Data Processing Agreement

This translation is provided for convenience; the Turkish text prevails.

1. Parties and roles

This agreement (the "**DPA**") is an annex to and part of the Cloud Service and Subscription Agreement (the "**Service Agreement**"). Its parties are:

- the **company** registered in the iyibir Cloud panel (the "**Customer**"), which is the **data controller** for the personal data in Customer Data;
- **İyibir Yazılım ve Teknoloji San. Tic. Ltd. Şti.** ("**iyibir**"); address 23 Nisan Mahallesi Atabulvarı Guzell Tower İş Merkezi No:2, 16230 Nilüfer / Bursa, Türkiye; MERSIS 0211110454100001; which is the **data processor** for that data.

The DPA is accepted on the Customer's behalf by its authorised person, who declares that they are authorised to bind the company.

Data iyibir processes for its own purposes (account, invoice, support and security data of the Customer's users) is outside this DPA; iyibir is the data controller for it and the Privacy Notice (KVKK) applies.

2. Definitions

The definitions of the Turkish Personal Data Protection Law No. 6698 ("**KVKK**") and its secondary legislation apply in this DPA. In addition:

- **Customer Data:** as defined in the Service Agreement; for this DPA, the personal data within it.
- **Sub-processor:** a third party iyibir uses to process Customer Data and that has access to Customer Data.
- **Breach:** a security event that leads to Customer Data being unlawfully obtained by others, altered, deleted or made unavailable.

3. Subject, purpose and duration of processing

- **Subject:** providing the Cloud Products (iyibir Copilot, iyibir Mind, iyibir WMS and, where offered, iyibir Workforce) and iyibir Assistant to the Customer.
- **Purpose:** answering Users' questions from the Customer's Logo ERP (and, if defined, payroll) data; producing boards, reports and documents; writing documents a User approves to Logo; running warehouse operations; running digital employee routines the Customer configures; keeping the records needed for these.
- **Nature:** reading, transferring (to the language model, through iyibir's model gateway), storing, organising, displaying, writing to Logo (only with approval), deleting.
- **Duration:** for the term of the Service Agreement and afterwards until the deletion under Section 13 is complete.

4. Data categories and data subjects

The personal data processed depends on the Customer's Logo installation, the data sources it connects and the Users' questions. Typically:

- **Data subjects:** the Customer's employees; representatives and employees of its customers and suppliers (people on account cards); Users; where Workforce is used, contact persons of the Customer's debtors.

- **Identity and contact:** name, title, e-mail, phone, address, tax or national identity number (as far as present on account cards).
- **Finance and customer transactions:** account movements, invoices, delivery notes, orders, collections and payments, bank account (IBAN) details.
- **Employee and payroll (if a payroll data source is defined):** personnel number, pay, deductions, social security details, leave and attendance records.
- **Special categories of personal data:** the payroll database may contain health reports, trade union membership or similar special-category data. The Cloud Products contain no ready-made queries targeting these fields; the Customer accepts that such data may be read in answer to a question, and its obligations under Section 11.
- **User content:** conversations, uploaded documents, boards, write proposals and their results.

5. Instructions

1. iyibir processes Customer Data only on the Customer's documented instructions. The Service Agreement, this DPA, the Customer's panel and product settings and Users' requests and approvals in the Service are the Customer's instructions.
2. iyibir does not use Customer Data for its own purposes, sell it, share it with third parties or **use it to train artificial intelligence models.**
3. If iyibir believes an instruction breaches the law, it tells the Customer without delay and may suspend carrying it out.
4. If law or a decision of a competent authority compels iyibir to disclose Customer Data, iyibir notifies the Customer before disclosure unless prohibited.

