

WizBI Data Processing Agreement

Version 1.2 · Effective October 17, 2026

This English version governs; a [Hebrew convenience translation](#) is available.

WIZBI AI LTD (וויזבי בינה מלאכותית בע"מ), company number 517297677, 23 Shir HaShirim St., Moshav Berechya, Israel ("**WizBI**")

This Data Processing Agreement (the "DPA") is issued by WizBI.AI Ltd. ("WizBI"), forms part of the [WizBI Terms of Service](#) (the "Terms") and applies to every Customer whose Customer Data includes Personal Data. It is made under Regulation 15 of the Protection of Privacy (Data Security) Regulations, 5777-2017, the Protection of Privacy (Transfer of Data to Databases Abroad) Regulations, 5761-2001, and, where they apply, Article 28 of the GDPR and Article 39 of the LGPD. Capitalised terms have the meaning given in the Terms. For Personal Data this DPA prevails over the Terms, except [Section 14 of the Terms](#) (Limitation of Liability), which applies to this DPA. A countersigned copy is available on request.

Contents

- | | |
|-------------------------------|---|
| 1. Roles | 7. Security Incidents |
| 2. Processing Details | 8. Data Subject Requests and Assistance |
| 3. Security | 9. Retention, Return and Deletion |
| 4. Personnel and WizBI Access | 10. Audit and Information |
| 5. Subprocessors | 11. Customer Obligations |
| 6. International Transfers | 12. Liability, Precedence and Term |
- Annex 1 – Processing Details
 - Annex 2 – Security Measures
 - Annex 3 – Subprocessors and Processing Locations
 - Signature

1. Roles

1.1. **Controller and processor.** For Personal Data within Customer Data, the Customer is the database owner and controller and WizBI is the holder and processor. WizBI processes that Personal Data only under the Terms, the Order Form, the Customer's account settings and Annex 1, which together are the Customer's complete documented instructions.

1.2. **WizBI as controller.** For Service Data, account and User data, Aggregated Data, security, billing and the business relationship, WizBI is an independent controller and the Privacy Policy applies. The Customer instructs WizBI to create Service Data and Aggregated Data and to improve the WizBI Materials under Section 9 of the Terms, and confirms that these are permitted purposes.

1.3. **Unlawful instructions.** If WizBI considers that an instruction breaches the law it will inform the Customer and may decline to carry it out.

2. Processing Details

2.1. **Data and data subjects.** The categories of Personal Data and data subjects are set out in Annex 1 and, where different, in the Order Form.

2.2. **Purposes.** WizBI processes Personal Data for:

- a. providing the Service, including operating models and Agents;
- b. support, onboarding and troubleshooting;
- c. security, monitoring and abuse prevention;
- d. improving the Service for the Customer;
- e. creating Service Data and Aggregated Data under Section 9 of the Terms; and
- f. billing, evidence and legal compliance.

2.3. **Sensitive data.** Data of special sensitivity is processed only if agreed in the Order Form, on the terms and at the price agreed there.

2.4. Systems and operations. WizBI accesses only the Data Sources the Customer connected under Section 6 of the Terms, with the permissions the Customer allocated. The default operations are reading, copying into the Customer's environment in the WizBI cloud, analysis and production of Output. Writing to, changing or deleting in the Customer's systems, and sending messages outside the organisation, are performed only when ordered and marked as such.

3. Security

3.1. Security level. WizBI applies the obligations of the Data Security Regulations at the security level stated in the Order Form, or otherwise the level the Customer has determined for its database, and in any event the measures in [Annex 2](#). A medium or high level may require adjustments and separate pricing.

3.2. Certification. WizBI operates an information security management system certified to ISO/IEC 27001:2022 within the scope of its certificate, and will inform the Customer if the certification lapses and is not renewed.

3.3. Customer's side. The Customer is responsible for security on its side: Users, permissions, passwords, join codes, Local Components and source systems.

4. Personnel and WizBI Access

4.1. Personnel. WizBI employees and contractors who access Personal Data are bound by written confidentiality undertakings, trained, and limited to the access their role requires.

4.2. Account access. Authorised WizBI personnel may access the Customer's account, view conversations and logs, converse with the Agent in the organisation's context and perform actions in the Service at the Customer's request, only for the purposes in Section 4.4 of the Terms. Such access is limited to personnel bound by confidentiality, granted on a least-privilege basis, and subject to WizBI's access-control and logging procedures.

4.3. Automated components. Agents and automated components act as authorised users within the scope defined for them.

5. Subprocessors

5.1. **Approval.** The Customer approves the categories of subprocessors in [Annex 3](#) and their replacement under this Section.

