Data Processing Agreement (DPA)

Version 2.1. Effective date: October 21, 2026

This Data Processing Agreement ("**DPA**") is entered into between

Controller: the customer identified in the Agreement (the "**Customer**"),

and

Processor: TODO for AI Korlátolt Felelősségű Társaság (registered office: 1121 Budapest, Csorna utca 3. 2. em. 2. ajtó, Hungary; company registration number: 01-09-443906; VAT number: HU32812154; represented by: Tamás Havlik, managing director) ("**TODOforAI**"),

as part of the agreement, order or subscription between the parties for the use of the TODOforAI services (the "**Services**") under the TODOforAI Terms of Service available at https://todofor.ai/legal/terms-of-service (the "**Agreement**"), pursuant to Article 28 of Regulation (EU) 2016/679 ("**GDPR**").

1. Definitions

1.1 "**Personal Data**", "**Processing**", "**Controller**", "**Processor**", "**Data Subject**", "**Supervisory Authority**" and "**Personal Data Breach**" have the meanings given in the GDPR.

1.2 "**Customer Data**" means any Personal Data that TODOforAI Processes on behalf of the Customer in the course of providing the Services, including data contained in todos, attached files, connected accounts, credentials and outputs.

1.3 "**Sub-processor**" means any third party engaged by TODOforAI to Process Customer Data.

1.4 "**Applicable Data Protection Law**" means the GDPR, the Hungarian Act CXII of 2011 on Informational Self-Determination and Freedom of Information (Info tv.), and any other data protection laws applicable to the Processing under this DPA.

2. Roles and Scope

2.1 With respect to Customer Data, the **Customer is the Controller** (or a Processor acting on behalf of another Controller) and **TODOforAI is the Processor**.

2.2 Each party shall comply with its own obligations under Applicable Data Protection Law. As controller, the Customer is responsible in particular for the legal basis of the Processing and for informing Data Subjects, including when collecting data about third parties. This does not affect TODOforAI's obligations under applicable law or this DPA.

2.3 The subject matter, duration, nature and purpose of the Processing, the types of Personal Data and the categories of Data Subjects are set out in **Annex I**.

3. Processing Instructions

3.1 TODOforAI shall Process Customer Data only on the Customer's documented instructions, including with regard to transfers to third countries, unless required to do so by EU or Member State law; in such a case, TODOforAI shall inform the Customer of that legal requirement before Processing, unless the law prohibits such information on important grounds of public interest.

3.2 The Agreement, this DPA, and the Customer's use and configuration of the Services (including the todos submitted, the AI models selected, the optional tools used, the services connected, and any provider restrictions configured under Section 6.5) constitute the Customer's complete documented instructions.

3.3 TODOforAI shall immediately inform the Customer if, in its opinion, an instruction infringes Applicable Data Protection Law.

3.4 TODOforAI does not use Customer Data for its own purposes and does not train AI models on Customer Data.

4. Confidentiality

TODOforAI shall ensure that persons authorised to Process Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and Process Customer Data only as needed to provide the Services.

5. Security

5.1 TODOforAI shall implement and maintain technical and organisational measures appropriate to the risk, as required by Article 32 GDPR. The current measures are described in **Annex II**.

5.2 TODOforAI may update these measures from time to time, provided the updates do not reduce the overall level of protection.

6. Sub-processors

6.1 The Customer provides general written authorisation for TODOforAI to engage the Sub-processors listed in **Annex III**.

6.2 TODOforAI shall inform the Customer of any intended addition or replacement of Sub-processors at least **14 days** in advance, by email and on https://todofor.ai/legal/gdpr, giving the Customer the opportunity to object on reasonable data-protection grounds. If the parties cannot resolve an objection in good faith, the Customer may terminate the affected Services without penalty and receive a pro-rata refund of prepaid fees.

6.3 TODOforAI shall impose on each Sub-processor, by written contract, data protection obligations no less protective than those in this DPA, and shall remain fully liable to the Customer for the performance of each Sub-processor's obligations.

6.4 **Use of AI providers and optional tools.** Customer Data is sent to an AI model provider listed in Annex III, Part B only when a model of that provider is used for a request, and only to that provider. Customer Data is sent to an optional tool provider listed in Annex III, Part C only when the agent uses that tool for a request. The Customer may indicate in Annex III, Part B which AI providers may be used; TODOforAI then configures the Customer's workspace accordingly and does not send Customer Data to any other AI provider.

