Data Processing Agreement

(Last updated: 22 April, 2025)

IMPORTANT NOTE

In order to apply this pre-signed document between inwise and the customer, each customer must complete the identification form below, sign it, and send it to inwise by Email at support@inwise.com. The DPA will become legally binding upon receipt of the validly completed copy.

This Data Processing Agreement ("**DPA**") supplements the agreement for the provision of services and products ("**Product**") by inwise LTD, a company incorporated under the laws of the State of Israel, registration number 512961186, of 14 Imber Street, Petach Tikwa, Israel ("**Company**") and the person or entity identified in the table below (the "**Customer**").
The Parties agree to share the responsibility for the processing of personal data in accordance with the requirements of the EU Data Protection Laws.

This DPA also includes Appendix A – Details of the Processing, which forms an integral part of this Agreement. Appendix A outlines the key aspects of how the Customer's Personal Data is processed under this DPA, including the subject matter, duration, nature and purpose of the processing, as well as the categories of data subjects and types of personal data involved. The Company's systems are not intended to process sensitive data, and such data must not be submitted. Appendix A shall be deemed an integral part of this Agreement.

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services ("**Principal Agreement**") between the "**Company**" and the "**Data Processor**" (together, the "**Parties**")

WHEREAS

(A) The Company acts as a Data Controller.
(B) The Company wishes to subcontract certain Services, which involve the processing of personal data, to the Data Processor.

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, which repeals Directive 95/46/EC (General Data Protection Regulation).
(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. <u>Definitions and Interpretation</u>

1.1. Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1. “Agreement” - means this Data Processing Agreement and all Schedules.

1.1.2. “Company Personal Data” - means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement.

1.1.3. “Contracted Processor” - means a Subprocessor.

1.1.4. “Data Protection Laws” - means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country.

1.1.5. “EEA” - means the European Economic Area.

1.1.6. “EU Data Protection Laws” - means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and any national laws implementing or supplementing the GDPR.

1.1.7. “GDPR” - means EU General Data Protection Regulation 2016/679.

1.1.8. “Data Transfer” means:

1.1.8.1. A transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.8.2. An onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be restricted by Data Protection Laws (or by

the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws).

1.1.9. "Services" - means the marketing cloud software tools, solutions, features and services the Company provides.

1.1.10. "Subprocessor" - means any person appointed by or on behalf of a Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.1.11. The terms: "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be interpreted accordingly.

2. <u>Processing of Company Personal Data</u>

2.1. Processor shall:

2.1.1. Comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2. Not process Company Personal Data other than in accordance with the relevant Company's documented instructions.

2.2. The Company hereby instructs the Processor to process the Company Personal Data.

2.3. The Customer represents and warrants that it has all necessary rights, consents, and legal bases to process the Personal Data under applicable Data Protection Laws. The Customer is solely responsible for ensuring:

2.3.1. The legality, accuracy, and integrity of the Personal Data.

2.3.2. Responding to requests from Data Subjects and regulatory authorities.

3. <u>Processor Personnel</u>

The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know or access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor.

The Processor shall ensure that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. <u>Security</u>

4.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall, in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2. In assessing the appropriate level of security, the Processor shall take particular account of the risks presented by processing, especially those resulting from a Personal Data Breach.

5. <u>Sensitive Data Restrictions</u>

The Customer shall not submit or include any Sensitive Personal Data (as defined in Article 9 of the GDPR), such as health data, biometric data, religious or political beliefs, or financial information, in the Company's systems. The Company's platform is not intended or designed to process such data.

6. <u>Subprocessing</u>

6.1. The Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor unless:

- Such appointment is required or explicitly authorized by the Company in writing; and;
- The Subprocessor is bound by a written agreement that imposes substantially the same data protection obligations as set out in this Agreement.

7. <u>Data Subject Rights</u>

7.1. Taking into account the nature of the Processing, the Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, to enable the Company to fulfil its obligations, as reasonably understood by the Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2. The Processor shall:

7.2.1. Promptly notify the Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

7.2.2. Ensure that it does not respond to that request except on the documented instructions of the Company unless it is legally required to do so under

applicable laws. In such a case, and to the extent permitted by law, the Processor shall inform the Company of that legal obligation before responding.

