BCRs) or specific contractual agreements that comply with the GDPR.
3. Use of (sub)processors outside the EEA:
   - The Processor may engage (sub)processors for processing personal data outside the EEA, provided that the Data Controller is informed in advance and appropriate safeguards are in place.
   - The Data Controller remains responsible for ensuring GDPR compliance in relation to the transfer and processing by these (sub)processors.
4. Information Obligation:
   - The Processor shall keep an up-to-date overview of (sub)processors processing data outside the EEA and make it available to the Data Controller upon request.
   - If new transfers outside the EEA are deemed necessary, the Processor shall promptly inform the Data Controller and provide all necessary documentation to ensure GDPR compliance.

Article 5. Engaging (Sub)Processors

1. The Processor may engage (sub)processors to perform specific processing activities. The list of engaged (sub)processors is included in Annex 2.
2. The Processor shall inform the Data Controller in advance of any changes in the list of (sub)processors. The Data Controller has the right to object within 14 days of receiving the notification if there are reasonable objections to the appointment of a new (sub)processor. If the Data Controller raises an objection and no solution is found, the Data Controller has the right to terminate the agreement to the extent that the change directly affects the service provision.
3. The Data Controller remains solely responsible for GDPR compliance when engaging (sub)processors and is obliged to ensure that (sub)processors comply with the obligations arising from this Data Processing Agreement.

Article 6. Security

1. The Processor shall take appropriate technical and organizational measures to protect personal data against loss or any form of unlawful processing (such as unauthorized access, alteration, or disclosure of personal data).
2. The Processor shall strive to maintain security at a level that is appropriate to the state of the art, the nature of the personal data, and the costs associated with implementing security measures.
3. An overview of the technical and organizational measures taken by the Processor to protect personal data:

Technical Security Measures

Encryption of Data	Encryption of stored data and data during transmission (e.g., TLS for network connections).
Access Control	Security of systems with multi-factor authentication (MFA), password management, and role-based access control (RBAC) to grant access to personal data only to authorized users.
Firewall & Intrusion Detection/Prevention Systems (IDS/IPS)	Firewalls and intrusion detection systems to prevent unauthorized access and detect and block suspicious activities.
Anti-malware & Antivirus Software	Regular checks and protection against malware and viruses to keep systems clean and secure.
Regular Software Updates and Patch Management	Keeping software and systems up to date to minimize security vulnerabilities.
Back-ups and Recovery Plans	Regular data back-ups and a disaster recovery plan to prevent data loss in case of incidents.
Secured Data Transmission	Use of secure connections (e.g., VPNs) for access to sensitive systems remotely.
Logging and Monitoring	Registration and monitoring of access and activities, especially in critical systems, to quickly detect unauthorized activities.
Security of Physical Infrastructure	Physical security of servers and data centers, such as locks, secured access, and surveillance systems.
Management of Rights and Accounts	Regular review and monitoring of access rights, with automatic deactivation of inactive accounts.
Organizational Measures	
Privacy and Security Policies	Clear internal guidelines and policy documents that comply with the GDPR and describe how personal data is handled.
Awareness and Employee Training	Regular training and awareness programs on data protection and security practices.
Incident Response and Reporting Procedures	A procedure for reporting data breaches and a response plan for security incidents.
Data Processing Agreements with Third Parties (Subprocessors)	Establishing agreements with third parties that have access to data, defining security and privacy requirements.
Documentation and Logs	Detailed documentation of processing activities and maintaining logs to ensure transparency and for audit purposes.

Limitation of Data Storage and Data Minimization	Only collecting, processing, and storing strictly necessary personal data.
Access Restrictions	Implementation of policies that ensure limited access to personal data based on role and necessity within the organization.
Regular Evaluation of Security Measures	Continuous evaluation and adjustment of technical and organizational measures, taking into account new threats and technological developments.

Article 7. Notification of Data Breaches

1. In the event of a security incident and/or a data breach (which includes a breach of security that accidentally or unlawfully results in the destruction, loss, alteration, unauthorized disclosure, or access to transmitted, stored, or otherwise processed data, as defined in Article 4(12) GDPR), the Processor shall make every reasonable effort to promptly notify the Data Controller of such a breach without undue delay and no later than 48 hours after discovery. The Data Controller will then assess whether notification to the supervisory authorities and/or the data subjects is required. The Processor shall make every effort to provide the most complete, correct, and accurate information possible. The obligation to notify applies only if the breach has actually occurred.
2. The Data Controller shall ensure compliance with any applicable (legal) reporting obligations. If required by law or regulation, the Processor shall cooperate in informing the relevant authorities and affected parties.
3. The notification shall at least include the following information:
   - The (suspected) cause of the data breach;
   - The known and/or expected consequences of the breach;
   - The proposed solution to the breach;
   - Contact details for follow-up on the report;
   - Who has been informed (such as the affected data subject, the Data Controller, or the supervisory authority).

Article 8. Handling Requests from Data Subjects

If a data subject submits a request concerning their personal data to the Processor, the Processor shall forward the request to the Data Controller. The Processor may notify the data subject of this transfer. The Processor shall provide the necessary assistance to the Data Controller in handling the request. If the Data Controller requires additional assistance from the Processor to fulfill a request from a data subject, the Processor may charge costs for this support.