6. Security measures

Based on Article 12 KVKK and the Board's Personal Data Security Guide, iyibir applies the following technical and organisational measures:

- **Read-only access.** The PaaS Agent reads the Customer's database only with a read-only user; it checks on every connection that the user has no write permission and does not run if it finds one. Every read is a single SELECT statement; statements that reach outside the database, connect to another server or read server information are refused.
- **Approved writes.** Writing to Logo happens only with a body a User has previewed and approved in the product and that is stored on the server, through Logo's own REST service; no delete requests are sent; the same approval is never executed twice; every write is recorded as proposal, approval and result.
- **Connection security.** The PaaS Agent connects outwards only; no inbound port is opened in the Customer's network. All traffic is encrypted with TLS. Database and Logo REST details stay only on the Customer's server, in an encrypted store.
- **Separation of companies.** Company and user identity are read only from the signed session token; a company cannot reach another company's data; a request for another company's record returns "not found".
- **Authentication.** Passwords are stored as one-way hashes; access tokens last 30 minutes; machine and agent identities work with short-lived, narrowly scoped tokens.
- **Hosting.** Servers and databases are on RNG Bilişim's infrastructure in Türkiye; Customer Data is stored in Türkiye; each module has its own database schema; services run with restricted database users, not superusers.
- **Staff.** Only iyibir technical staff who need it for their role can reach production systems; staff are bound by confidentiality; access is logged.

- **Model gateway.** Requests to a language model pass through iyibir's model gateway, running on iyibir's server in Türkiye. Provider keys are held only in the gateway. The gateway writes the content of requests and answers to no record; it records only the company, a pseudonymous (hashed) identifier of the person, the type of job, the amount used and the cost, and limits the rate of use per company.
- **Monitoring.** Logs, traces and metrics of the Service are kept in iyibir's own monitoring system on its own server, with internal access only (logs 14 days); traffic records under Law No. 5651 are kept for 2 years.
- **Continuous improvement.** Security vulnerabilities are fixed with priority; measures are updated as technology develops. iyibir may change these measures provided the overall level of security is not reduced.

7. Sub-processors

The Customer gives iyibir general authorisation to use the following sub-processors:

- **OpenAI, L.L.C. (USA):** the language model in the Cloud Products and iyibir Assistant; requests are sent through iyibir's model gateway. The User's question and the Customer Data needed to produce the answer (for example query result rows) are sent to the model. Requests are sent with storage switched off (store=false); OpenAI does not store requests or answers (except OpenAI's abuse-monitoring logs, kept for at most 30 days), processes them only at the time of the request and does not use them for model training. Although not stored, the data leaves for the USA to be processed; the transfer is governed by Section 8.
- **RNG Bilişim Teknolojileri San. ve Tic. Ltd. Şti. (Türkiye):** the infrastructure hosting the Service's servers and databases; Customer Data is stored in Türkiye.
- **Google (Google Workspace, outside Türkiye):** sending and receiving iyibir's iyibiryazilim.com.tr e-mails through the Gmail infrastructure, including service notices and the Workforce messages the Customer configures.

1. This list is published in its current form in the panel as it changes.
2. iyibir enters into a written agreement with each sub-processor containing obligations no less protective than those in this DPA, and is responsible to the Customer for the sub-processor's performance.
3. Adding a new sub-processor or replacing an existing one is announced in the panel and to the authorised person's e-mail address **at least 30 days** before the sub-processor gets access to Customer Data. The Customer may object on reasonable grounds within that period; if the parties find no solution, the Customer may terminate the Service Agreement under its Section 16; iyibir refunds the price of the bought and unused credits under that Section.
4. If iyibir later runs the language model on its own server in Türkiye, this is announced as the removal of a sub-processor.

Vercel Inc. (USA), which serves the static files of the panel and web interfaces, does not access Customer Data; it processes only the IP and request details of the person opening a page, which is described in the Privacy Notice. iyzico (İyzi Ödeme ve Elektronik Para Hizmetleri A.Ş., Türkiye), which takes payments, does not access Customer Data either; payment and billing details are described in the Privacy Notice.

8. Transfers abroad

1. Customer Data sent to the language model is processed by OpenAI in the USA; Customer Data in e-mails is processed by Google outside Türkiye. OpenAI not storing requests does not change this: because the data leaves Türkiye to be processed, this is a transfer abroad within the meaning of Article 9 KVKK.
2. As there is no adequacy decision of the Personal Data Protection Board for these countries, iyibir makes these transfers under Article 9 KVKK as amended by Law No. 7499 and the Regulation on the Procedures and Principles for the Transfer of Personal Data Abroad, using the Board's **processor-to-**

processor standard contract, and notifies each contract to the Personal Data Protection Authority within **5 business days** of signature.

