Legal document · annex to the T&C

Data Processing Agreement (DPA)

The data processing agreement under Article 28 GDPR for the use of the Monolith ERP service. It applies to all our customers on identical terms; on request we also provide it as a signed document.

This data processing agreement (hereinafter: the **Agreement** or **DPA**) is an inseparable annex to the Terms and Conditions (hereinafter: the **T&C**) and governs the processing of personal data carried out in the course of using the Monolith ERP system (hereinafter: the **Service** or the **System**). The Agreement comes into existence and is binding between the parties upon acceptance of the T&C, without a separate signature; at the Customer's request the parties also execute a signed document with content identical to this text.

The parties to the agreement

Controller (hereinafter: the **Customer**) — the natural or legal person subscribing to the Service:

Name / company name: .....
Registered office: .....
Tax number: ..... · Company registration number: .....
Representative: ..... · E-mail: .....
Data protection contact: .....

Processor (hereinafter: the **Service Provider**):
5PL ERP Solutions Kft. · Registered office: 2724 Újlengyel, Petőfi Sándor utca 48., Hungary
Tax number: 32956522-2-13 · EU VAT number: HU32956522 · Company registration number: 13-09-244440
E-mail: erp@5pl.hu · Phone: +36 20 504 8805
Data protection contact: erp@5pl.hu

The parties agree as follows on the basis of **Article 28 of Regulation (EU) 2016/679 (GDPR)** on the protection of natural persons with regard to the processing of personal data.

1. Subject matter of the Agreement and the roles of the parties

In the course of using the Service, the Service Provider **processes personal data on behalf of and on the instructions of the Customer**. With regard to such data, the **Customer qualifies as the controller** (Article 4(7) GDPR) and the **Service Provider as the processor** (Article 4(8) GDPR).

The Agreement covers personal data uploaded by the Customer to the System, generated in the System in the course of the Customer's activity, or received into the System through integrations enabled by the Customer (webshop, marketplace, courier service, invoicing and payment provider).

The Service Provider qualifies as an **independent controller** solely in respect of its own processes (website contact, quotations, contract management, invoicing, customer service, administration of the System's user accounts); these are governed by the Privacy Policy, not by this Agreement.

2. Details of the processing

The **subject matter, nature, purpose and duration** of the processing, the **categories of data subjects** and the **types of personal data** processed are set out in **Annex 1** to this Agreement (Article 28(3) GDPR).

The Service **is not intended** for the processing of special categories of data under Article 9 GDPR or criminal-conviction data under Article 10 GDPR. If the Customer nevertheless uploads or transmits such data to the System, it does so at its own responsibility and on its own legal basis, and must inform the Service Provider in advance so that the parties can agree on the necessary additional safeguards.

3. Obligations of the Customer (controller)

The Customer warrants that:

- it has an **appropriate legal basis** for the processing of the personal data uploaded to or received into the System, and has taken the necessary steps to inform the data subjects;

- its instructions to the Service Provider are **lawful** and do not infringe the GDPR or any other data protection legislation;
- on its own side it ensures the secure handling of user accounts, passwords and API keys, keeps permissions up to date and revokes the access of departing employees;
- the operation configured in the System (enabled integrations, automatic notifications, data retention settings) complies with its own privacy policy.

As controller, the Customer is entitled to give **documented instructions** to the Service Provider; this Agreement, the T&C, the intended use of the Service, the settings made in the System and any separate instruction sent in writing to erp@5pl.hu qualify as documented instructions.