Article 9. Confidentiality and Secrecy

1. The Processor has a duty of confidentiality towards third parties concerning all personal data received from or collected on behalf of the Data Controller under this Data Processing Agreement. The Processor shall not use this information for any purpose other than that for which it was obtained unless it is rendered untraceable to data subjects.
2. The duty of confidentiality does not apply in the following cases:
   - If the Data Controller has explicitly given consent to disclose the information to third parties;
   - If the provision of information to third parties is logically necessary for executing the Main Agreement or this Data Processing Agreement;
   - If there is a legal obligation to provide the information to a third party.

Article 10. Liability

1. The Processor is liable for all damage or harm resulting from non-compliance with, or acting in violation of, the provisions and requirements set forth by the GDPR, and/or for failure to comply with or acting in violation of this agreement, without prejudice to claims based on statutory regulations. The Processor is liable for damage or harm insofar as it results from a data breach, fine, or violation of the GDPR due to an attributable shortcoming of the Processor under this Data Processing Agreement, including any damage or harm to the privacy of data subjects caused by the data breach.

2. The Processor is expressly not liable for any damage suffered by the Data Controller as a result of a fine imposed by one of the national supervisory authorities, including the Dutch Data Protection Authority, particularly in relation to legal reporting obligations.

Article 11. Duration and Termination

1. This Data Processing Agreement comes into effect upon signature by the Parties and on the date of the latest signature.
2. This Data Processing Agreement is valid for the duration specified in the Main Agreement between the Parties, and in the absence of such a provision, it remains valid for as long as the cooperation continues.
3. Once the Data Processing Agreement is terminated, for any reason and in any manner, the Processor shall delete and/or destroy all personal data in its possession.
4. The Parties may only amend this Data Processing Agreement with mutual written consent.

Article 12. Applicable Law and Dispute Resolution

1. This Data Processing Agreement and its execution are governed by Dutch law.
2. Any disputes arising between the Parties in relation to this Data Processing Agreement shall be submitted to the competent court in the district where the Processor is established.

ANNEX 1: SPECIFICATION OF PERSONAL DATA AND DATA SUBJECTS

1. Types of Personal Data

As part of the execution of the Main Agreement, the Processor processes the following categories of personal data on behalf of the Data Controller:

Category of Personal Data	Examples
Identity Data	Name, address, place of residence, date of birth, citizen service number (BSN)
Contact Information	Email address, phone number
Financial Data	Bank account number, invoices, income and expenses, tax-related data
Salary and Employment Data (if applicable)	Payslips, pension information, employment contracts
Transaction Data	Payment history, VAT returns, debtor and creditor information
Company Data	Chamber of Commerce (KvK) number, VAT number, legal structure of the company
Other Data	Any additional data necessary for executing the Main Agreement

2. Categories of Data Subjects

The processing of personal data relates to the following categories of data subjects:

- **Clients** of the Data Controller (self-employed professionals, freelancers, and companies);
- **Customers of clients** (if they are involved in the processing, such as debtors or creditors);
- **Employees of clients** (if salary administration is provided);
- **Contact persons** from business relations of the Data Controller;
- **Website visitors** (if analytical data or form submissions are processed).

3. Purposes of Processing

The processing of personal data by the Processor is exclusively for the following purposes:

- Managing financial administration and accounting;
- Processing tax returns and fulfilling fiscal obligations;
- Managing payroll administration (if applicable);
- Assisting in debtor and creditor administration;
- Performing other administrative and financial services in accordance with the Main Agreement;
- Complying with legal obligations, such as fiscal and labor law regulations.

The Processor shall not process the personal data for any purposes other than those specified in this Annex 1, unless explicitly agreed upon in writing with the Data Controller.

Annex 2 – Overview of (Sub)Processors

1. Introduction

This overview contains the current list of (sub)processors engaged by Van Passe B.V. for the execution of services as described in the Data Processing Agreement. If Van Passe B.V. engages new (sub)processors or makes changes to existing (sub)processors, the Data Controller will be informed in a timely manner and given the opportunity to object.

2. Overview of (Sub)Processors

(Sub)Processor	Purpose of Processing	Processing Location
PandaDoc	Creating, signing, and managing documents and contracts	Outside the EEA*
Pipedrive	CRM management and customer relationship management	Within the EEA
OneDrive	Storage and backup of documents and data	Within the EEA
Make	Automating workflows and integrating applications	Outside the EEA*
Zapier	Connecting and automating data streams between applications	Outside the EEA*
MailChimp	Email marketing and customer communication	Outside the EEA*
Rinkel	Business telephony and communication	Within the EEA
MoneyMonk	Accounting and invoicing	Within the EEA
Calendly	Online appointment scheduling and calendar integration	Outside the EEA*
WordPress	Website management and content publication	Within the EEA
Microsoft Teams	Online meetings and internal communication	Within the EEA
OpenAI	AI-supported customer communication and automation	Outside the EEA*
Visma Nmbrs	Payroll administration and HR processing	Within the EEA
Logius	Access to verification via government services (e.g., DigiD, eHerkenning)	Within the EEA
WhatsApp	Business communication and customer service	Outside the EEA*

* *(Sub)processors processing personal data outside the EEA fall under GDPR regulations for international data transfers. Van Passe B.V. ensures that appropriate safeguards are applied, such as Standard Contractual Clauses (SCCs) or other mechanisms compliant with GDPR.*

3. Changes and Objection Rights

The Data Controller will be notified in advance of changes in the list of (sub)processors and has the right to object within 14 days of receiving the notification against the engagement of a new (sub)processor. If no objection is made within this period, the change will be considered accepted.

Van Passe B.V. remains fully responsible for GDPR compliance when engaging (sub)processors and will, where necessary, conclude appropriate agreements to ensure the protection of personal data.