6.5 **Provider restrictions (Team and Scale plans).** On Team and Scale plans, the owner of the Customer's organisation may restrict processing to AI providers that process data within the European Union and/or AI providers with zero data retention. While a restriction is in effect, requests are routed only to permitted providers, and models or features without a permitted provider are unavailable to the organisation's members. Restrictions configured by the owner form part of the Customer's documented instructions.

7. Data Subject Rights

Taking into account the nature of the Processing, TODOforAI shall assist the Customer by appropriate technical and organisational measures, insofar as this is possible, in fulfilling the Customer's obligation to respond to Data Subject requests (access, rectification, erasure, restriction, portability, objection). If a Data Subject makes a request directly to TODOforAI, TODOforAI shall promptly forward the request to the Customer and shall not respond substantively without the Customer's authorisation, unless legally required.

8. Personal Data Breach

8.1 TODOforAI shall notify the Customer **without undue delay, and in any event within 48 hours**, after becoming aware of a Personal Data Breach affecting Customer Data, so that the Customer can meet its 72-hour notification obligation to the Supervisory Authority under Article 33 GDPR.

8.2 The notification shall, to the extent known, describe the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed to address the breach and mitigate its effects. Where the information cannot be provided at the same time, it may be provided in phases without undue delay.

8.3 TODOforAI shall reasonably cooperate with the Customer and take reasonable steps to mitigate the effects of the breach.

9. Assistance with the Controller's Obligations

Taking into account the nature of the Processing and the information available to it, TODOforAI shall assist the Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR, in particular regarding security of Processing, notification of Personal Data Breaches and communication to Data Subjects, data protection impact assessments (Article 35 GDPR) and prior consultations with Supervisory Authorities (Article 36 GDPR).

10. Deletion and Return of Data

10.1 Upon termination or expiry of the Services, TODOforAI shall, at the Customer's choice, delete or return all Customer Data, and delete existing copies, within **30 days**, unless EU or Member State law requires storage of the Personal Data.

10.2 The Customer may export Customer Data via the Services' export functionality at any time during the term.

11. Audits

11.1 TODOforAI shall make available to the Customer all information reasonably necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR.

11.2 TODOforAI shall allow for and contribute to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer, subject to: (a) at least **30 days'** prior written notice; (b) no more than **once per 12-month period**; (c) the auditor being bound by confidentiality; (d) the audit being conducted during business hours without unreasonable disruption to TODOforAI's operations; (e) each party bearing its own costs of the audit. Points (a) and (b) do not apply where they would defeat the purpose of the audit in the event of a Personal Data Breach, a reasonably substantiated suspicion of non-compliance, or a requirement of a Supervisory Authority.

12. Data Location and International Transfers

12.1 Customer Data stored by TODOforAI (databases, files, backups, workspaces) is stored exclusively in the **European Union**, in data centres in Germany and Finland (Helsinki). Data sent to a Sub-processor to perform a request is processed, and may be retained for a limited period under its terms, at the locations stated in Annex III.

12.2 On Team and Scale plans, AI model providers can be limited under Section 6.5 to those that process data within the European Union; these are listed in Annex III, Part B/1. The restriction does not change the processing location of infrastructure providers or optional tools.

12.3 Where Processing by a Sub-processor involves a transfer of Personal Data to a country outside the EU/EEA, Annex III states the transfer mechanism for each Sub-processor: an adequacy decision of the European Commission (including the **EU-US Data Privacy Framework**, where the recipient is certified), or the European Commission's **Standard Contractual Clauses** (Decision (EU) 2021/914) included in the Sub-processor's data processing terms. Where Annex III states "Provider terms", no transfer mechanism under Chapter V GDPR is in place with that provider at the effective date of this DPA; AI model providers in this group may be excluded by the Customer under Section 6.4 or 6.5; optional tool providers in this group receive only the data listed for them in Annex III, Part C.

13. Liability

Each party's liability arising out of or related to this DPA is subject to the limitations and exclusions of liability set out in the Agreement, without prejudice to Section 6.3 and Article 82 GDPR. This DPA does not limit either party's liability to Data Subjects or Supervisory Authorities under Applicable Data Protection Law.

14. Term, Precedence, Governing Law

14.1 This DPA takes effect on the effective date of the Agreement (or, if later, the date both parties sign this DPA) and remains in force for as long as TODOforAI Processes Customer Data.

