

# Data Processing Agreement

Under Article 28 GDPR – AI assistant and website hosting. Effective from 6 October 2026.

## 0. The Parties

**Controller:** the Customer named in the Individual Agreement (quote) (the "Controller").

**Processor:** Vilbergsson Viktor E.V., a Hungarian sole proprietorship (the "Processor").

|                  |                                                    |
|------------------|----------------------------------------------------|
| REGISTERED SEAT  | Patakpart u. 19/2., 2111 Szada, Hungary            |
| REGISTRATION NO. | 62901350                                           |
| TAX NO.          | 92435335-1-33                                      |
| PRIVACY CONTACT  | Viktor Vilbergsson, viktor@vmv.hu, +36 20 232 0742 |

## 1. Subject matter and scope

- 1.1. This agreement sets out the terms required by Article 28(3) GDPR. It applies whenever the Processor processes personal data on behalf of the Controller while performing services under the VMV General Terms and Conditions (ÁSZF) and the Individual Agreement (together, the "Main Agreement").
- 1.2. Annex 1 sets out, for each service, the subject matter, duration, nature and purpose of the processing, the types of personal data and the categories of data subjects.
- 1.3. Terms defined in Article 4 GDPR (such as personal data, processing, controller, processor, data subject and personal data breach) have the same meaning in this agreement. "GDPR" means Regulation (EU) 2016/679, "Infotv." means Hungarian Act CXII of 2011, and the "AI Act" means Regulation (EU) 2024/1689.
- 1.4. This agreement forms part of the Main Agreement. Where the two differ on the processing of personal data, this agreement prevails.

## 2. Rights and obligations of the Controller

- 2.1. The Controller is responsible for:
- having a legal basis for the processing;
  - informing data subjects under Articles 13–14 GDPR (the template in Annex 4 can help);
  - ensuring that its instructions to the Processor are lawful.
- 2.2. The Controller's documented instructions are:
- the Main Agreement and this agreement;
  - the settings the Controller enters in the portal (e.g. notification email address, practice details);
  - the Controller's written instructions, including instructions given by email.

An instruction that requires a material change to the service is subject to a separate agreement.

- 2.3. The Controller will not instruct the Processor to use the AI assistant to collect health data or any other special category data under Article 9 GDPR. It will not upload such data to the system, for example in a

document.

### 3. Obligations of the Processor

**3.1. Processing on instructions.** The Processor processes personal data only on the Controller's documented instructions, including with regard to transfers to third countries. The exception is processing required by Union or Member State law. In that case, the Processor informs the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest.

**3.2. Infringing instructions.** The Processor immediately informs the Controller if, in its opinion, an instruction infringes the GDPR or other data protection provisions.

**3.3. Confidentiality.** Only persons who have committed themselves to confidentiality, or who are under a statutory obligation of confidentiality, may access the personal data.

**3.4. Security.** The Processor implements the technical and organisational measures required by Article 32 GDPR (Annex 2). It may update the measures as technology develops, provided the level of protection does not decrease.

**3.5. Data minimisation in the AI assistant.**

- a. Before storage, the system automatically redacts any sentence in a visitor's message that mentions a symptom, complaint, medication, diagnosis or health condition, as well as Hungarian social security (TÁJ) numbers.
- b. A medical filter removes such sentences or clauses before any model call. They therefore reach neither the answering model nor the model that extracts callback details.
- c. Conversations are deleted automatically 30 days after they are created.
- d. Callback notifications sent to the Controller contain no health data.
- e. Neither the Processor nor the model providers use the data to train AI models. Model calls are sent with a no-training setting, so they can only be routed to providers that do not train on requests.
- f. IP addresses are kept only as an irreversible identifier hashed with a daily-rotating salt, used to prevent abuse.

The Parties acknowledge that the automatic filter relies on typical health-related expressions in Hungarian, English and German, so it may not recognise every mention of health data. The Processor keeps improving the filter, and the Controller asks data subjects in its privacy notice not to share health data in the chat.

**3.6. Data subject rights.** The Processor uses appropriate technical and organisational measures to help the Controller respond to data subject requests. If a data subject contacts the Processor directly, the Processor forwards the request to the Controller within 5 business days and does not answer it on the merits. On the Controller's instruction, the Processor exports, corrects or deletes the specified data within 10 business days.

