Linnovate AI Chatbot

DATA PROCESSING AGREEMENT ('DPA')

Last updated and effective as of June 15, 2026

I. General and Subject matter and term of the DPA

1. This DPA forms part of the SaaS Agreement of your Principal Agreement (as defined below), Privacy Policy and any other applicable terms governing the use of the services provided to you according to the Principal Agreement (collectively the "**LINNO Policies**"). The terms of the LINNO Policies shall apply to this DPA as applicable. In the event of contradiction between this DPA and any of LINNO Policies, the provisions of this DPA shall govern. Any capitalized term not defined herein shall have the meaning ascribed to it in the LINNO Policies.
2. Subject matter of this DPA is the performance of the services by the Processor: according to the Principal Agreement (as defined below).
3. The term of this DPA shall commence and terminate along with the term of the principal agreement executed by and between you (the "**Processor**") and Linnovate Technologies Ltd. 514840156, a registered Israeli Company,. (the "**Controller**") according to which the Processor provides certain services to the Controller (the "**Principal Agreement**").
4. Notwithstanding the above, this DPA may be terminated for important cause by either party with immediate effect. Such an important cause may include but is not limited to: if there is a material breach of the provisions of this agreement by the Processor, for example because the Processor is unable or unwilling to comply with data protection instructions issued by the Controller, or the Processor refuses an inspection by the Controller in violation of this contract.

II. The nature and purpose of the data processing

1. The nature and purpose of the data processing by the Processor are detailed as follows:

   Personalize the interaction of the Controller with its customers and extract business insights from the data.

   - Collection and management of customer service data and personal details of the Controller's customers;
   - Collection and management of contact information of the Controller's customers;
   - Providing the Controller with certain customers services features to the Controller's customers.

2. The types of personal data subject to the data processing are detailed as follows (enumeration/description of data types):

   - Personal data (e.g. title, name, address);

- Contact details (e.g. phone, e-mail address);
- Contract data (e.g. data regarding contractual relationship);
- Marketing data (e.g. data on product or contract interests;
- Customer history, (e.g. previous transactions);
- Use communication preferences;
- Gender and date of birth
- Anything the customers of the Controller is sharing with the services of the Processors, which may be considered as personal data, such as family statue, health situation, economic situation, etc.
- Banking and transaction data
- Personality traits (e.g. Big five);
- Cognitive details (e.g. Tendency to spend);

3. The categories of data subjects affected by data processing are detailed as follows: (enumeration/description of affected data subjects):

    - Customers of the Controller

4. Data Processing shall be carried out within a member state of the European Union (EU) or within a member state of the European Economic Area (EEA). Each and every transfer of personal data to a third country, including the grant of access to Personal Data stored in the EU / EEA from a third country shall require the prior authorization of the Controller (see VIII) and shall only be permitted if the specific conditions of articles 44 of the GDPR are met before Personal Data is transferred, i.e. if an adequate level of protection is ensured by

    - an adequacy decision of the Commission (Art. 45 (3) GDPR);
    - binding corporate rules (Art. 46 (2) (b), 47 GDPR);
    - standard data protection clauses (Art. 46 (2) (c) and (d) GDPR);
    - an approved code of conduct (Art. 46 (2) (e), 40 GDPR);
    - an approved certification mechanism (Art. 46 (2) (f), 42 GDPR), or
    - other measures (Art. 46 (2) (a), (3) (a) and (b) GDPR).

    - The Controller shall be informed in writing of the relevant requirements in the specific case, stating the reasons prior to obtaining the authorization.

III. Controller's Rights and Obligations

1. The Controller remains responsible vis-à-vis the data subjects and ensures that the data processing will be carried out in accordance with the relevant provisions of applicable data protection law, including the GDPR as applicable, and therefore shall be the responsible data Controller in terms of applicable data protection laws.
2. Subject to section X in this agreement, the Controller is the sole responsible to obtaining from the data subjects which are its customers, all the required consents with respect to the processing of their personal data according to this agreement, including their explicit consent for processing special categories of data as defined in the GDPR and profiling, all as applicable according to the applicable law. ANY BREACH OF THIS SECTION BY THE CONTROLLER SHALL BE CONSIDERED AS A MATERIAL BREACH OF THIS AGREEMENT.

