

Data Processing Agreement

This data processing agreement with its appendices ("**DPA**") is a part of the service agreement and its appendices (including GTCs) (the "**Agreement**") and governs the provision of the software platform, its modules, and the documentation by Supplier (collectively the "**Deliverables**") provided by the entity stated on the service agreement (the "**Supplier**" or "**Processor**") to its Customer (the "**Customer**" or "**Controller**").

1 INTRODUCTION

The Customer and its Users' use of the Deliverables means that the Processor will Process Personal Data, including Customer Content, on behalf of the Controller.

2 SCOPE OF THE AGREEMENT AND EXCEPTIONS

The DPA sets out the framework for the Processor's Processing of Personal Data on behalf of the Controller and regulates the Processing of Personal Data included in Customer Content, except for the Processing described in the last paragraph of this section 2.

The purpose of this DPA is to:

- a) regulate the parties' rights and obligations when Processing Personal Data,
- b) ensure that the requirements of the Personal Data Legislation and GDPR are complied with in the implementation of the Agreement, and
- c) ensure that Personal Data is not Processed unlawfully or disclosed to unauthorized persons.

In the event of a conflict between the provisions of this DPA and other agreements between the Parties, including the Agreement, the provisions of the DPA shall prevail.

The DPA does not regulate Supplier's Processing of Personal Data when Supplier is the data controller. This applies, for example, to subscriber information, service history, payment information, communication content, and certain other information. The same applies to Supplier's storage and processing of feedback that Users provide to the Customer (e.g., through the feedback function) in order to improve the quality of the Deliverables. This includes diagnostic, technical, or usage data strictly necessary for maintaining and improving the Deliverables, as further described in the Supplier's Privacy Policy. In these circumstances, Supplier determines the purpose of the Processing of the Personal Data, and the Processing is regulated by Supplier's Privacy Policy.

3 DEFINITIONS

Capitalized terms in the DPA shall have the same meaning as in the Agreement. The following definitions apply to this DPA:

"Personal Data" means any type of data or information that is considered personal data under Data Protection Legislation and the GDPR and contained in Customer Content.

"Processing" (of Personal Data) means any use of Personal Data, such as collection, storage, organization, alteration or adaptation, disclosure, and/or transfer.

"Customer Content" as defined in the Agreement.

"GDPR" means EU Regulation 2016/679 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.

"Data Protection Legislation" refers to any laws and regulations related to data privacy in the country where the Supplier and Customer maintain their principal place of business, including GDPR.

"Law" means any other applicable law to which the parties are subject.

"Sub-processor" means other data processors that the Processor uses to process the Personal Data.

"Data Subject" means any identified or identifiable person to whom the Personal Data relates.

4 GENERAL

The parties shall Process Personal Data in accordance with Data Protection Legislation, GDPR, and this DPA.

The Processor shall only collect, register, compile, store, and otherwise Process Personal Data to the extent necessary to fulfill the Agreement and the DPA.

The Controller must ensure a lawful basis for Processing the Personal Data.

The Processor has no control over whether Personal Data is uploaded by the Users or the purpose of Processing such Personal Data. The Processor does not Process any Personal Data unless the Users decide to upload it and have determined the purpose of the Processing. The Processor is under no obligation to monitor Customer Content or verify the lawfulness of Personal Data submitted by the Controller or its Users.

If the Users decide to upload Personal Data, it may contain sensitive data, special category data, and other professional information.

The Controller determines whether the Customer Content includes Personal Data, the purpose of Processing the Personal Data, and how the Personal Data is processed when using the Deliverables.

The Controller warrants that any Personal Data uploaded, transmitted or otherwise Processed through the Deliverables by the Controller or its Users has been collected and is Processed in compliance with Data Protection Legislation and the GDPR.

The Controller shall ensure that it has obtained all necessary consents, authorizations, or other valid legal bases from the relevant Data Subjects for the Processing of their Personal Data through the Deliverables, including any sensitive or special category data, before such Personal Data is uploaded or otherwise made available to the Processor.