5.2. **Flow-down.** WizBI imposes on each subprocessor, by written agreement (including the subprocessor's standard terms), protection obligations not materially less protective than this DPA, and remains responsible to the Customer for the subprocessor as for its own acts, subject to [Section 14 of the Terms](#).

5.3. **Changes.** WizBI will notify the Customer, by email or in the Service, at least 15 days before a new category of subprocessor starts processing Customer Data. The Customer may object in writing within that period on reasonable data-protection grounds. If no solution is found within 30 days the Customer may terminate the affected Service with a pro-rata refund of prepaid fees; this is the sole remedy. An urgent change needed for security or continuity will be notified as soon as possible.

5.4. **Not subprocessors.** The Customer's own systems and accounts and their vendors (such as the Customer's Priority, monday.com, Dropbox, Google Drive or BigQuery), and external AI agents the Customer connects through MCP or an API, are not WizBI subprocessors. They are governed by the Customer's agreements with them and by Sections 4.7 and 6 of the Terms.

6. International Transfers

6.1. **Locations.** Customer Data may be stored and processed in Israel, the European Union, the United States and other locations where WizBI's providers operate, with appropriate safeguards, as set out in [Annex 3](#) and the Order Form. A Customer that requires storage or processing in a particular region only will state this in the Order Form; absent a statement, the Customer approves the locations in [Annex 3](#).

6.2. **Basis for transfer.** Transfers to the European Union and to countries subject to EU law are made under Regulation 2(8) of the Transfer Regulations. Transfers to the United States and other countries are made under Regulation 2(4), on the basis of the recipient's written undertaking (including in its data processing terms) to meet the conditions of Israeli law, including purpose limitation, confidentiality, security and assistance with data-subject rights, together with Regulation 3 on onward transfer.

6.3. **EEA-origin data.** For Personal Data originating in the European Economic Area, WizBI complies with the Protection of Privacy (Provisions regarding Data Transferred to Israel from the European Economic Area) Regulations, 5783-2023. Onward transfer to the United States is made under the EU-US Data Privacy Framework where the recipient is certified, or otherwise under the EU Standard Contractual Clauses (Module 3), which are incorporated by reference where required.

6.4. **Brazil.** For Personal Data subject to the LGPD, transfers are made under Article 33 on the basis of standard contractual clauses or consent, as applicable.

7. Security Incidents

7.1. **Notice.** WizBI will notify the Customer without undue delay, and no later than 72 hours after becoming aware, of a serious security incident or of any unauthorised use of, or use in excess of authorisation of, Customer Data, even if the investigation is not complete. The notice will include what is known: what happened, the data types, the estimated scope, measures taken and recommendations, with updates as details emerge.

7.2. **Cooperation.** WizBI will cooperate with the Customer, preserve evidence and reasonably assist with notifications to authorities and data subjects. The Customer, as controller, is responsible for its own reporting. Where the law imposes a direct reporting duty on WizBI, WizBI will report and inform the Customer.

7.3. **No admission.** A notification or cooperation under this Section is not an admission of liability.

8. Data Subject Requests and Assistance

8.1. **Requests.** A request for access, correction, deletion or objection that reaches WizBI and relates to Customer Data will be forwarded to the Customer within a reasonable time. WizBI will not respond to the requester beyond acknowledging receipt and referring them to the Customer, unless the law requires otherwise.

8.2. **Assistance.** WizBI will reasonably assist the Customer in handling requests, through the Service's tools or on written request. Assistance of unusual scope is charged at a reasonable rate.

9. Retention, Return and Deletion

9.1. **During the term.** Customer Data is kept for the Subscription Term and the export period in Section 16.9 of the Terms. Conversation history and Agent turns are kept during the Subscription Term for the rolling period in Section 9.8 of the Terms or as set in the Customer's account settings or the Order Form.

9.2. **Deletion.** After the export period WizBI deletes Customer Data from its active systems within 60 days. Copies in backups are overwritten in the normal backup cycle, within 90 days, and are not restored for use. WizBI confirms deletion in writing on request.

9.3. **Exceptions.** WizBI may retain after termination: Service Data and Aggregated Data, which are not Customer Data; billing, invoicing and contract records as required by law and for up to seven years; and Input, Output and logs connected to suspected abuse, a security incident, a claim or a legal hold, for as long as needed to investigate, defend or comply with law. A legal hold (investigation, proceeding, incident or authority demand) suspends deletion until it is lifted.

9.4. **Links.** A link to a file the Service produces is valid for a limited time; the Customer is responsible for the persons with whom it shares such a link.