Controller shall ensure that such consent is documented and that is made before the Processor processes any Personal Data on its behalf.

3. The Controller has the right to give further instructions to the Processor concerning the data processing.
4. For this purpose, authorized persons on the part of the Controller to provide instructions shall be those persons the Controller shall notify the Processor during their engagement.
5. The recipients of the instructions on the part of the Processor are: Lyron Wahrmann.
6. Changes of the persons entitled to receive or to issue instructions are to be communicated to the respective contractual partner immediately in writing, including in electronic form (e.g. e-mail).
7. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes applicable data protection law. The Processor shall then be entitled to suspend the execution of the relevant instruction until the Controller confirms or changes it. The Controller shall inform the Processor without undue delay, if an error or irregularities in the examination of the contract results have been detected.

IV. Processing, rectification, restriction and erasure of data by the Processor

1. The Processor may solely process personal data on behalf of the Controller pursuant to this DPA and, as the case may be, according to the instructions of the Controller and exclusively for the purposes stated in this DPA. The Processor may not process personal data for any other purposes unless required under applicable law; in the latter case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
2. Copies or duplicates of the data shall never be created without the knowledge of the Controller, with the exception of copies as far as they are necessary to ensure orderly data processing or orderly performance of (remote) maintenance as well as data required to meet regulatory requirements to retain data.
3. The Processor ensures that the data provided by the Controller or collected on its behalf will be processed and stored strictly separated from other data stocks of other commissioned processing/orders, whereas a logical separation is sufficient.
4. The Processor shall not rectify, delete or restrict the processing of the data processed within the scope of the commission on an unauthorized basis, but only according to the documented instructions of the Controller. Where a data subject contacts the Processor directly in this respect, the Processor shall immediately forward this request to the Controller.
5. Information to third parties or the data subject may only be provided by the Processor with prior written authorization of the Controller.
6. As far as the scope of services comprises, the deletion concept, right to be forgotten, rectification, data portability and access by the data subject are to be ensured directly by the Processor in accordance with the documented instructions of the Controller.

V. Quality assurance and other obligations of the Processor

- In addition to complying with the provisions of this contract, the Processor has legal obligations under Articles 28 to 33 GDPR; in this respect, the parties agree on the following:

a) With regard to the appointment of a data protection officer by the Processor, the parties state:

- That as of the date of this agreement, the Processor is not required to appoint a data protection officer. The Controller must be informed immediately of any change of data protection officer.

-

- With regard to the appointment of a representative of the Processor in the EU, the parties state:

- That as of the date of this agreement, the Processor is not required to designated a representative in the European Union in accordance with Art. 27 (1) GDPR. The Controller must be informed immediately of any change with respect of designation of an EU representative.

b) The parties agree upon the following with regard to ensuring the confidentiality pursuant to Art. 28 (3) (b), 29, 32 (4) GDPR:

- The Processor shall ensure that all persons authorized to process personal data belonging to the Controller under the terms of this DPA have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and have previously been made familiar with the data protection provisions relevant for them.
- The Processor and any person subordinated to the Processor who has access to personal data may process such data only in accordance with the instructions of the Controller, including the authorizations granted in this agreement, unless the processing is required by applicable law.
-

c) With regard to the implementation of and compliance with technical and organizational measures required for this processing in accordance with Art. 28 (3) (c), 32 GDPR, the parties agree on the 'Minimum requirements for the technical and organizational measures (TOM)' set out in **Annex 1**. More specific TOMs of the Processor, if applicable, are described in **Annex 2** to this DPA.

d) With regard to dealing with supervisory authorities, the parties agree upon following:

- The Controller and the Processor shall, upon request, cooperate with supervisory authorities within the performance of their tasks.
-
- The Processor shall inform the Controller immediately on audit activities or any other controlling measures of data protection supervisory authorities, insofar as they relate to or have impact on the data processing under this DPA. Same shall apply if a competent authority investigates in the context of administrative or criminal proceedings with regard to the processing of personal data under this DPA.

