Data processing agreement (DPA) based on the EU standard contractual clauses

between

ThinkOwl Europe GmbH

Carl-Benz-Straße 10-12
D-56218 Mülheim-Kärlich

hereinafter referred to as „ThinkOwl“

and

_____

_____
_____

hereinafter referred to as „**Customer**“

Preamble
This Order Processing ("**DPA**") is part of the Master Subscription Agreement ("**MSA**") between ThinkOwl Europe GmbH ("**Processor**") and the Customer ("**Controller**"). This DPA has been drawn up on the basis of the EU Standard Contractual Clauses from 4 June 2021 ("**EU SCC**").

1 Components of the contract

Parts of the contract are this **contract text** and the **EU standard contractual clauses** consisting of:

- Section I – General
- Section II – Obligations of the Parties
- Section III – Final Provisions
  as well as
- Annex I – List of Parties
- Annex II – Description of the processing
- Annex III – Technical and organisational measures including technical and organisational measures to ensure the security of the data
- Annex IV – List of sub-processors

2 Supplements to the standard contractual clauses

2.1 Evidence and costs for tests

Pursuant to clause 7.6 of the Standard Contractual Clauses, the Processor shall provide evidence of compliance with the Standard Contractual Clauses. ThinkOwl is entitled to demand remuneration for this. The remuneration shall be agreed in advance. ThinkOwl shall submit an offer to the customer prior to an audit. The rates of remuneration may not exceed the rates of remuneration customary for IT services, in any case the rate of remuneration pursuant to Section 1.13 of the MSA. External costs of ThinkOwl such as audit costs at service providers shall be fully borne by the Customer.

The following evidence of data protection audit rights is provided free of charge:

- Compliance with approved rules of conduct pursuant to Article 40 of the General Data Protection Regulation.
- Certification in accordance with an approved certification procedure pursuant to Article 42 of the General Data Protection Regulation
- current certificates, reports or report extracts from independent bodies (e.g. auditors, auditing, data protection officers, IT security department, data protection auditors, quality auditors);
- suitable certifications by IT security or data protection auditors.

Mülheim-Kärlich, 1 August 2025

ThinkOwl

Customer

Standard contractual clauses

Section I - General

Clause 1

Purpose and scope

a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation.

b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

c) These Clauses apply to the processing of personal data as specified in Annex II.

d) Annexes I to IV are an integral part of the Clauses.

e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 – Optional

Docking clause

a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1 Instructions

a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4 Security of processing

a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5 Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7 Use of sub-processors

a) GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 4 weeks in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8 International transfers

a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

4) the obligations in Article 32 of Regulation (EU) 2016/679

d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

2) the likely consequences of the personal data breach;

3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay. The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I – List of Parties

Controller(s): *[Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]*

1. Name:

   Adress:

   Contact person's name, position and contact details:

   Signature and accession date:

2. Name:

   Adress:

   Contact person's name, position and contact details:

   Signature and accession date:

Processor(s): [*Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer]*

1. Name: ThinkOwl Europe GmbH

   Adress: Carl-Benz-Str. 10-12, D-56218 Mülheim-Kärlich

   Contact person's name, position and contact details: Rolf Esau, CEO, rolf.esau@thinkowl.com

   Signature and accession date: 1 August 2025

2. Name: ThinkOwl Europe GmbH

   Adress: Carl-Benz-Str. 10-12, D-56218 Mülheim-Kärlich

   Contact person's name, position and contact details: Peter Macherey, Data Protection Officer, privacy@thinkowl.com

   Signature and accession date: 1 August 2025

ANNEX II – Description of the processing

Categories of data subjects whose personal data is processed

All types of customers, consumers and business partners of the Company who request a service from the Company.

Categories of personal data processed

Email addresses and other contact information may be stored as personal data in the Service. The Company is obliged to store or record only the personal data in the Service that is required in the normal course of business and use of the Service.

Nature of the processing and Informatiokn about processing sensitive data

As part of a cloud application, the Service processes emails, documents, voice recordings, text messages, any kind of attachments, chats, names and other Service data. In this context, personal data may be stored by the Company in the Service. The Company itself has control over what personal data is stored in the Service. The exact data that the Company wishes to store in the Service is not known to ThinkOwl and is also stored in encrypted form. ThinkOwl has no information about:

a) what kind of service data is stored in the service
b) what kind of personal data the service data contains
c) whether sensitive data are processed

Duration of the processing

The duration of the processing of the company's personal data corresponds to the term of the main contract.