14.2 In case of conflict between this DPA and the Agreement regarding the Processing of Personal Data, this DPA prevails.

14.3 This DPA is governed by the laws of **Hungary**, and disputes are subject to the exclusive jurisdiction of the courts of Hungary.

14.4 This DPA is made in Hungarian and English. In case of any discrepancy between the two language versions, the Hungarian version prevails.

Annex I: Details of Processing

Subject matter: Provision of the TODOforAI Services: an AI agent platform that completes the Customer's todos, including by signing in to and acting within services connected by the Customer.

Duration: The term of the Agreement, plus the deletion period in Section 10.

Nature and purpose of Processing: Storage, transmission, analysis and automated processing of Customer Data as necessary to (a) execute todos submitted by the Customer, including via AI models, optional tools and services connected by the Customer; (b) authenticate to connected services; (c) provide support; and (d) operate, secure and troubleshoot the Services.

Categories of Data Subjects:

- the Customer's employees, contractors and authorised users;
- the Customer's own customers, suppliers, partners and other business contacts, to the extent contained in Customer Data (e.g. correspondents, invoice recipients, CRM contacts).

Types of Personal Data:

- identification and contact data (names, email addresses, phone numbers, job titles, organisations);
- access credentials for connected services (stored in an encrypted vault);
- business and financial data contained in todos (e.g. invoices, receivables, contracts);
- communication content (emails, messages, drafts processed or produced by the agent);
- usage and technical data (logs, IP addresses, device identifiers).

Special categories of data: Not intended to be processed. The Customer shall submit data under Articles 9 and 10 GDPR only on the basis of a separate written agreement.

Annex II: Technical and Organisational Measures

Encryption

- TLS 1.2+ for all external connections; communication between the agent and clients runs over an end-to-end encrypted channel based on the Noise Protocol Framework.
- Secrets stored in the TODOforAI vault are encrypted at rest and access-controlled.

Access control

- Role-based access; access to production systems is restricted to authorised personnel on a need-to-know basis.
- Multi-factor authentication for administrative access.
- Logical separation of Customer Data per account and workspace.

Execution isolation

- Agent workloads and browser automation run in isolated virtual machines (Firecracker microVMs), without cross-customer access.

AI model data handling

- On every AI provider account it uses, TODOforAI has opted out of the use of inputs and outputs for model training. The only exceptions are providers whose terms do not offer this opt-out; the model picker marks these models, and they are used only when selected.
- AI providers may retain inputs and outputs for a limited period under their own terms (for example for abuse monitoring). Zero data retention is not currently in place with any AI provider; where it becomes available, it will be marked in Annex III.

Operations security

- Logging and monitoring of production systems; an audit log of every tool call made by the agent.
- Regular software updates and vulnerability management.
- Backups with defined retention; tested restore procedures.

Organisational measures

- Confidentiality obligations for all personnel.
- Documented incident-response procedure with escalation and customer notification (Section 8).
- Due diligence on Sub-processors and contractual flow-down of data protection obligations.
- Data minimisation: only data needed to complete a todo is processed.

Human approval

- In the permission settings of the Services, the Customer can require prior user approval for specific actions (e.g. sending an email, making a payment, deleting data); where so configured, the agent prepares the action and carries it out only after approval.

Annex III: Authorised Sub-processors

Current list: https://todofor.ai/legal/gdpr

Transfer mechanism: "Not applicable (EU)" means processing within the EU/EEA. "Adequacy" means a European Commission adequacy decision for that country. "EU-US DPF" means the recipient is certified under the EU-US Data Privacy Framework. "SCCs" means the EU Standard Contractual Clauses included in the provider's data processing terms. "Provider terms" means the transfer relies only on the provider's own terms and privacy commitments, with no DPF certification or SCCs in place (see Section 12.3). Where two mechanisms are listed for one provider, each applies to part of the traffic to that provider.

