CONTRATO DE ENCARGO DE TRATAMIENTO DE DATOS PERSONALES

(Versión AI – con la participación de proveedores de IA como subencargados del tratamiento)

celebrado de conformidad con el art. 28, apdo. 3 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, el «**RGPD**») (en adelante, el «**DPA**»)

entre:

Denominación social:	**[●]**
Domicilio social:	**[●]**
N.º de registro:	**[●]**
Inscrita:	en el Registro Mercantil **[●]**, sección: **[●]**, n.º **[●]**
Representada por:	[nombre y apellidos], [cargo]

(en adelante, el «**Responsable del tratamiento**»)

y

Denominación social:	**Nethemba s. r. o.**
Domicilio social:	Klemensova 2524/4, 811 09 Bratislava, República Eslovaca
N.º de registro (IČO):	36 777 234
Inscrita:	en el Registro Mercantil del Tribunal de Distrito de Bratislava I, sección: Sro, n.º 61232/B
Representada por:	Ing. Pavol Lupták, administrador
Correo electrónico:	info@nethemba.com

(en adelante, el «**Encargado del tratamiento**»)

(el Responsable y el Encargado, conjuntamente, las «**Partes**»)

1. Disposiciones introductorias

1.1 Las Partes han celebrado un contrato de prestación de servicios de seguridad, en virtud del cual el Encargado presta al Responsable servicios en el ámbito de la seguridad de las tecnologías de la información, en particular pruebas de penetración y auditorías de seguridad (en adelante, el «**Contrato Principal**» y los «**Servicios**»).

1.2 En el curso de la prestación de los Servicios, el Encargado puede tratar, por cuenta del Responsable, datos personales contenidos en los sistemas probados del Responsable o en la comunicación con ellos. El objeto de este DPA es regular los derechos y obligaciones mutuos de las Partes en relación con dicho tratamiento de conformidad con el art. 28 del RGPD.

1.3 Los términos «herramientas de IA» y «proveedores de IA» tienen el significado establecido en el artículo del Contrato Principal que regula el uso de herramientas de inteligencia artificial.

2. Objeto y duración del tratamiento

2.1 El Encargado se compromete a tratar los datos personales por cuenta del Responsable exclusivamente en el alcance y en las condiciones acordadas en este DPA y en el Contrato Principal. La descripción detallada del tratamiento (objeto, naturaleza, finalidad, categorías de interesados y categorías de datos personales) figura en el Anexo n.º 1.

2.2 Este DPA se celebra por la duración del Contrato Principal. Las obligaciones de las Partes que, por su naturaleza, deban subsistir tras la finalización del tratamiento (en particular la confidencialidad) subsistirán tras la terminación de este DPA.

3. Obligaciones del Encargado

El Encargado se compromete a:

(a) tratar los datos personales únicamente siguiendo instrucciones documentadas del Responsable, inclusive con respecto a las transferencias a terceros países, salvo que esté obligado a ello en virtud del Derecho de la UE o de un Estado miembro; el Contrato Principal, incluido su artículo sobre el uso de herramientas de IA, se considera asimismo una instrucción documentada;

(b) garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

(c) adoptar, teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, medidas técnicas y organizativas apropiadas conforme al art. 32 del RGPD; su descripción básica figura en el Anexo n.º 3;

(d) respetar las condiciones para recurrir a subencargados establecidas en el art. 4 de este DPA;

(e) teniendo en cuenta la naturaleza del tratamiento, asistir al Responsable, siempre que sea posible, mediante medidas técnicas y organizativas apropiadas, en el cumplimiento de su obligación de responder a las solicitudes de ejercicio de los derechos de los interesados (Capítulo III del RGPD);

(f) ayudar al Responsable a garantizar el cumplimiento de las obligaciones establecidas en los arts. 32 a 36 del RGPD, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el Encargado;

(g) notificar al Responsable las violaciones de la seguridad de los datos personales sin dilación indebida después de tener conocimiento de ellas y, en cualquier caso, en un plazo de 48 horas desde su detección;

(h) una vez finalizada la prestación de los Servicios, suprimir los datos personales (de conformidad con los plazos de supresión acordados en el Contrato Principal, en particular la supresión del informe final a los 60 días de su entrega y la supresión de los registros y datos relacionados conforme al período de archivo acordado) o devolverlos al Responsable, y suprimir las copias existentes, salvo que el Derecho de la UE o de un Estado miembro exija su conservación; las Partes reconocen que la supresión por parte de los proveedores de IA se rige por sus normas de retención conforme al art. 4.4 de este DPA;

(i) poner a disposición del Responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el art. 28 del RGPD y permitir y contribuir a las auditorías en las condiciones establecidas en el art. 6 de este DPA.