-

- In case the Controller is subject to an inspection by the supervisory authority, to administrative or criminal proceedings, to liability claims of the data subject or of a third party or to any other claim in connection with the commissioned data processing by the Processor, the Processor shall assist the Controller to the best of his ability.

-

e) With regard to quality assurance, the parties agree on the following:

- The Processor regularly monitors the internal processes and the technical and organizational measures in order to ensure that the performance of the contract within his area of responsibility is compliant with the requirements of the applicable data protection laws and the rights of the data subject.
- The Processor shall make available to the Controller all information necessary to demonstrate compliance with Processors' obligations laid down in this DPA, in particular the execution of TOMs.

VI. Audit rights and assistance obligations

1. The Processor shall make available to Controller, on written request, all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by Controller or an auditor mandated by Controller in relation to the processing of the Personal Data according to this DPA, and subject to confidentiality provisions specify in the Principal Agreement. Both Parties are liable for their own costs arising from the audit.
2. Taking into account the nature of the data processing and the information available, the Processor shall assist the Controller, as far as possible, in fulfilling its obligations laid down in Art. 32 to 36 GDPR concerning the security of personal data, notification obligations in the event of a data breach, data protection impact assessments and prior consultations. This may include but is not limited to:
    - ensuring an adequate level of protection through appropriate technical and organizational measures taking into account the circumstances and purposes of the processing as well as the predicted probability and severity of a possible infringement of rights due to security gaps and enable an immediate determination of relevant infringement events
    - the obligation to report personal data breaches to the Controller without undue delay
    - the obligation to assist the Controller in the context of its obligation to communicate the personal data breach to the data subject and to make all relevant information available to the Controller in this regard without undue delay
    - provision of assistance to the Controller with any data protection impact assessments
    - provision of assistance to the Controller with prior consultations with supervising authorities.
3. The Processor may claim appropriate remuneration only for assistance not included in this agreement or not caused by misconduct on the part of the Processor.

VII. Deletion and return of personal data

1. After termination of this DPA or upon request of the Controller - at the latest upon termination of the Principal Agreement - the Processor shall, at the choice of the Controller, (i) delete or (ii) return to the Controller all the personal data processed under this DPA and any copies hereof, unless applicable law requires further storage of the personal data (e.g. retention obligations). In the latter case, Processor shall ensure that data processing is restricted to that purpose. The same applies to any and all connected test, waste, redundant and discarded material.
2. Documentation which is used to demonstrate orderly data processing in accordance with this DPA and the Principal Agreement shall be stored beyond the contract duration by the Processor in accordance with the respective retention periods. It may hand such documentation over to the Controller at the end of the contract duration to relieve the Processor of this contractual obligation.
3. Processor shall provide, upon request, written certification to the Controller that the Processor has fully complied with this section VII.
4. This Section shall not apply to data stored on third party service providers that provided the Controller and the Processor with Large Language Models.

VIII. Subcontracting

1. Subcontracting for the purpose of this DPA is to be understood as meaning services, which relate directly to the provision of the principal service according to the Principal Agreement. This does not include ancillary services, such as telecommunication services, postal / transport services, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Processor shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of Controller’s personal data, even in the case of outsourced ancillary services.
2. Any commissioning or replacement of subcontractors requires the prior explicit written approval of the Controller (**Annex 3**). The Processor shall conclude corresponding data processing agreements with the subcontractors. The Processor undertakes to set out the data processing agreements with subcontractors in such a way that they reflect the data protection provisions agreed under this DPA. The processor shall regularly monitor compliance with these obligations. Where a sub-processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of the subcontractor’s obligations.
3. The transfer of the Controller's personal data to the sub-contractor and its first activity with regard to this personal data are only permitted provided all requirements for subcontracting are met.
4. Data processing by subcontractors outside the EU must be agreed upon with the Controller prior to data processing. The Processor shall ensure data protection compliance and the guarantees of the subcontractor for compliance with European data protection laws. Appropriate guarantees may be at hand, for example, if the EU standard data protection clauses have been agreed upon with the subcontractor and the data security measures

taken meet the requirements of the GDPR. Notwithstanding the foregoing, any changes shall be documented and communicated to the Controller.