A) Infrastructure (always used)

Sub-processor	Purpose	Location of processing	Transfer mechanism
Hetzner Online GmbH (Germany)	Servers, databases, file storage, backups, sandboxes	Germany, Finland (EU)	Not applicable (EU)
PostHog, Inc. (USA)	Product analytics (usage events, no message content)	EU (Frankfurt)	EU-US DPF
Stripe Payments Europe, Limited (Ireland)	Payments (billing data only)	EU, USA	EU-US DPF
Cloudflare, Inc. (USA)	DNS, CDN, network security, TLS termination	Global network, EU points of presence	EU-US DPF
Plus Five Five, Inc. (Resend) (USA)	System notification emails	USA	EU-US DPF
650 Industries, Inc. (Expo) (USA)	Mobile push notifications (notification text)	USA	EU-US DPF

B) AI model providers (used only when a model of that provider is selected; the Customer may mark the permitted providers, see Section 6.4)

B/1. AI model providers processing data within the European Union (the only providers used under an EU restriction pursuant to Section 6.5)

☐	Sub-processor	Purpose	Location of processing	Transfer mechanism
☐	Mistral AI SAS (France)	Mistral models	EU	Not applicable (EU)
☐	Amazon Web Services EMEA SARL (Luxembourg)	Claude models via Amazon Bedrock, EU cross-region inference	EU	Not applicable (EU)
☐	Google Cloud EMEA Limited (Ireland)	Claude models via Google Vertex AI, EU multi-region	EU	Not applicable (EU)
☐	Microsoft Ireland Operations Limited (Ireland)	OpenAI models via Microsoft Azure, EU Data Zone	EU	Not applicable (EU)
☐	OpenAI Ireland Limited (Ireland)	OpenAI models with EU data residency	EU	Not applicable (EU)
☐	OpenRouter, Inc. (USA)	Routing via the EU in-region gateway to EU-hosted model providers only, with no fallback outside the EU	EU (request content); TODOforAI's account and billing data in the USA, without Customer Data	Not applicable (EU)

B/2. AI model providers processing data outside the European Union

☐	Sub-processor	Purpose	Location of processing	Transfer mechanism
☐	Anthropic Ireland, Limited (Ireland) / Anthropic, PBC (USA)	Claude models	USA	SCCs, Provider terms
☐	OpenAI Ireland Limited (Ireland) / OpenAI, L.L.C. (USA)	GPT models, realtime voice, image generation	USA	SCCs, Provider terms
☐	Google Cloud EMEA Limited (Ireland) / Google LLC (USA)	Gemini models, image generation	USA, global	EU-US DPF, SCCs
☐	SpaceXAI LLC (xAI) (USA)	Grok models	USA	SCCs
☐	Cohere Inc. (Canada)	Command models	Not stated by the provider	Adequacy (Canada)

☐	**Sub-processor**	**Purpose**	**Location of processing**	**Transfer mechanism**
☐	Cerebras Systems Inc. (USA)	Fast models, including the voice assistant	USA	Provider terms
☐	OpenRouter, Inc. (USA)	Routing to other model providers (only the provider of the selected model receives the request)	USA and the serving provider's country	Provider terms
☐	Other US model hosts: Deep Infra Inc., Together Computer, Inc., Groq, Inc., Novita AI, Atlas Cloud, Meta Platforms, Inc. (Llama API), OpenCode	Open-weight and other models	USA	Provider terms
☐	Model providers based in China: DeepSeek, Moonshot AI, Z.ai (Zhipu), MiniMax, Xiaomi (MiMo), SiliconFlow	Their own models	China or the provider's country	Provider terms

Customer Data is not sent to an AI provider that the Customer has not permitted (Section 6.4).

C) Optional tools (used only when the agent uses the tool for a request)

Category	**Purpose**	**Data sent**	**Location of processing**	**Transfer mechanism**
Speech providers (4)	Speech-to-text, text-to-speech	Voice audio, reply text	EU, USA, not stated by the provider	Not applicable (EU), EU-US DPF, Adequacy (UK), Provider terms
Music generation (1)	Music generation	Prompt, lyrics	Not stated by the provider	Provider terms
Web search and page reading (2)	Web search, reading public web pages	Search query or public URL	USA, not stated by the provider	Provider terms
Social profile reading (4)	Reading public social media profiles	Public profile URL or name	USA, not stated by the provider	Not applicable (EU-based provider), Adequacy (Israel), Provider terms

The names of the providers in this part are listed in the signed copy of this DPA. Request it at privacy@todofor.ai.

Web search, web page reading and social profile reading receive only a search query, a public URL or a public profile name, not other Customer Data.

D) Services connected by the Customer

Services that the Customer connects itself (e.g. its own Gmail, Microsoft 365, CRM, invoicing or social media accounts) operate under the agreement between the Customer and that service provider, act on the Customer's behalf, and are **not** Sub-processors of TODOforAI.