4. Obligations of the Service Provider (processor)

Pursuant to Article 28(3) GDPR, the Service Provider undertakes the following obligations:

- **Processing on instructions** — it processes personal data solely on the documented instructions of the Customer, including with regard to transfers to a third country. If it is required by law to process data otherwise, it informs the Customer before processing, unless the law prohibits this on important grounds of public interest. The Service Provider immediately informs the Customer if, in its opinion, an instruction infringes the GDPR or other data protection provisions.
- **Confidentiality** — it ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Only those employees and contributors have access to the data whose tasks require it (the "need-to-know" principle).
- **Security of processing** — it takes the technical and organisational measures required by Article 32 GDPR; these are described in detail in **Annex 3**.
- **Sub-processors** — it engages further processors solely under the conditions set out in Section 5.
- **Assistance with data subject rights** — it assists the Customer in fulfilling data subject requests in accordance with Section 8.
- **Cooperation regarding the obligations under Articles 32–36** — taking into account the information available to it, it assists the Customer in complying with the security obligations, in handling and notifying personal data breaches, in carrying out data

protection impact assessments (DPIA) and, where necessary, in prior consultation with the supervisory authority.

- **Deletion or return** — after the end of the provision of the Service it acts in accordance with Section 11.
- **Demonstrating compliance** — it makes available to the Customer the information necessary to demonstrate compliance with the obligations set out in this Agreement, and allows for audits under Section 9.

The Service Provider **does not use for its own purposes** the personal data covered by this Agreement, and does not disclose it to any third party — other than the sub-processors listed in Annex 2 and transmissions made on the Customer's own instruction.

5. Sub-processors

By accepting this Agreement, the Customer gives the Service Provider a **general written authorisation** to engage further processors. The complete current list of the sub-processors engaged is set out in **Annex 2**.

The Service Provider notifies the Customer of the engagement of any new or replaced sub-processor **at least 15 days in advance** (by notice published in the System or by e-mail). The Customer may **object** on reasonable grounds within 15 days of the notice. If the parties are unable to resolve the objection by consultation, the Customer is entitled to terminate its subscription to the Service with extraordinary notice, with a pro-rata refund of the fee for the remaining period.

The Service Provider imposes on sub-processors **data protection obligations identical to those in this Agreement**, and remains fully liable to the Customer for the performance of the sub-processor's obligations.

6. Security of processing

Taking into account the state of the art, the costs of implementation and the nature, scope and risks of the processing, the Service Provider implements appropriate technical and organisational measures to protect personal data (Article 32 GDPR). A detailed description of the measures applied is set out in **Annex 3**.

The Service Provider reserves the right to develop and modify the measures, provided that the level of protection achieved is not reduced.

7. Personal data breach

The Service Provider notifies the Customer of any personal data breach it detects affecting data covered by this Agreement **without undue delay and in any event within 48 hours of becoming aware of it**, at the contact address provided by the Customer.

The notification includes — to the extent of the information available — the nature of the breach, the approximate categories and number of data subjects and records concerned, the likely consequences and the measures taken or proposed. Where the information cannot be provided at the same time, the Service Provider supplements it in phases without further undue delay.

Notification to the supervisory authority (Article 33 GDPR) and communication to the data subjects (Article 34 GDPR) are the obligations of the Customer as controller; the Service Provider assists the Customer in this by providing the information available to it and by reasonable cooperation.

8. Exercise of data subject rights

Using the tools available in the System (search, export, rectification, erasure, restriction of access), the Service Provider assists the Customer in fulfilling data subject requests — access, rectification, erasure, restriction, objection and data portability.

The Service Provider **does not independently fulfil** data subject requests received directly by it, but forwards them to the Customer without delay and informs the data subject accordingly.

For assistance requested by the Customer that cannot be performed with a function available in the System (e.g. a bespoke query or data extraction), the Service Provider may charge a reasonable fee communicated in advance.

9. Audits and inspections

At the Customer's written request, the Service Provider makes available **within 30 days** the information necessary to demonstrate compliance with the obligations undertaken in this Agreement (e.g. a description of the measures, a completed security questionnaire, certificates).

The Customer, or an independent auditor mandated by it and bound by confidentiality, is entitled to carry out an on-site or remote inspection **on the basis of prior written consultation of at least 15 days, during working hours, without disproportionate disruption to operations, at most once per calendar year**. In the event of a personal data breach or an authority procedure, the Customer may also initiate an extraordinary inspection.