The Controller further warrants that the Processing of such Personal Data by the Processor in accordance with this DPA does not violate any Data Protection Legislation, the GDPR, or any rights of the relevant Data Subjects.

The Controller is solely responsible for determining the appropriateness and lawfulness of its use of the Deliverables, including any AI-based functionalities, and for ensuring that such use complies with applicable Law, including GDPR.

The Parties acknowledge that the Processor acts solely as a processor and does not determine the purposes or means of Processing. Nothing in this DPA shall be construed as creating joint controllership under GDPR Article 26.

Customer Content, including Personal Data, will not be used to train or improve underlying machine learning models.

5 THE CONTROLLER'S AUTHORITY TO INSTRUCT

The Processor shall Process Personal Data in accordance with documented instructions from the Controller. The Controller's instructions to the Processor are set out in the Agreement and the DPA.

The Processor may also Process Personal Data if this is required by applicable laws. In such case, the Processor shall notify the Controller of the legal obligation prior to the Processing, unless the relevant Law prohibits the provision of such information for reasons of public interest.

The Controller may give subsequent instructions to the Processor for as long as the Processor Processes Personal Data on behalf of the Controller. Such subsequent instructions shall be given to the Processor in writing and must be documented.

The Processor shall immediately notify the Controller if the Processor believes that instructions or requirements from the Controller are in breach of Data Protection Legislation or GDPR.

If the Controller issues instructions that result in material additional costs to the Processor, the parties shall, in good faith, agree on reasonable compensation.

Any instructions issued by the Controller shall be reasonable, justified, and proportionate, and shall relate solely to the Processing of Personal Data under this DPA and the Agreement. The Processor shall not be required to act on instructions that are technically infeasible, unlawful, or materially inconsistent with the Deliverables or the Processor's technical capabilities. The Processor may notify the Controller if an instruction cannot be carried out, and the parties shall cooperate in good faith to find a practical solution.

The Processor is not obligated to comply with any instruction that would (i) require a fundamental change to the architecture of the Deliverables, (ii) undermine security, or (iii) impose disproportionate technical or financial burden compared to the value of the Agreement.

6 THE PROCESSOR'S DUTY TO ASSIST THE CONTROLLER

Considering the nature of the Processing and the information available to the Processor, the Processor shall, to the extent reasonably possible and taking into account the nature of the Processing, assist the Controller in ensuring compliance with the Controller's obligations under GDPR Articles 32 - 36. This includes an obligation for the Processor to assist in performing risk assessments and conducting prior consultations. The Processor may charge reasonable costs for assistance not expressly included in the Deliverables.

7 SECURITY MEASURES

The Processor shall comply with the information security requirements set out in the Data Protection Legislation and the GDPR, including implementing and maintaining appropriate technical and organizational security measures to achieve a level of security appropriate to the risk, in line with GDPR Article 32.

The technical and organizational measures to be implemented are described in Appendix A to the DPA.

The Processor shall also assist the Controller in ensuring compliance with the Controller's obligations regarding adequate information security pursuant to GDPR Article 32.

The Processor may update or modify the technical and organizational measures in Appendix A, provided that such updates do not reduce the level of security.

8 THE PROCESSOR'S USE OF SUB-PROCESSORS

If the Processor engages a Sub-Processor to carry out specific processing activities on behalf of the Controller, the Sub-Processor shall be subject to the same obligations as set out in this DPA and to the data protection requirements in accordance with relevant legislation.

The Sub-Processors used by the Processor in connection with the Agreement are set out in Appendix B to the DPA. The Controller accepts that the Processor uses these Sub-Processors.

The Processor has entered into separate data processing agreements with the Sub-Processors.