5. The Controller acknowledges that some parts of the Personal Data shall be subcontracted to third parties which provide Large Language Models and Artificial Intelligence. In such event. The Processor cannot ensure that such subcontractors shall enforce the terms of this agreement and that Personal Data shall not be used outside the scope of the DPA. The Controller may review the Processor's agreements with these subcontractors and the Processor's responsibility and liability shall be subject to such agreements back-to-back.

IX. Technical and Organizational Measures

1. The Processor shall document the implementation of the required technical and organizational measures set out in advance of this DPA prior to the start of the processing, in particular with regard to the actual execution of the processing, and shall hand them over to the Controller for inspection. If accepted by the Controller, the documented measures shall become the foundation of this DPA. If the Controller's inspection/audit indicated a need for adjustment, this shall be implemented by mutual agreement.
2. The Processor shall establish TOMs pursuant to Art. 28 (3) (c), 32 and 5 (1), (2) GDPR which guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems and services. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons shall be taken into account pursuant to Art, 32 (1) GDPR [Details in **Annex 1**].
3. TOMs are subject to technical progress and further development. In this respect, it is permissible for the Processor to change the described TOMs, as long as the security level of the defined measures is not reduced, and by prior written notice to the Processor reasonable time ahead. Notwithstanding the foregoing, any changes shall be documented and communicated to the Controller, e.g. by providing an updated list of TOMs. Significant changes must be agreed upon in writing.

X. Liability

1. The parties agree that the Processor shall be liable for any breaches of this DPA caused by the Processor's acts and omissions or negligence. The Processor shall also be liable for any breaches of this DPA caused by the acts and omissions or negligence of its subcontractors (except as stated in section IX) to the same extent the Processor would be liable if performing the services of each subcontractor directly under the terms of the DPA.
2. For the compensation of damages, which a data subject suffers because of an inadmissible or incorrect data processing within the scope of this DPA according to the data protection laws, the Controller may be responsible, if necessary, in relation to the data subject. To the extent that the Controller is required to pay damages to the data subject, the Controller reserves the right of recourse to the Processor, if the latter is liable for this damage.
3. **WITHOUT DEROGATING FROM THE ABOVE, THE CONTROLLER IS THE SOLE RESPONSIBLE TO OBTAIN ALL CONSENTS REQUIRED TO BE COLLECTED**, according to the applicable law, from the data subjects according to this DPA (which are mainly the Controller's customers). The parties agree that the Controller shall be liable for any breaches of this DPA caused by

the Controller's acts and omissions or negligence, including any other breach of applicable law, to which the Controller is subject. The Controller shall indemnify and hold Processor harmless for any breach of this section for the full amount of damage incurred to the Processors due to such aforesaid breach.

4. Part of the Personal Data which Processor may collect from Controller's customers for the Controller, may be considered as Special Category of Personal Data (as defined in the GDPR), and this kind of Personal Data will be collected and be used or processed otherwise only according to this DPA. It is the Controller's sole and full responsibility to obtain **EXPLICIT CONSENT TO THE PROCESSING OF THE PERSONAL DATA FROM CONTROLLER'S CUSTOMERS**. This explicit consent is also required for the profiling which will be made by the Processor as part of the services provided by the Processor to the Controller.
5. The parties agree that the Controller shall be liable for any breaches of this DPA, including not obtaining the required Explicit Consent from the data subjects (its own customers) caused by the Controller's acts or omissions or negligence, including any other breach of applicable law, to which the Controller is subject. The Controller shall indemnify and hold Processor harmless for any breach of this section for the full amount of damages incurred to the Processors due to such aforesaid breach.

-

XI. Incorporation of the Standard Contractual Clauses.

The parties hereby incorporate the EU Standard Contractual Clauses of 2021, with the following choices and references.