The audit **may not extend** to the data of other customers, the business secrets or source code of the Service Provider, or information the disclosure of which would infringe the rights of a third party. The auditor may not be a competitor of the Service Provider. The costs of the audit are borne by the Customer, unless the audit reveals a material breach by the Service Provider.

10. Transfers to third countries

The Service Provider stores personal data **within the European Union (EEA)**.

Transfers outside the EEA take place solely subject to the safeguards under Chapter V GDPR — an adequacy decision, the European Commission's Standard Contractual Clauses (SCC) or other appropriate safeguards. The Service Provider has concluded agreements containing such safeguards with the sub-processors established outside the EEA listed in Annex 2.

If the Customer, on its own decision, connects a provider established outside the EEA (e.g. a foreign marketplace, courier or payment provider), the resulting transfer **qualifies as an instruction of the Customer**, and the Customer as controller is responsible for its legal basis and safeguards.

11. Deletion and return of the data

Upon termination of the Service, the Service Provider, at the Customer's choice, **returns (exports) the personal data in a machine-readable format** or **erases** them.

The data export may be requested within **30 days** of the termination of the Service. After this deadline — or on the basis of an earlier erasure request by the Customer — the Service Provider erases the data from the production system, and from the backups upon expiry of the given backup cycle, but no later than **within 90 days**.

Data whose retention is required by law (e.g. accounting or tax rules) need not be erased; the Service Provider retains such data separately, with restricted further processing, solely for the statutory purpose.

At the Customer's request, the Service Provider issues a written statement confirming the erasure.

12. Confidentiality

The Service Provider treats the data covered by this Agreement and the Customer's business secrets as confidential. The mutual confidentiality obligations of the parties are set out in the Non-Disclosure Agreement (NDA) and in Section 14.3 of the T&C, which apply together with this Agreement.

13. Liability

The parties are liable for damage caused by processing in accordance with Article 82 GDPR. The Service Provider as processor is liable where it has not complied with obligations specifically directed to processors, or where it has acted outside or contrary to the lawful instructions of the Customer.

The Customer is liable where its instruction to the Service Provider was unlawful, or where it uploaded personal data to the System without an appropriate legal basis; any resulting administrative fine or damage is borne by the Customer.

The general limitation of liability under the T&C **does not limit** the GDPR-based liability under this Section.

14. Term of the Agreement

The Agreement enters into force upon acceptance of the T&C (or, in the case of a separately signed document, upon its signature) and remains in force for as long as the Service Provider processes personal data on behalf of the Customer.

Sections 11 (deletion and return) and 12 (confidentiality) survive the termination of the Agreement.

The Service Provider may adapt the Agreement to legislative changes; it notifies the Customer of any material amendment at least 15 days in advance. If the Customer does not

accept the amendment, it may terminate its subscription to the Service before the amendment takes effect.

15. Miscellaneous provisions

Matters not regulated in this Agreement are governed by the T&C, the GDPR and Hungarian law, in particular Act CXII of 2011 on informational self-determination and freedom of information.

In the event of a conflict, the provisions of this Agreement prevail over the T&C in matters of data processing.

If any provision of the Agreement becomes invalid, this does not affect the validity of the remaining provisions; the invalid provision is replaced by a valid provision closest to the parties' intention.

Contact for data protection matters: erp@5pl.hu.

Signatures

The parties sign this Agreement in approval, having read and interpreted it, as being in all respects in accordance with their intention. Place and date: ....., ... 20..... .

Customer (controller)
5PL ERP Solutions Kft. (processor)

Annex 1 — Details of the processing

Subject matter and nature of the processing: processing operations in the Monolith ERP system relating to the management of the Customer's orders, buyers, inventory, procurement and customer communication — collection, recording, organisation, storage, retrieval, use, transmission to the integrated systems enabled by the Customer (marketplaces, webshops, courier services, invoicing and payment providers), and the sending of notification e-mails on behalf of the Customer.