If the Processor wishes to use Sub-Processors other than those listed in Appendix B, the Processor must notify the Controller in advance. If the Controller reasonably objects to the use of a new Sub-Processor based on fair, justified, and reasonable data protection grounds, they shall inform the Processor without undue delay. If the Controller does not object within fourteen (14) days of receiving the notice, the Sub-Processor will be considered approved. If the Deliverables cannot be provided without using the relevant Sub-Processor, the Processor's obligation to deliver the Deliverables is suspended.

If the Sub-Processor fails to fulfill its data protection obligations, the Processor shall remain liable to the Controller for the actions or omissions of the Sub-Processor.

9 THIRD COUNTRY TRANSFERS

The Processor may transfer the Personal Data processed by the Processor on behalf of the Controller only to the countries where the Processor and Sub-Processors operate. These countries are listed in Appendix B.

The Controller is aware of this and accepts this transfer for as long as necessary to carry out the agreed Deliverables.

Processor shall not transfer the Personal Data to a country outside the EU/EEA without the prior written consent of the Controller.

If the Controller agrees to such a transfer of Personal Data to a country outside the EU/EEA, the Processor shall ensure that the transfer takes place in accordance with the rules in Chapter V of the GDPR.

To the extent that agreed Processing involves a transfer of Personal Data to a third country outside the EU/EEA for which no adequacy decision exists, and where such transfer requires appropriate safeguards under GDPR Article 46, the Parties agree that the applicable EU Commission Standard Contractual Clauses ("SCCs") shall automatically apply and are hereby incorporated by reference without the need for further action.

The SCCs shall apply in the unmodified form published by the European Commission and shall take precedence over any conflicting provisions of this DPA or the Agreement. The Controller authorizes the Processor to enter into the SCCs, including Module Two (Controller → Processor) and Module Three (Processor → Sub-Processor), on behalf of the Controller to the extent required to legitimize such transfers.

The Controller agrees that the Processor may rely on the SCCs concluded between the Processor and a Sub-Processor as a sufficient safeguard for onward transfers. The Controller further agrees that it shall not require the Processor to amend, supplement, or negotiate alternative terms to the SCCs.

10 HANDLING OF DATA SUBJECTS RIGHTS

The Controller shall be the point of contact for the Data Subjects and provide necessary information about the Processing.

The Controller is responsible for handling the Data Subjects' requests for access, rectification, erasure, restriction, data portability, etc., and ensuring such requests are met.

The Processor shall, taking into account the nature of the Processing and to the extent possible using appropriate technical and organizational measures, assist the Controller in fulfilling the Controller's obligation to respond to requests made by Data Subjects in order to exercise their rights set out in Chapter III of the GDPR.

If the Processor receives a request from the Data Subject, the Processor shall notify the Controller as soon as possible.

11 NON-CONFORMITY MANAGEMENT AND NOTIFICATION

Any unauthorized use of information systems contrary to the established procedures of the Processor, the instructions of the Controller, Data Protection Legislation, and any other security breach shall be treated as an incident.

The parties shall establish and maintain procedures and systematic measures for incident resolution, including steps to rectify the situation, eliminate the root cause of the incident, and prevent future occurrences.

Upon becoming aware of an incident, the Processor shall inform the Controller of any security breaches without undue delay and no later than within 36 hours and shall immediately take all necessary and appropriate measures to rectify the situation.

Such notification does not constitute an admission of fault or liability and is provided solely to enable the Controller to comply with its own legal obligations.

The Controller is responsible for reporting incidents to the Data Protection Authority and the Data Subjects in accordance with GDPR Articles 33 and 34. If necessary, the Data Processor shall assist the Data Controller in ensuring compliance with GDPR Articles 33 and 34.

12 AUDIT AND INSPECTION

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the Processor's obligations under the Data Protection Legislation, the GDPR, and this DPA.

The Processor shall enable and contribute to audits, including inspections conducted by the Controller or another inspector authorized by the Controller, of the Processor's compliance with the GDPR, the Data Protection Legislation, and this DPA. The Controller has the right to carry out such audits at its own cost, a maximum of once a year, with four weeks' prior written notice.