4. In respect to section 7, "Docking", the parties agree that Docking is an option to the SCC. Module Two is selected; as Linnovate-AI is the Processor and the Customer is the Processor. However, if other activities shall apply, the relevant module shall be incorporated. In respect to section 9, Option 2, a general written authorization for sub-processors is agreed to undertake between the parties.
5. In respect to section 11, complaints may be lodged with the relevant authority.
6. In respect to section 17 and 18, the governing law shall be Ireland.
7. In respect to the APPENDIX, the following shall be incorporated: The Data Importer and Exporter details are as stated in this DPA.
8. The Categories of Data Subject are the Customer's end-users and customers.
9. The Categories of Personal Data transferred are as required and specified in Linnovate's privacy policy https://linnovate.net/ai-products-Linno-privacy/.
10. The frequency of the transfer is upon demand.
11. The nature of processing is as stated in the Privacy Policy and Data Processing Agreement.
12. The purpose of processing is as stated in the Privacy Policy and Data Processing Agreement.
13. The period of processing is as stated in the Privacy Policy and Data Processing Agreement
14. The sub-processors are as stated in the Privacy Policy and Data Processing Agreement.

15. The supervisory authority is the Irish data protection committee.
16. The Sub-processors are as stated in the Privacy Policy.
17. In respect to ANNEX II, The technical and organizational measures to ensure the security of the data are as stated in the Privacy Policy.

XII. Miscellaneous

1. In case the property of the Controller is endangered by measures of third parties (such as seizure or confiscation), by insolvency or settlement proceedings or by other events, the Processor must inform the Controller without undue delay.
2. Amendments or additions to this DPA must be made in writing to be effective.
3. In the event that one or more current or future provisions of this agreement shall be, or shall be deemed to be, fully or partly invalid or unenforceable, the validity and enforceability of the other provisions of this agreement shall not be affected thereby. The same shall apply in the event that the agreement contains any gaps. The invalid or unenforceable provision shall be replaced by such appropriate provision that, to the extent legally permissible, comes closest to the actual or assumed intention of the parties, in case they had taken such issue into account.
4. All disputes or claims arising out of or relating to this DPA shall be subject to the exclusive jurisdiction of the competent courts in Israel, Tel Aviv.

Annex 1: TOMs – Technical and organizational measures

Minimum requirements for the technical and organizational measures (TOM)

1. Confidentiality (Article 32 paragraph 1 lit. b GDPR)

Physical access control: No unauthorized access to data processing facilities

Electronic access control: No unauthorized use of the data processing and data storage systems

Internal access control (permissions for user rights of access to and amendment of data): No unauthorized reading, copying, changes or deletions of data within the system

Isolation control: The isolated data processing, which is collected for differing purposes

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

Data transfer control: No unauthorized reading, copying, changes or deletions of personal data with electronic transfer or transport

Data entry control: Verification, whether and by whom personal data is entered into a data processing system, is changed or deleted

3. Availability and Resilience (Article 32 Paragraph 1 lit. b GDPR)

Availability control (article 32 paragraph 1 lit. c GDPR): Prevention of accidental or willful destruction or loss

Rapid recovery (article 32 paragraph 1 lit. c GDPR): It is assured that systems used can be rapidly restored in the event of a malfunction.

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 lit. d GDPR; Article 25 paragraph 1 GDPR)

Data protection management: Data protection guidelines and processes are established and their timeliness, compliance and implementation are checked regularly**.**

Incident-Response-Management: In particular, it is ensured that the Controller is informed immediately in the event of data protection incidents.

Data protection by design and default (Article 25 paragraph 2 GDPR): The Processor ensures that its data processing systems are preset and operated in compliance with data protection laws.

Order or contract control: No third party data processing as per article 28 GDPR without corresponding instructions from the Controller

-

Annex 2: Description of the technical-organizational measures (TOM) of the Processor

(If necessary to be replaced by already existing TOM of the Processor.)