**3.7. Assistance.** The Processor helps the Controller meet its obligations under Articles 32–36 GDPR: security, breach notification, data protection impact assessments and prior consultation. The help reflects the nature of the processing and the information available to the Processor. For an impact assessment, it provides a description of the AI assistant and its data flows. The Parties agree in advance on the cost of assistance beyond the usual scope.

**3.8. Records.** The Processor keeps the record of processing activities required by Article 30(2) GDPR.

### 4. Roles under the AI Act

The Processor develops the AI assistant and makes it available, so it is the provider under the AI Act. The Controller, which uses the system on its own website, is the deployer. The Processor designs the AI assistant to

tell users at the start of each conversation that they are interacting with an AI system (Article 50(1)). It also marks the generated replies in a machine-readable format (Article 50(2)). Annex 3, point M3.5 of the ASZF sets out the division of tasks in detail.

## 5. Sub-processors

**5.1.** The Controller gives general written authorisation to engage the sub-processors listed in Annex 3 (Article 28(2) GDPR).

**5.2.** Before adding or replacing a sub-processor, the Processor notifies the Controller by email at least 15 days in advance. Within that period, the Controller may object in writing on reasonable grounds. The Parties will then consult in good faith. If they cannot agree, the Controller may terminate the affected service with effect from the date of the change, without penalty. In that case, the Processor refunds the unused part of any prepaid fees pro rata.

**5.3.** If a sub-processor has to be replaced urgently, for security reasons or because its service ends, the Processor may make the change at the same time as notifying the Controller. The Controller may then exercise its right to object afterwards.

**5.4.** By contract, the Processor imposes on each sub-processor the same data protection obligations that bind the Processor itself (Article 28(4) GDPR). The Processor remains fully liable to the Controller for the performance of its sub-processors.

## 6. Transfers to third countries

**6.1.** Data is stored primarily in the European Union: the database runs in Ireland and the application in Frankfurt (Annex 3).

**6.2.** Data is transferred outside the European Economic Area only under the conditions of Chapter V GDPR. One such condition is an adequacy decision, including the EU–US Data Privacy Framework (DPF) for certified recipients. Another is the European Commission’s standard contractual clauses (SCCs, Decision (EU) 2021/914), with supplementary measures where needed. Annex 3 states the transfer mechanism for each recipient.

**6.3.** The Controller approves the transfers listed in Annex 3.

## 7. Personal data breaches

**7.1.** The Processor notifies the Controller of a personal data breach without undue delay, and no later than 48 hours after becoming aware of it. The notice goes to the contact email address the Controller has provided and, where available, also by phone.

**7.2.** To the extent available, and in phases if necessary, the notification describes:

- the nature of the breach;
- the categories and approximate number of data subjects and records concerned;
- the likely consequences;
- the measures taken or proposed;
- a contact point.

**7.3.** The Processor cooperates in investigating the breach and mitigating its effects, and documents the breach. It notifies authorities or data subjects on the Controller’s behalf only on the Controller’s instruction or where the law requires it.

8. Information and audits

8.1. On request, the Processor makes available the information needed to demonstrate compliance. This includes, for example, this agreement, the description of the measures in Annex 2, the sub-processor list and the sub-processors’ available certifications.

8.2. The Controller, or an independent auditor it appoints who is bound by confidentiality, may carry out one audit per calendar year. More frequent audits are allowed after a breach or at an authority’s request. Audits must be announced at least 30 days in advance. They take place during business hours, without disproportionate disruption, and primarily remotely or on the basis of documents. The Controller bears the cost of the audit. Sub-processors are audited on the basis of their reports and certifications.

9. Liability

The Parties are liable to data subjects under Article 82 GDPR. Between the Parties, the liability rules of the Main Agreement (ÁSZF, section 8) apply, except for liability that cannot be limited by law.

10. Term, termination and return or deletion of data

10.1. This agreement remains in force for as long as the Processor processes personal data on the Controller’s behalf under the Main Agreement.

10.2. When the Main Agreement ends, the Processor acts as the Controller chooses. On request, it exports the personal data in a machine-readable format within 15 days. Within 30 days after termination, it deletes all personal data, including copies, unless Union or Member State law requires storage. Data held in sub-processors’ backups is deleted at the end of the backup cycle. On request, the Processor confirms the deletion in writing.

10.3. The obligations of confidentiality and deletion survive termination until they are fulfilled.

11. Final provisions

11.1. This agreement may be amended in writing. The exception is Annex 3, which is updated under section 5.

11.2. This agreement is governed by Hungarian law. This English version is a translation for convenience; if the versions differ, the Hungarian text prevails.