13 CONFIDENTIALITY AND NON-DISCLOSURE

The Processor has a duty of confidentiality regarding the Personal Data and documentation to which the Processor gains access through the DPA. The duty of confidentiality also applies after the termination of the DPA.

The Processor shall not disclose or give access to the Personal Data to anyone other than its employees, Sub-Processors, or employees of the Controller unless this has been agreed in writing with the Controller or is required by law, regulation, or a public authority's decision or as required for legal or audit purposes under a duty of confidentiality.

The Processor shall ensure that persons authorized to Process the Personal Data have undertaken to Process the data confidentially in the form of a confidentiality agreement or are subject to an appropriate statutory duty of confidentiality.

Where Customer Content includes information subject to legal professional privilege, the Processor shall treat such information as strictly confidential. The Processor does not waive, challenge or assume responsibility for maintaining legal professional privilege, which remains the sole responsibility of the Controller.

The Processor does not monitor, review, verify, or assess the legality, accuracy, or sensitivity of Customer Content, and is under no obligation to detect confidential, privileged, sensitive, or unlawful information uploaded by Users.

Access to Customer Content is limited to personnel with a strict need-to-know for the purpose of providing the Deliverables, subject to confidentiality obligations and role-based access controls.

14 DURATION OF THE AGREEMENT

The agreement applies for as long as the Processor Processes Personal Data on behalf of the Controller.

15 TERMINATION

When the Agreement is terminated, the Data Processor shall delete all Personal Data and Customer Content covered by the DPA and the GTC.

The parties agree in more detail on how such deletion and/or destruction shall take place and how the Data Processor shall document that deletion and/or destruction has been carried out in accordance with the agreement within a reasonable time after the Agreement terminates.

Exceptions apply if the Data Protection Legislation, GDPR, or law requires the Personal Data to be stored by the Data Processor.

Unless otherwise agreed, the Processor shall delete Personal Data and Customer Content within 60 days after termination.

16 GOVERNING LAW AND DISPUTES

The DPA shall be governed by and construed in accordance with the governing law and dispute-resolution provisions of the Agreement.

17 AGREEMENT, DPA AND APPENDIXES

This DPA (including the Appendices) forms an integral part of the Agreement and must be read in conjunction therewith. The Parties agree that the limitation of liability, exclusions, and disclaimers set out in the Agreement apply equally to this DPA. Nothing in this DPA shall increase or expand either Party's liability beyond the limits agreed in the Agreement.

Appendix A Technical and organizational measures for information security

Appendix B Overview of the Processor's Sub-Processors

Appendix A Technical and Organizational Security Measures

In the legal sector, information security and compliance are paramount. The AI platform (the "**Platform**"), which forms a part of Deliverables, offers robust and secure technology that aligns with Law, Data Protection Legislation, and GDPR.

1 ENTERPRISE-GRADE SECURITY MEASURES

The Platform uses encrypted communication and secure data storage solutions, ensuring that all information processed remains confidential. All data stored is encrypted using industry-standard encryption algorithms and best practices, with enforced use of secure, encrypted connections for all data transmission between the Users and the Platform.

The Platform is deployed on Microsoft Azure ("**Azure**"), and the Customers can be confident that their sensitive information and Personal Data are protected. The Processor is ISO/IEC 27001 certified, and updated security information is set out in our Trust Center at trust.sagalegal.io.

2 DATAFLOW AND ARCHITECTURE

The Platform is deployed in the Supplier's secure and monitored Azure tenant. Azure is widely recognized as one of the most secure cloud platforms available, and most organizations trust Microsoft as a provider for various services, including Teams, SharePoint, OneDrive, and Outlook Online. Azure is certified with important industry-leading security certifications, including:

- ✓ ISO/IEC 27001 – Internationally recognized standard for managing information security.
- ✓ SOC 1, SOC 2, and SOC 3 – Independent audit reports that cover Azure's internal controls over financial reporting, security, availability, processing integrity, confidentiality, and privacy.
- ✓ GDPR Compliance – Ensures Azure adheres to the European Union's General Data Protection Regulation for Customer data protection.