4. Subencargados del tratamiento

4.1 El Responsable otorga al Encargado una autorización general por escrito en el sentido del art. 28, apdo. 2 del RGPD para recurrir a subencargados. La lista de subencargados contratados en la fecha de celebración de este DPA, incluidos los proveedores de IA, constituye el Anexo n.º 2.

4.2 El Encargado informará al Responsable de cualquier cambio previsto en la incorporación o sustitución de subencargados con antelación, al menos 14 días antes de la incorporación, dando así al Responsable la oportunidad de oponerse a dichos cambios. Si el Responsable no formula objeción antes del inicio de la incorporación, el cambio se considerará aprobado. La información podrá facilitarse por correo electrónico o mediante la actualización de la lista pública en el sitio web del Encargado combinada con un aviso por correo electrónico.

4.3 Si el Responsable formula una objeción justificada a la incorporación de un subencargado que sea un proveedor de IA con arreglo al Contrato Principal, las Partes debatirán una solución alternativa; si no se llega a un acuerdo, cualquiera de las Partes podrá resolver el Contrato Principal en la parte afectada por la objeción, y el Responsable abonará el precio de los Servicios prestados hasta la resolución.

4.4 El Encargado impondrá a cada subencargado, mediante contrato, las mismas obligaciones de protección de datos que las estipuladas en este DPA. En el caso de los proveedores de IA, dichas obligaciones se rigen por sus acuerdos estándar de tratamiento de datos (Data Processing Agreement/Addendum) celebrados entre el Encargado y el proveedor de IA correspondiente; el Responsable reconoce que el Encargado no puede modificar individualmente las condiciones de tratamiento (incluidos los plazos de retención) de los proveedores de IA. Si un subencargado incumple sus obligaciones de protección de datos, el Encargado seguirá siendo plenamente responsable ante el Responsable del cumplimiento de las obligaciones de dicho subencargado, con sujeción a las limitaciones de responsabilidad acordadas en el Contrato Principal.

5. Transferencias a terceros países

5.1 Las Partes reconocen que los subencargados enumerados en el Anexo n.º 2 pueden tratar datos personales en servidores situados fuera de la UE/EEE, en particular en EE. UU. Toda transferencia de este tipo se realizará únicamente con garantías adecuadas conforme al Capítulo V del RGPD, en particular sobre la base de una decisión de adecuación (el EU-U.S. Data Privacy Framework, cuando la entidad correspondiente esté certificada) o de las cláusulas contractuales tipo adoptadas por la Comisión Europea.

6. Auditoría

6.1 El Responsable tiene derecho a auditar el cumplimiento de este DPA por parte del Encargado como máximo una vez cada 12 meses, a su propia costa, previa notificación por escrito con al menos 30 días de antelación, en horario laboral habitual y de forma que no interfiera de manera desproporcionada en las operaciones del Encargado. Las personas que realicen la auditoría deberán estar sujetas a confidencialidad.

6.2 Con respecto a los subencargados (incluidos los proveedores de IA), la auditoría se realizará mediante certificaciones, informes de auditoría y demás documentación que dichos subencargados pongan a disposición (p. ej., certificaciones ISO 27001, informes SOC 2). El Responsable reconoce que el Encargado no tiene derecho a realizar una auditoría física en las instalaciones de los proveedores de IA.

7. Responsabilidad

7.1 La responsabilidad de las Partes en virtud de este DPA se rige por las disposiciones sobre responsabilidad y limitación de daños acordadas en el Contrato Principal, incluida la exclusión de la responsabilidad del Encargado por actos u omisiones de los proveedores de IA en el alcance acordado en el Contrato Principal. Lo anterior se entiende sin perjuicio de los derechos de los interesados y de la responsabilidad en virtud del art. 82 del RGPD.

8. Disposiciones finales

8.1 Este DPA entra en vigor en la fecha de su firma por ambas Partes. En caso de conflicto entre este DPA y el Contrato Principal, prevalecerá este DPA en materia de protección de datos personales.

8.2 Este DPA se rige por el Derecho de la República Eslovaca y por el RGPD. Las modificaciones solo podrán realizarse mediante una adenda por escrito.