Annex 1 – Details of the processing

A) AI assistant – chatbot

|         |                                                                                                                                                                                                                                                                        |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Purpose | Answering website visitors’ questions from the Customer’s knowledge base. Recording callback and appointment requests and forwarding them to the Customer. Monitoring service quality through the conversations, ratings and unanswered questions shown in the portal. |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Operations</b>         | Collection (chat window), redaction, storage, answer generation with a language model (knowledge-base search, answer drafting, automatic fact check), extraction of callback details, notification email, display in the Customer's portal, deletion.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Data subjects</b>      | Visitors who use the chat (patients and prospective patients). Customer staff whose names appear on the public website or in uploaded documents. Staff who use the portal.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Personal data</b>      | <p><b>Conversation:</b> the visitor's messages (redacted before storage) and the assistant's replies; language and time; title and URL of the page where the chat was opened; a random session identifier; ratings of replies.</p> <p><b>Callback request:</b> name, phone number or email address, requested service, preferred time, a short organisational note (without health data).</p> <p><b>Technical data:</b> an irreversible identifier derived from the IP address with a daily-rotating salt. If bot protection is triggered (after many messages), the Cloudflare Turnstile verification data.</p> <p><b>Knowledge base:</b> text of the public website and of uploaded documents (files are not stored), and practice details.</p> <p><b>Portal:</b> staff email addresses and login times.</p>                                                                                                               |
| <b>Special categories</b> | The AI assistant does not ask for health data and does not knowingly process it. If a visitor nevertheless provides such data, the filtering in section 3.5 redacts it. The name of the requested service (e.g. teeth whitening, consultation) is recorded as needed for the callback.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Retention</b>          | <ul style="list-style-type: none"> <li>• <b>Conversations and messages:</b> 30 days, then automatic deletion.</li> <li>• <b>Callback requests:</b> 180 days from creation, then automatic deletion. Earlier when the Main Agreement ends or at the Controller's request.</li> <li>• <b>Knowledge base and practice details:</b> until the Main Agreement ends. Content changed on the website is refreshed at the weekly re-crawl; pages deleted from the website are removed from the knowledge base when the Controller tells us.</li> <li>• <b>Login links:</b> deleted 7 days after they expire.</li> <li>• <b>Abuse-prevention counters</b> (with the pseudonymised IP identifier): a few days, then automatic deletion.</li> <li>• <b>Application logs:</b> without message content, for the hosting provider's log retention period.</li> <li>• <b>Model providers and the email service:</b> see Annex 3.</li> </ul> |

## B) AI assistant – voice assistant

The voice assistant is under development, and no processing currently takes place under this service. Before launch, the Processor will add the service's details to this annex and notify the Controller under section 5. The addition will cover the phone number, audio and transcripts, call recording, retention periods and sub-processors.

## C) Website hosting and maintenance

|                |                                                                  |
|----------------|------------------------------------------------------------------|
| <b>Purpose</b> | Hosting, maintaining and troubleshooting the Customer's website. |
|----------------|------------------------------------------------------------------|

|                      |                                                                                                                                                                                                                                                                                                                  |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Data subjects</b> | Website visitors, people who submit forms, staff who use the content management system.                                                                                                                                                                                                                          |
| <b>Personal data</b> | The host's server logs (IP address, time, requested URL, browser data). Data entered in forms (e.g. name, email address, phone number, message), if a system operated by the Processor forwards or stores it. Data from the website's measurement tools, if any. User accounts of the content management system. |
| <b>Operations</b>    | Storage, forwarding (email notification), backup, access needed for troubleshooting.                                                                                                                                                                                                                             |
| <b>Retention</b>     | Server logs according to the hosting provider's settings. Form data as set out in the Individual Agreement; failing that, until the Main Agreement ends.                                                                                                                                                         |
| <b>Location</b>      | Per website, as set out in the Individual Agreement. For websites hosted on Vercel, the Vercel row of Annex 3 applies.                                                                                                                                                                                           |