ANNEX III – Technical and organisational measures including technical and organisational measures to ensure the security of the data

ThinkOwl shall take technical and organisational measures to adequately secure the Client's data against misuse and loss that comply with the legal requirements for data protection and data security. These are measures of data security and to ensure a level of protection appropriate to the risk in terms of confidentiality, integrity, availability and resilience of the systems. In this context, the state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) GDPR shall be taken into account. In particular, ThinkOwl designs its internal organisation to meet the specific requirements of data protection. These are described in more detail below.
Essential preliminary services are provided by data center operators (subcontractors). For this purpose, the aforementioned providers have each contractually assured ThinkOwl that they will maintain appropriate technical and organisational data protection measures for the duration of the contract.
The measures described below are not disclosed in detail, in particular for security reasons, i.e. to minimize security risks with regard to access to company data and the corresponding protection of company and business secrets, but serve only as a basic requirement to meet the requirements of Article 32 of the GDPR.

1 Confidentiality (Art. 32 para. 1 lit. b GDPR)

a) Access control

Unauthorized access must be prevented, whereby the term is to be understood spatially. Technical or organizational measures for access control, in particular also for the legitimation of authorized persons:

Technical measures	**Organisational measures**
Alarm system	Key management / documentation Key allocation
Biometric access control to the building, office floors and separately protected office rooms	Logging of visitors
Protection of the building shafts	Protection of the building shafts
Bell system with camera	Care in the selection of service providers and partners (Supplier Security Directive)
Safety glazing	
Secured server room with reinforced door and separate biometric access authorization or locking system	
Motion detector	

Independent access to the building is only possible (even outside normal business hours, but not during the nightly lockdown period) with biometric deactivation of the alarm system and access (fingerprint) with appropriate authorization.

Additional fingerprint scanners are available within the individual security areas, depending on the security level.

During normal business hours, visitors are recorded by the visitor in visitor lists and a corresponding confidentiality agreement is accepted in writing by the visitor's signature.

b) Access control

The intrusion of unauthorized persons into the data processing systems must be prevented.

Technical measures	**Organisational measures**
Login with username + password	User profile creation and management
Anti-Virus Software Server	Creation and management of user permissions
Anti-virus software clients	User Passwort Management
Firewall	Secure Password Policy
Use VPN for remote access	Clean Desk / Clear Screen Policy
Monitoring for critical IT systems	Policy "Use of e-mail and Internet
	Information Security Policy
	Privacy Policy

Access to client systems in the network is only possible via password-protected network authentication. Direct access from the outside (i.e. from outside the network) is only possible via secured and encrypted connections and a computer/laptop (or similar hardware) provided by the company. Firewalls and proxy servers are used for secure access to third-party systems.

c) Access Control

Unauthorized activities in DP systems outside of granted authorizations must be prevented.

Technical measures	**Organisational measures**
User ID + Password	Authorization concepts
Logging of accesses to applications, specifically when entering, changing and deleting data	Management of user rights by administrators
File shredder (at least level 3, cross cut)	Regular review of access rights

External document destruction	Employee onboarding/offboarding processes
	Access Control Directive
	Local Administrative Rights Directive

It is based on an authorization concept with a corresponding definition of user profiles and roles with regard to all IT systems. Authorizations are assigned according to the "least-privileged" principle. This means that users only receive the authorizations in the respective IT system that they need to implement their tasks. Access is always via a user account with user ID and password. Access is logged via a log entry on the relevant servers.

d) Separation control

Data collected for different purposes shall also be processed separately.

Technical measures	**Organisational measures**
Multi-client capability of relevant applications	Separation of functions
Separate folder structures (order processing)	Control via authorization concept
	Setting database rights

All employees are instructed and trained to collect, process or use personal data only within the scope of service provision and in compliance with the purpose limitation.

Integrity (Art. 32 para. 1 lit. b GDPR)

a) Transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and determine to which entities personal data is intended to be transmitted by data transmission equipment.

Technical measures	Organisational measures
Tunnel connection (VPN)	Information Security Policy
Hybrid encryption protocol TLS	Sealed containers
Firewall	
Logging of accesses and retrievals	

Personal data from IT systems is not passed on as a matter of principle. If a transfer is permitted in accordance with a corresponding legal or contractual basis, it may be made to affiliated companies, customers, partners or suppliers. The transfer of data must be secured by concluding confidentiality agreements and order processing agreements with the respective third party.

b) Input Control

Traceability or documentation of data management and maintenance must be ensured.