Purpose of the processing: the provision of the Service (the Monolith ERP system and related services) to the Customer, as set out in the T&C and in this Agreement.

Duration of the processing: the term of the subscription, or until deletion or return under Section 11.

Categories of data subjects:

- buyers, orderers and prospects of the Customer's webshops and marketplace channels;
- contact persons of the Customer's business partners and suppliers;
- employees and agents of the Customer who are users of the System;
- recipients of the notification, order status and invoice e-mails sent on behalf of the Customer.

Types of personal data processed: first and last name; billing and delivery address; e-mail address; phone number; order details (products, quantity, value, date, identifiers); transaction and payment data (payment method, status, transaction identifier — the System does not store full payment card numbers); shipping and parcel tracking data; customer communication history (e-mail, chat, tickets); user account data (username, permissions, password hash) and system logs (IP address, timestamp, operation).

Special categories of data: the Service is not intended for the processing of data under Articles 9 and 10 GDPR.

Annex 2 — Sub-processors

The Service Provider engages the following sub-processors for the provision of the Service. The list is complete and current; the Service Provider gives prior notice of any change in accordance with Section 5.

- **DigitalOcean, LLC** — 105 Edgeview Drive, Suite 425, Broomfield, CO 80021, USA.
  Activity: the hosting and cloud infrastructure used to operate the Monolith system (servers, database, storage, backups).
  Place of processing: a data centre located within the European Union (EEA).
  Safeguards: a data processing agreement under Article 28 GDPR; for any access from outside the EEA, the European Commission's Standard Contractual Clauses (SCC).
- **Twilio Inc. (SendGrid)** — 101 Spear Street, Suite 500, San Francisco, CA 94105, USA.
  Activity: delivery of the bulk transactional e-mails sent from the System on behalf of the Customer (order confirmations, status notifications, invoice delivery).
  Data processed: recipient name and e-mail address, message subject and content, delivery status.

Safeguards: a data processing agreement under Article 28 GDPR, the European Commission's Standard Contractual Clauses (SCC) and/or EU–US Data Privacy Framework certification.

The operators of integrations enabled by the Customer on its own decision (marketplaces, webshop engines, courier services, invoicing and payment providers) are **not sub-processors of the Service Provider**: the Customer is in a contractual relationship with them, and any transmission to them takes place on the Customer's instruction.

Annex 3 — Technical and organisational measures (TOM)

Pursuant to Article 32 GDPR, the Service Provider applies the following technical and organisational measures:

- **Access control:** role- and permission-based access management in the System; individual, named user accounts; passwords stored only as one-way, salted hashes; the option of two-factor authentication; minimisation of the scope of administrative access.
- **Encryption in transit:** all traffic of the System and the integrations runs over an encrypted channel (HTTPS/TLS); API calls use key-based authentication.
- **Protection at rest:** the database and backups are kept in a protected environment with restricted access; access keys and passwords are stored encrypted and separately.
- **Physical security:** operation takes place in the certified, EEA-based data centre of the sub-processor (DigitalOcean), which provides access control, video surveillance, fire protection and uninterruptible power supply.
- **Segregation:** the data of individual customers are handled in a logically segregated manner; no customer has access to another customer's data; live personal data may not be used in test and development environments.
- **Logging and traceability:** the system logs logins, permission changes and material data operations; logs can be reviewed retrospectively.
- **Availability and recovery:** regular automatic backups; separate storage of backups; a documented recovery procedure and regular verification of restorability.
- **Software security:** regular updating of system components and dependencies; out-of-cycle installation of security patches; version control and review of development changes.

- **Organisational measures:** a written confidentiality undertaking from every employee and contributor with access to the data; internal data protection and incident handling procedures; regular review of access permissions and immediate revocation upon termination of the legal relationship.
- **Incident handling:** a documented procedure for detecting, investigating and recording personal data breaches and for the notification within 48 hours under Section 7.

The Service Provider reviews the measures regularly and adapts them to changes in risk. The current version of this Annex is available at all times on this page, or on request via the contact page.