---

## Annex 2 – Technical and organisational measures

### TOM Security measures

- 1. Infrastructure.** The database runs in AWS's Ireland region (eu-west-1), operated by Supabase. The server side of the application runs in Vercel's Frankfurt region (fra1).
- 2. Encryption.** All connections are encrypted (HTTPS/TLS). The database is encrypted at rest by the provider.
- 3. Access.**
  - Only the server-side application can reach the database, using a key held in the hosting provider's encrypted environment variables. There is no direct database access from browsers.
  - Every record carries the practice identifier and every query filters on it, so each practice's data is kept separate.
  - The Customer's portal opens with a per-practice 192-bit random key or with an expiring login link sent by email.
  - Only the Processor can access the administration interface.
  - Provider accounts (hosting, database, code repository, email) are protected by two-factor authentication. Keys are rotated whenever compromise is suspected.
- 4. Data minimisation.** The filtering and redaction described in section 3.5, and the no-training setting. The chat sets no cookies; the browser keeps the conversation identifier only until the tab is closed.
- 5. Deletion.**
  - A daily automatic job deletes conversations older than 30 days.
  - Trial demos are deleted with all their data when they expire.
  - Permanently deleting a practice removes all of its data in a single transaction. The deletion is logged without personal data.

6.

**Abuse prevention.** Rate limits by pseudonymised IP, a daily message cap per practice and per-conversation limits. Bot protection, and embedding restricted to the practice’s own domain. Suspicious messages are checked by a filter.
7.

**Monitoring.** Automatic health checks every 5 minutes, with email alerts. Error logs contain no message content. Alerts flag unusual traffic, such as reaching 80% of the daily cap or a burst of rejected messages.
8.

**Model use.** Model calls go through Vercel AI Gateway, pinned to each model’s own provider and sent with the no-training setting. The gateway does not store request content.
9.

**Development.** Version-controlled code, with automated tests run before every release. No secret keys are stored in the code repository.
10.

**Organisation.**
  - Only the Processor, a sole proprietor, has access to the personal data. Any future staff or subcontractors will be bound to confidentiality in writing.
  - A written procedure governs breach handling (assessment, containment, notification within 48 hours, documentation) and data subject requests.
  - The measures and the sub-processors are reviewed annually.
  - Work devices use encrypted storage and a screen lock, and are kept up to date.

## Annex 3 – Sub-processors

### List Sub-processors engaged

#### Supabase

Supabase Pte. Ltd., 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513

|                  |                                                                                                           |
|------------------|-----------------------------------------------------------------------------------------------------------|
| TASK             | Database: conversations, callback requests, knowledge base, practice details, portal login                |
| DATA             | The data listed in Annex 1, section A                                                                     |
| LOCATION         | Ireland, EU (AWS eu-west-1)                                                                               |
| SAFEGUARD, NOTES | Supabase data processing terms. SCCs (Modules 2 and 3) for any access from outside the EU (e.g. support). |

#### Vercel

Vercel Inc., 440 N Barranca Ave #4133, Covina, CA 91723, USA

|                  |                                                                                                                                                          |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| TASK             | Running the application (chat server, portal), website hosting, relaying model calls (AI Gateway)                                                        |
| DATA             | Requests in transit. Application logs without message content. The gateway does not store request content, only metadata (model, token count, duration). |
| LOCATION         | Frankfurt, EU (fra1). Gateway traffic may pass through other Vercel regions.                                                                             |
| SAFEGUARD, NOTES | Certified under the EU–US Data Privacy Framework (DPF).                                                                                                  |

## Mistral AI

15 rue des Halles, 75001 Paris, France (RCS Paris 952 418 325); via Vercel AI Gateway

|                  |                                                                                                                                                                             |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TASK             | Language model: answer drafting, fact checking, search vectors, extraction of callback details                                                                              |
| DATA             | The non-health part of the question, the redacted conversation history, relevant knowledge-base excerpts                                                                    |
| LOCATION         | EU company. The provider does not commit to a processing location.                                                                                                          |
| SAFEGUARD, NOTES | Not used for training: the gateway routes with the no-training setting. May retain requests for up to 30 days for abuse monitoring. SCCs for any processing outside the EU. |

---

## OpenAI

OpenAI Ireland Ltd, 117-126 Sheriff Street Upper, Dublin 1, Ireland; via Vercel AI Gateway

|                  |                                                                                                        |
|------------------|--------------------------------------------------------------------------------------------------------|
| TASK             | Automated processing of the public website text (practice profile) and quality-assurance tests         |
| DATA             | Only public website text (which may include staff names) and test questions. Receives no patient data. |
| LOCATION         | USA as well                                                                                            |
| SAFEGUARD, NOTES | Not used for training. May retain requests for up to 30 days for abuse monitoring. SCCs.               |