These certifications demonstrate Azure's commitment to stringent security standards and regulatory compliance.

Each Customer is provided with a dedicated database within the Supplier's private Azure tenant, where chat histories and chat files are secured. This ensures complete isolation of data, enhancing security and privacy.

For advanced functionality, such as transforming textual data into vector databases, we leverage a private Datastax or Weaviate Microsoft Azure tenant. The data flow between tenants is secured via a private network, configured and maintained by Microsoft, Datastax, or Weaviate, and the Microsoft Cloud Expert vendor Sirrus. The private network ensures that the data never leaves the Azure network.

The core of the Platform is to provide Customers with best-in-class Large Language Models (LLMs) and other AI tools. The Customer Content processed by these models will

not be sent to the LLM vendor's databases (such as OpenAI or Anthropic) for storage and training.

All Customer Content is Processed within the Supplier's secure Azure tenant and Microsoft Service Boundary utilizing Azure services. This architecture ensures that the Customer Content remains within the same regional Azure data center in the EU/EEA (standard is set to The Netherlands), or other countries where the platform is deployed, e.g., Switzerland.

The Platform supports an LLM-agnostic approach, which implies that the functionality is not locked into any specific LLM vendor. Customers will get access to additional LLMs like Claude or Gemini upon request. If this should be the case, the Platform will utilize LLM services from the Supplier's EU AWS tenant or Google Cloud, where the Customer Content will not be stored or used for training.

3 AUTHENTICATION

The Supplier provides Single Sign-On (SSO) integration to ensure secure and centralized access to the Platform, with all access restricted to SSO-only methods. Our platform integrates with leading identity providers, such as Microsoft Entra ID, for centralized user management and authentication.

This allows Customers' Users to log in using their existing credentials, minimizing the risk associated with creating or managing separate accounts. Additionally, this approach means that the Users' account credentials are not stored, further enhancing the overall security.

4 SYSTEM ACCESS CONTROL

User role management controls and monitors data access, ensuring that only authorized personnel have access. A strict minimal access policy, based on the principle of least privilege, restricts access to databases containing Personal Data to only those specific employees who are explicitly authorized.

5 MONITORING AND SECURITY UPDATES

The Supplier conducts regular audits, updates security protocols, and maintains audit logs of system and network events to maintain the highest standards. These logs are tamper-evident and monitored 24/7. We have well-defined incident response procedures tested annually and a defined process for promptly applying security updates and patches.

The Supplier also works directly with the Customers to ensure that their platform use aligns with their compliance requirements, and the Supplier offers support to navigate regulatory requirements and maintain legal standards.

The Processor maintains logs for security and operational integrity but does not review Customer Content unless strictly necessary for support or troubleshooting, and only upon the Controller's request.

Appendix B Overview of the Sub-processors

Company	Purpose and data	Address	Information	Processing/storage location (country)
Microsoft Ireland Operations, Ltd.	The purpose is to provide AI-powered text generation, analysis, and modification based on documents or texts uploaded at the Customer's request. Depending on the content in uploaded documents, text, and user interactions, the processing may include but is not limited to (i) identification data, (ii) sensitive data, (iii) special category data, and (iv) professional information.	Attn: Privacy Policy One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland	https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA	For EU/EEA customers: The Netherlands, and no transfer/access outside the EU/EEA. For Swiss customers: Switzerland, and no transfer/access outside Switzerland. For US customers: United States, and no transfer/access outside United States.
Weaviate B.V.	The purpose is to provide search and analysis of uploaded documents as vectorized data requested by the Customer. Depending on the content in uploaded documents, text, and user interactions, the processing may include but is not limited to (i) identification data, (ii) sensitive data, (iii) special category data, and (iv) professional information.	Prinsengracht 769A, 1017JZ, Amsterdam, the Netherlands	https://trust.weaviate.io	For EU/EEA customers: The Netherlands, and no transfer/access outside the EU/EEA. For Swiss customers: Switzerland, and no transfer/access outside Switzerland. For US customers: United States, and no transfer/access outside United States.
Sirrus B.V.	The purpose is to monitor and configure infrastructure to ensure security and availability, and, if necessary, potential access to personal data following strict policies. Depending on the content in uploaded documents, text, and user interactions, the processing may include but is not limited to (i) identification data, (ii) sensitive data, (iii) special	Evert van de Beekstraat 354 1118 CZ Schiphol info@sirrus.nl	https://www.sirrus.nl/	The Netherlands, and (i) no transfer/access outside the EU/EEA, (ii) only potentially access to data with a strict policy.