3. As data controller, the Customer informs data subjects of this transfer in its privacy notice.
4. iyibir transfers no Customer Data abroad other than as set out in this Section and Section 7.

9. Breach notification

1. When iyibir becomes aware of a Breach affecting Customer Data it notifies the Customer **without delay and at the latest within 48 hours**, to the authorised person's e-mail address and in the panel.
2. The notice states, as far as known at the time, when the Breach happened, its nature, the categories of data and approximate number of people affected, its likely consequences, the measures taken and proposed, and iyibir's contact person; it is completed as new information becomes known.
3. iyibir takes the measures needed to contain the Breach at once and provides the information and help the Customer needs to notify the Personal Data Protection Board within 72 hours and to notify data subjects.
4. Notifying the Board and data subjects is the Customer's obligation as data controller; iyibir does not notify on the Customer's behalf without the Customer's written request.

10. Data subject requests and assistance

1. If a data subject request about Customer Data reaches iyibir directly, iyibir does not answer it and forwards it to the Customer without delay.
2. iyibir provides reasonable help for the Customer to answer requests under Article 11 KVKK, assess data security and meet requests from the Board. For help requiring more than ordinary effort, the parties agree the fee in advance.

11. Customer obligations

As data controller the Customer:

1. undertakes that it has a legal basis to process the data it connects to the Service, that it has informed data subjects, including of the transfer to iyibir and abroad, and that it has obtained their explicit consent where required.
2. defines the payroll data source only when it needs it; meets the conditions of Article 6 KVKK and the adequate measures the Board requires for special categories of data; and uses product roles so that only the Users who need it can reach payroll data.
3. defines only a read-only database user for the PaaS Agent and keeps the server on which the agent runs secure.
4. manages its Users and their permissions inside the products, and closes the access of people who leave.

12. Audit

1. To show compliance with this DPA, iyibir provides once a year, on the Customer's written request, documents and information describing its security measures.
2. If that is not enough, or the Board requires it, the Customer may carry out an audit with at least **30 days'** written notice, in business hours, without disrupting iyibir's operations and through an independent auditor bound by confidentiality. The Customer bears the cost of the audit; the audit does not include access to other customers' data. If the audit finds a breach, iyibir asks nothing of the Customer for its own costs.

13. Deletion and return

1. When the Service Agreement ends, Customer Data is kept for **30 days**, during which the Customer may export it. If the Customer asks in writing within that period, iyibir delivers the data under Section 11 of the Service Agreement.
2. At the end of the period deletion starts and is completed, backups included, at the latest **90 days** after the day the Service Agreement ended.
3. The Customer's core business data is in its own Logo database; iyibir keeps no copy of that database, so it is not affected by this deletion.
4. iyibir keeps records it must keep by law (for example the audit trail of write operations, invoices) only for that purpose and for the statutory period.
5. On the Customer's request iyibir confirms in writing that deletion is complete.

14. Liability

The parties' liability under this DPA is subject to Section 17 of the Service Agreement. This does not remove liabilities that KVKK imposes on the data controller and data processor as mandatory rules; under Article 12/2 KVKK the parties are jointly responsible for security measures.

15. Term, changes and acceptance

1. The DPA takes effect together with the Service Agreement and lasts until the deletion under Section 13 is complete.
2. A new version of the DPA takes effect under the procedure in Section 21 of the Service Agreement (announcement at least 30 days ahead, renewed acceptance, termination right for a Customer who does not accept). Sub-processor changes are governed by Section 7 and need no new version of the DPA.
3. Acceptance is recorded electronically with the document version, content fingerprint, accepting person and company, time and IP address.
4. If the DPA and the Service Agreement conflict, the DPA prevails as to personal data.
5. The DPA is governed by Turkish law; jurisdiction is as in the Service Agreement. The Turkish text is binding.