---

## Resend

Plus Five Five, Inc., 2261 Market Street #5039, San Francisco, CA 94114, USA

|                  |                                                                               |
|------------------|-------------------------------------------------------------------------------|
| TASK             | Email delivery: callback notifications, login links, system notices           |
| DATA             | Callback request details (without health data), portal users' email addresses |
| LOCATION         | USA                                                                           |
| SAFEGUARD, NOTES | DPF-certified, SCCs. Stores email data in the USA, typically for 30 days.     |

---

## Cloudflare

Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94107, USA

|                  |                                                                                                    |
|------------------|----------------------------------------------------------------------------------------------------|
| TASK             | Bot protection (Turnstile): in the chat after many messages, and on the trial-demo form            |
| DATA             | IP address, browser characteristics (TLS fingerprint, User-Agent)                                  |
| LOCATION         | Global network                                                                                     |
| SAFEGUARD, NOTES | DPF-certified, SCCs. May also use these signals as an independent controller to improve Turnstile. |

---

## Rackhost

Rackhost Zrt., Tisza Lajos körút 41., 6722 Szeged, Hungary (Cg. 06-10-000489)

|                  |                                                                              |
|------------------|------------------------------------------------------------------------------|
| TASK             | Server (VPS): crawling the website for the knowledge base, health monitoring |
| DATA             | Public website content (which may include staff names), crawl logs           |
| LOCATION         | Hungary, EU                                                                  |
| SAFEGUARD, NOTES | Processing within the EU.                                                    |

---

## Google Workspace

Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland

|                  |                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------|
| TASK             | The Processor's email account (viktor@vmv.hu): correspondence with the Customer, forwarding data subject requests |
| DATA             | Data the Customer sends by email                                                                                  |
| LOCATION         | EU and USA                                                                                                        |
| SAFEGUARD, NOTES | SCCs; Google LLC is DPF-certified.                                                                                |

We update this list at least 15 days before any change and notify Customers by email (section 5 of the agreement). Sub-processors for the voice assistant will be published before that service launches.

## Annex 4 – Template text for the Controller's privacy notice

### Template Online assistant (chat)

The Controller may insert the following text into its privacy notice. The parts in square brackets must be completed.

#### Online assistant (chat) on our website

On our website, an assistant based on artificial intelligence (AI) answers questions about our practice's services, prices, opening hours and contact details. The assistant also records your callback or appointment request. It generates its answers from the content of our website. It does not give medical advice, and it can make mistakes; our staff provide the final information.

**Please do not share health data in the chat** (symptoms, complaints, medication, diagnoses, social security number). If you do, the system automatically redacts those sentences: it neither stores them nor passes them to the AI model that writes the answers. For any complaint, please call our practice.

**Controller:** [name, address and contact details of the practice].

#### Data processed:

- the messages you type into the chat and the assistant's replies;
- for callback requests: your name, phone number or email address, the requested service and time;
- technical data: a random session identifier, language, the title of the page you opened, and the time. In addition, an irreversible identifier derived from your IP address that changes daily, used to prevent abuse.

#### Purposes and legal bases:

- answering your questions: our legitimate interest in giving website visitors quick answers (Article 6(1)(f) GDPR);
- handling your callback or appointment request: steps taken at your request before entering into a contract (Article 6(1)(b) GDPR).

**Retention:** conversations are deleted automatically after 30 days, and callback requests after 180 days. [If our practice also records the request in its own systems, its own retention rule applies there: ...]

**Processor:** the assistant is operated by Vilbergsson Viktor E.V. (VMV; Patakpart u. 19/2., 2111 Szada, Hungary; viktor@vmv.hu). Its sub-processors (hosting, database, language model, email delivery, bot protection) are listed at [www.vmv.hu/adatbiztonsag#alfeldolgozok](http://www.vmv.hu/adatbiztonsag#alfeldolgozok). Conversations are stored in the European Union. Transfers to US-based providers rely on the EU-US Data Privacy Framework or on the European Commission's standard contractual clauses.

**Automated decision-making:** the assistant does not make any decision based solely on automated processing that produces legal effects concerning you or similarly significantly affects you (Article 22 GDPR).

**Cookies:** the chat uses no cookies. Your browser keeps the conversation identifier only until you close the tab (sessionStorage).

**Your rights:** [reference to the section of the privacy notice on data subject rights and remedies].

*This template agreement is effective from 6 October 2026. If the language versions differ, the Hungarian text prevails.*