8. Personal Data Breach

8.1. The Processor shall notify Company without undue delay upon becoming aware of a Personal Data Breach affecting Company Personal Data and shall provide sufficient information and cooperation to enable it to meet its obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

8.2. The Processor shall cooperate with the Company and take reasonable commercial steps as directed by the Company, to assist in the investigation, mitigation, containment and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

9.1. The Processor shall provide reasonable assistance to the Company with:

- Any data protection impact assessments (DPIAs); and
- Any prior consultations with Supervising Authorities or other competent data privacy authorities, which the Company reasonably considers to be required under Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law.

Such assistance shall apply solely in relation to the processing of Company Personal Data by the Processor, taking into account the nature of the Processing and the information available to the Contracted Processors.

9.2. In addition, solely in relation to Customers subject to Israeli law, the Processor confirms that it complies with Regulation 15 of the Israeli Privacy Protection Regulations (Data Security), 2017, and Directive 2/2011 of the Israeli Privacy Protection Authority, including by ensuring that all sub-processors engaged on its behalf have signed data processing agreements in accordance with these requirements.

10. Deletion or return of Company Personal Data

Subject to section 9, the Processor shall promptly and in any event within 30 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the “Cessation Date”), delete and procure the deletion of all copies of such Company Personal Data.

The Processor shall certify in writing to the Company that it has complied with the above obligations upon request.

11. Audit rights

11.1. Subject to section 10, the Processor shall make available to the Company upon request, all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company, in relation to the Processing of the Company Personal Data by the Contracted Processors.

11.2. The Company has the right to information and audit under section 10.1 only if the extent of that Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11.3. The Processor shall keep records of its processing activities. Upon written request, it will provide the Company with relevant information to demonstrate compliance. The Company may conduct an audit (or assign a third party), with at least 30 business days' notice, no more than once per year (unless required by law or in case of a data breach), during normal business hours, and without disrupting operations.

12. Data Transfer

12.1. The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the EEA to a country outside the EEA, the Parties shall ensure that the personal data is adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU-approved Standard Contractual Clauses (SCCs) for the transfer of personal data.

13. Limitation of Liability

Each Party's liability under this DPA shall be subject to the "Limitation of Liability" provision set forth in the Principal Agreement.

14. General Terms

14.1. Confidentiality.

Each Party must keep this Agreement and any information received about the other Party and its business in connection with this Agreement ("Confidential Information"), confidential. Such information must not be used or disclosed without the prior written consent of the other Party, except to the extent that:

(a) Disclosure is required by law;

(b) The relevant information is already in the public domain.

14.2. Notices.

All notices and communications under this Agreement must be in writing and shall be delivered personally, sent by post or sent by email to the address or email address specified in the heading of this Agreement, ot to such other address as notified by the Parties from time to time.

15. <u>Term and Termination</u>

This Agreement shall become effective upon execution by both Parties and shall remain in force until the termination of the Principal Agreement or until all processing of Personal Data is completed and such data is deleted or returned to the Company in accordance with Section 10 of this Agreement. Either Party may terminate this DPA upon written notice if the other Party is in material breach of its obligations hereunder and such breach is not cured within 30 days of receiving notice.

16. <u>Governing Law and Jurisdiction</u>

This Agreement shall be governed by the laws of _____.

Any dispute arising in connection with this Agreement, which the Parties are unable to resolve amicably, shall be submitted to the exclusive jurisdiction of the courts of _____, subject to possible appeal to _____.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

	Processor Company	**Customer**
Complete Legal Name	inwise Ltd	
Title of the authorized representative		
Date of Signature		
Country of registration	Israel	
Address	14 Imber st. Petach Tikwa	
Phone number	972-3-5627070	
Email	support@inwise.com	
Signature of the authorized representative		

Appendix A – Details of the Processing

This Appendix A outlines key aspects of the processing of the Customer’s Personal Data, in accordance with Article 28(3) of the GDPR, or equivalent requirements under other applicable data protection laws.

Subject matter: Processing of Personal Data provided by the Customer through the platform for the purpose of marketing, communication, and campaign management.
Duration: Duration of the service agreement.
Nature and purpose of processing: Storage, sending communications, segmentation, track ing interactions, analytics.
Categories of data subjects: Customer's end users, contacts, leads.
Types of personal data: Name, email address, phone number, company name, IP address, engagement data, campaign behavior, browser and device information, location data, cookie data.
Sensitive data: The Company’s systems are not designed to process Sensitive Data. Such data must not be submitted.