	category data, and (iv) professional information.			
DeepL SE	The purpose is to provide translation services for uploaded documents or texts as requested by the customer. Depending on the content in uploaded documents, text, and user interactions, the processing may include but is not limited to (i) identification data, (ii) sensitive data, (iii) special category data, and (iv) professional information.	Maarweg 165 50825 Cologne Germany datenschutz@dhp.g.de	https://www.deepl.com/en/pro-privacy_info	Sweden and Iceland, and (i) no transfer/access outside the EU/EEA, (ii) no storage.
Amazon Web Services EMEA SARL	The purpose is to provide LLMs (Claude) text generation, analysis, and modification based on documents or texts uploaded at the Customer's request. Depending on the content in uploaded documents, text, and user interactions, the processing may include but is not limited to (i) identification data, (ii) sensitive data, (iii) special category data, and (iv) professional information.	38 Avenue John F. Kennedy, L-1855, Luxembourg	https://aws.amazon.com/compliance/data-privacy	For all customers except US: Germany (Frankfurt) and (i) no transfer/access outside the EU/EEA, (ii) no storage. For US customers: United States and (i) no transfer/access outside United States, (ii) no storage.
Google Cloud EMEA Limited IE3668997OH	The purpose is to provide LLMs (Gemini) text generation, analysis, and modification based on documents or texts uploaded at the Customer's request. Depending on the content in uploaded documents, text, and user interactions, the processing may include but is not limited to (i) identification data, (ii) sensitive data, (iii) special category data, and (iv) professional information.	Velasco Clanwilliam Place Dublin 2 Ireland	https://cloud.google.com/terms/data-processing-addendum	For all customers except US: Belgium / Netherlands and (i) no transfer / access outside the EU/EEA, (ii) no storage. For US customers: United States and (i) no transfer/access outside United States, (ii) no storage.
Scaleway S.A.S.	The purpose is to provide LLMs (GLM) text generation, analysis, and modification based on documents or texts uploaded at the Customer's request. Depending on the content in uploaded documents, text, and user interactions, the processing	8 rue de la Ville l'Evêque 75008 Paris France	https://www.scaleway.com/en/docs/generative-apis/reference-content/data-privacy/	France (Paris), and (i) no transfer/access outside the EU/EEA, (ii) no storage (zero data retention).

	may include but is not limited to (i) identification data, (ii) sensitive data, (iii) special category data, and (iv) professional information.			
Moonlit Legal Technologies B.V.	The purpose is to provide a search in legal databases/sources. Depending on the content of the users' search query, the processing may include but is not limited to (i) identification data, (ii) sensitive data, (iii) special category data, and (iv) professional information.	Westeinde 14 1017 ZP Amsterdam Netherlands	https://app.eu.vanta.com/moonlit.ai/trust/8rjylywwont3lu42e1fp1	Netherlands and (i) no transfer / access outside the EU/EEA, (ii) no storage. Moonlit sources are optional.
AlphaAI Technologies Inc.	The purpose is to provide a search web search based on the Customer's request. Depending on the content of the users' search query, the processing may include but is not limited to (i) identification data, (ii) sensitive data, (iii) special category data, and (iv) professional information.	1350 Broadway, 24th Floor, New York, NY 10018, USA	https://trust.tavily.com	United States.