Technical measures	Organisational measures
Technical logging of data entry, modification and deletion	Traceability of input, modification and deletion of data through individual user names (not user groups)
	Assignment of rights to enter, change and delete data on the basis of an authorization concept

Availability and resilience (Art. 32 para. 1 lit. b GDPR)

a) Availability control

The data must be protected against accidental destruction or loss.

Technical Measures	Organisational measures
Fire and smoke detection systems	Emergency plan
Fire extinguisher	Backup procedure
Server room air conditioned	Recovery procedure
USV	
Firewall and antivirus programs	

Regular backups	

Procedures for regular review, assessment and evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

The following measures ensure that compliance with the requirements of the GDPR regarding the protection of personal data is continuously reviewed, assessed and evaluated.

a) Data protection management

Technical measures	**Organisational measures**
Software solutions for data protection management in use	Data Protection Officer
Central documentation of all procedures and regulations on data protection with access for employees according to need / authorization	Regular training of the Data Protection Officer
	Training of employees and commitment to confidentiality/data secrecy
	Regular sensitization of employees
	Carrying out the data protection impact assessment as required
	Information obligations according to Art. 13 and 14 GDPR are complied with.
	Employees are obligated to comply with the data protection requirements according to GDPR

b) Incident response management

Technical measures	**Organisational measures**

Use of firewall and regular updating	Documented process for detecting and reporting security incidents/data breaches.
Use of spam filters and regular updating	Involvement of the data protection officer in security incidents and data breaches
Use of virus scanners and regular updating	Documentation of security incidents and data mishaps via ticket system

c) Data protection-friendly default settings (Art. 25 (2) GDPR)

Technical measures	**Organisational measures**
Only the personal data required for the respective purpose is collected	
Simple exercise of the right of withdrawal of the data subject by technical measures	

d) Order control

No commissioned data processing within the meaning of Art. 28 GDPR without corresponding instructions from the client, e.g.: Clear contract design, formalized order management, strict selection of the service provider, obligation to convince in advance, follow-up checks.

Technical measures	**Organisational measures**
	Supplier Security Directive
	Prior verification of the safety measures taken by the contractor and their documentation
	Careful selection of the contractor, especially with regard to data protection and data security
	Conclusion of necessary agreements on commissioned

	processing or EU standard contractual clauses
	Obligation of the contractor's employees to maintain data secrecy
	Obligation to appoint a data protection officer by the contractor in the event of an appointment obligation
	Regulation on the use of further subcontractors
	Ensuring the destruction or return of data after order completion

ANNEX IV – List of sub-processors

Sub-processor	Purpose	Data storage
Oracle Deutschland B.V. & Co. KG Riesstrasse 25, 80992 München Germany	Oracle Cloud infrastructure for ThinkOwl Europe application operations	DE
ITyX Labs GmbH Carl-Benz-Straße 10-12, 56218 Mülheim-Kärlich Germany	Software Support	DE
fileee GmbH Windthorstraße 68, 48143 Münster Germany	Possibility for ThinkOwl users to use CONVERSATIONS	DE
Amazon Web Services Inc. 38 avenue John F. Kennedy, L-1855 Luxemburg	Primary cloud infrastructure provider for ThinkOwl Europe data storage, where all content of processes (e.g. email content including attachments) is stored. Storage location for encrypted backups.	DE
Amazon Web Services Inc. 38 avenue John F. Kennedy, L-1855 Luxemburg	AWS SES (Simple Email Service): Temporary storage for receiving and sending emails when using a ThinkOwl email address until the emails are retrieved.	EU

OpenAI Ireland Limited The Liffey Trust Centre 117-126 Sheriff Street Uppe Dublin 1 D01 YC43 Ireland	As an option or even as default for many of the AI features, such as conversation bot, summary, translation, TTS, STT, etc.)	EU
Bird Trompenburgstraat 2c, Amsterdam, Netherlands	The ability for ThinkOwl users to use SMS Service	EU
OwlSpot Carl-Benz-Straße 10-12, 56218 Mülheim-Kärlich, Germany	App-Store + Integrations	DE
Microsoft Ireland Operations ltd. One Microsoft Place South County Business Park Leopardstown Dublin 18 D18P521 Ireland	Microsoft Voice API with LLM Provision of speech processing services (speech-to-speech, speech-to-text, text-to-speech)	EU
Google Cloud EMEA ltd. 70 Sir John Rogerson´s Quay Dublin 2 Ireland	Gemini Flash and Pro LLM for processing speech, text, images and videos in the context of generative AI applications	EU