10. Audit and Information

10.1. **Information.** On request, once a year, WizBI will provide reasonable information demonstrating compliance with this DPA: certificates and reports (including the ISO/IEC 27001 certificate and statement of applicability, where available), a policy summary and answers to a standard security questionnaire. These are WizBI's confidential information.

10.2. **Audit.** An audit is available only where the information above is reasonably insufficient, after a material security incident, or at an authority's demand; once in any 12 months; on 30 days' notice; during business hours; without access to other customers' data, source code or WizBI Materials; by an auditor that is not a competitor of WizBI and is bound by confidentiality; and at the Customer's cost, including WizBI staff time beyond one working day.

11. Customer Obligations

11.1. **Controller duties.** The Customer represents and undertakes that:

- a. it has a lawful basis to collect Customer Data and provide it to WizBI for the purposes of this DPA;
- b. it has given the notice required by Section 11 of the Protection of Privacy Law, including processing by a service provider, by artificial intelligence and outside Israel;
- c. it has classified the security level of its database and informed WizBI;
- d. it will not provide sensitive data that was not agreed;
- e. its instructions are lawful; and
- f. it has performed its duties under Regulation 15 as a party engaging an outsourced service, including the risk assessment before engagement.

12. Liability, Precedence and Term

12.1. **Liability.** Each party's liability under this DPA is subject to Section 14 of the Terms. A sanction, fine or statutory compensation imposed on a party for its own act or omission is borne by that party.

12.2. **Precedence.** For Personal Data this DPA prevails over the other parts of the Terms, except Section 14 of the Terms.

12.3. **Changes in law.** Where a change in law requires it, WizBI will update this DPA and the updated version applies under Section 17 of the Terms.

12.4. **Term.** This DPA applies for as long as WizBI processes Personal Data for the Customer, including the retention periods in Section 9.

Annex 1 – Processing Details

Item	Default (unless the Order Form states otherwise)
Data subjects	Users (employees, consultants and other persons the Customer admits); the Customer's customers, suppliers and contacts; participants in a group or shared conversation in which an Agent participates; persons appearing in the Customer's business data.
Categories of data	Identification and contact details of Users (name, phone, email, role); content of conversations, messages, files and recordings, including, in a group or shared conversation in which an Agent participates, the messages needed for the Agent to respond; business data of the Customer that may include data about its employees, customers, suppliers and contacts; online identifiers and IP addresses.
Sensitive data	None, unless agreed in the Order Form.
Purposes	<u>Section 2.2 of this DPA.</u>
Operations	Read-only from the Customer's systems; copy to the Customer's environment in the WizBI cloud; analysis; production of Output; write, change, delete or external messaging only where ordered.
Security level	As stated in the Order Form, under the Data Security Regulations.
Processing locations	<u>Annex 3.</u>
Retention	<u>Section 9 of this DPA</u> and Section 9.8 of the Terms.

Annex 2 – Security Measures

WizBI operates an information security management system certified to ISO/IEC 27001:2022 and applies reasonable administrative, physical and technical measures within it, including:

- encryption of data in transit and at rest;
- logical separation of customer data and permissions between customer organisations at the application layer;
- role-based access control and least-privilege permissions, with strong authentication for WizBI personnel, including multi-factor authentication for administrative access;
- read-only access to the Customer's systems by default, through dedicated credentials;
- logging and monitoring of access to Customer Data, including every question and data access;
- secure storage of connection credentials, not displayed in the interface;
- model providers operated under commercial terms that do not permit training on Customer Data;
- vendor and subprocessor management;
- backup and recovery procedures;
- a security-incident response procedure; and
- confidentiality undertakings and training for personnel.

Further detail provided on request, including answers to security questionnaires, is information only and not part of this DPA.

Annex 3 – Subprocessors and Processing Locations

WizBI uses subprocessors in the following categories, at the processing locations stated. Further detail is provided to the Customer on request.

Category	Purpose	Location
Cloud and storage (Google Cloud)	Hosting, storage and processing of the Service and Customer Data	EU, US
AI models (Google; other providers where used)	Generating responses, analysis, transcription	EU, US and other locations where the provider operates
Messaging channels and email	Delivering messages on the channels the Customer connects, and email	Per provider
Public web search	Answering questions that need public information from the web	Per provider

Category	Purpose	Location
Analytics	Measuring and improving the Service	US, EU
Payments and bookkeeping	Invoicing, payment processing, accounts	Israel, EU, US

Not subprocessors: the Customer’s own systems and accounts that it connects, their vendors, and external AI agents the Customer connects ([Section 5.4](#)).

Signature

(Optional – this DPA applies automatically under the Terms; a countersigned copy is provided on request.)

	WizBI.AI Ltd.	Customer
Name	Omer Cohen	
Title	CEO	
Signature		
Date		