8.3 Forman parte integrante de este DPA: el Anexo n.º 1 (Descripción del tratamiento), el Anexo n.º 2 (Lista de subencargados) y el Anexo n.º 3 (Medidas técnicas y organizativas).

En [●], a [●]	**En Bratislava, a ……**
Responsable del tratamiento	**Encargado del tratamiento**
Por: **[●]**	Por: **Nethemba s. r. o.**
Nombre: **[●]**	Nombre: Ing. Pavol Lupták
Cargo: **[●]**	Cargo: administrador

_____ _____

Anexo n.º 1 – Descripción del tratamiento

Objeto del tratamiento	Datos personales contenidos en los sistemas probados del Responsable, en la comunicación con ellos o en los materiales facilitados por el Responsable para la prestación de los Servicios
Duración del tratamiento	Durante la prestación de los Servicios; supresión conforme a los plazos acordados en el Contrato Principal (informe final: 60 días desde la entrega; registros y datos relacionados: conforme al período de archivo acordado, máx. 24 meses)
Naturaleza del tratamiento	Recogida, consulta, análisis, conservación temporal y supresión de datos en el curso de pruebas de penetración y auditorías de seguridad, incluido el tratamiento mediante herramientas de IA conforme al Contrato Principal
Finalidad del tratamiento	Evaluación de la seguridad de los sistemas probados, identificación de vulnerabilidades y elaboración del informe final
Categorías de interesados	Empleados, clientes, proveedores y usuarios de los sistemas del Responsable; otras personas cuyos datos se encuentren en los sistemas probados
Categorías de datos personales	Datos de identificación y contacto, identificadores de acceso y de red (correo electrónico, dirección IP, cookies), contenido de las comunicaciones y cualesquiera otros datos personales ordinarios contenidos en los sistemas probados; categorías especiales de datos únicamente en la medida en que se encuentren en los sistemas probados, sin ser objetivo del tratamiento

Anexo n.º 2 – Lista de subencargados del tratamiento

Proveedores de IA (conforme al artículo del Contrato Principal sobre el uso de herramientas de IA):

Entidad	Sede	Servicio	Garantías de transferencia
Anthropic, PBC (incl. Anthropic Ireland, Limited)	EE. UU. / Irlanda	Claude, Claude Code	EU-U.S. DPF / SCC
OpenAI, Inc. / OpenAI, L.L.C. (incl. OpenAI Ireland Ltd)	EE. UU. / Irlanda	ChatGPT, Codex, GPT API	EU-U.S. DPF / SCC
Google LLC / Google Ireland Limited	EE. UU. / Irlanda	Gemini, Vertex AI	EU-U.S. DPF / SCC
Microsoft Corporation / Microsoft Ireland Operations Limited	EE. UU. / Irlanda	Azure OpenAI, GitHub Copilot	EU-U.S. DPF / SCC
xAI Corp.	EE. UU.	Grok	SCC
Mistral AI SAS	Francia	Le Chat, La Plateforme	– (UE)
Amazon Web Services, Inc.	EE. UU.	infraestructura en la nube	EU-U.S. DPF / SCC

Otros subencargados: [●] *(p. ej., subcontratistas – especialistas conforme al Contrato Principal; completar o tachar)*

Anexo n.º 3 – Medidas técnicas y organizativas

- El acceso a los datos personales está limitado a personas autorizadas sujetas a confidencialidad, en la medida necesaria para la prestación de los Servicios (need-to-know).
- Cifrado de los datos en tránsito (TLS, SSH, VPN); comunicación por correo electrónico cifrada y firmada digitalmente (PGP o S/MIME), cuando el Responsable lo permita.
- Cifrado de disco completo de las estaciones de trabajo (full-disk encryption); autenticación multifactor para el acceso a los sistemas del Encargado.
- Minimización: los datos se tratan únicamente en la medida necesaria para la evaluación de seguridad; las credenciales (contraseñas, claves API, tokens) no se revelan a las herramientas de IA en forma utilizable (best effort conforme al Contrato Principal).
- Las herramientas de IA se utilizan en versiones de pago/empresariales/API con prohibición contractual de entrenamiento con entradas y salidas y, cuando estén disponibles, modos de retención cero de datos (zero data retention).
- Supresión: informe final en un plazo de 60 días desde la entrega; registros y datos relacionados conforme al período de archivo acordado; borrado seguro de los soportes.
- Gestión de incidentes: procedimiento interno de detección, escalado y notificación de violaciones de la seguridad de los datos personales (notificación al Responsable en un plazo de 48 horas desde la detección).