1. Confidentiality (Article 32 paragraph 1 lit. b GDPR)	
Physical Access Control e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems	LINNO services is deployed on Google cloud (GCP) and on Google data centers (https://cloud.google.com) Linnovate-AI offices access is control with key card to access building and code to enter specific offices.
Electronic Access Control e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media	All Linnovate-AI documents are sourced on Google Workspace and Office 365. All production system access is limited to production team.
Internal access control (permissions for user rights of access to and amendment of data) e.g. rights authorization concept, need-based rights of access, logging of system access events	Access to data is limited to authorized personnel: - Inside Linnovate-AI portal - Access to GCP - Access to infrastructure services: 360Dialogue, OpenAI & GCP - Roles and permissions inside LINNO services
Isolation Control e.g. multiple client support, sandboxing	LINNO systems are separated into different areas each with its own access control: - Development environment - Production environment - Within production environment, separated logical instance
Pseudonymization - if possible taking into account the purpose of processing (article 32 paragraph 1 lit. a GDPR; article 25 paragraph 1 GDPR): Replacement of the name and other identifiers by a pseudonym (usually a multi-digit letter or number combination, e.g. numeric personnel or customer numbers or user IDs) to impede the attribution of data and persons. Personal data will then only be processed on the basis of the pseudonym, and additional information that allows a connection to the person will be kept separately and will be subject to appropriate technical and organizational measures.	Personal data is encrypted and deleted when no longer needed, upon termination of the agreement.
2. Integrity (Article 32 Paragraph 1 Point b GDPR)	

Data Transfer Control e.g.: encryption, virtual private networks (VPN), electronic signature	All data transfer between servers is performed using encryption or within secured network
Data entry control e.g.: logging, document management	LINNO services have extensive logs of all operations performed and new logs are added when new requirement is defined
3. Availability and Resilience (Article 32 Paragraph 1 lit. b GDPR)	
Availability control (article 32 paragraph 1 lit. c GDPR) e.g.: backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting procedures and contingency planning	LINNO services has been built on top of Google cloud with necessary measures to enable security, integrity and resilience of all systems.
Rapid recovery (article 32 paragraph 1 lit. c GDPR)	Processes are defined in order to be able to recover entire services in case of need.
4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 lit. d GDPR; article 25 paragraph 1 GDPR)	
Data Protection Management e.g. availability of a data protection management system (data protection guidelines), documentation of the data protection measures taken.	N/A
Incident-Response-Management	N/A
Data protection by design and default (Article 25 paragraph 2 GDPR) e.g. minimization of the processing of personal data, early pseudonymization, transparency with regard to the functions and processing of personal data	LINNO platform takes in account data protection requirements in its design.
Contract control e.g.: clear and unambiguous contractual arrangements, formalized order management, strict controls on the selection of the service providers,	All required measures are being taken for contract control.

duty of pre-evaluation, supervisory follow-up checks	

-

Annex 3: List of approved subcontractors

The Controller authorizes the engagement of the following subcontractors:

Name of the subcontractor	Type of subcontracting	Address (location) of the company and if not corresponding: the location of data processing
360Dialogue	WhatsApp Business Service Provider	360dialog GmbH Torstraße 61 10119 Berlin Germany https://www.360dialog.com/en/
Google Cloud Platform	Location & language services	Google Cloud EMEA Limited Gordon House, Barrow Street Dublin 4, Ireland
OpenAI	Provision of large language models	OpenAI Inc, 3180 18th Street Suite 100 San Francisco, CA 94110 United States
OpenRouter	Provision of large language model routing/aggregation services	OpenRouter, Inc., 169 Madison Avenue, New York, NY 10016 United States
Groq	Provision of large language model inference services	Groq, Inc., 2700 Zanker Road, Suite 150, San Jose, CA 95134 United States
ActiveTrail	SMS service	ActiveTrail Ltd Derech Menachem Begin 48 Tel Aviv-Yafo Israel https://www.activetrail.co.il/

The Processor shall inform the Controller of any intended changes concerning the replacement of sub-contractors listed above. The Processor shall not replace the sub-contractor without prior specific written authorization of the Controller.