spotler

DATA PROCESSING AGREEMENT

This data processing agreement is an integral part as an annex to the Agreement with contract number [**NUMBER**] dated [**DATE**], between [CUSTOMER] ('**Controller**') and Spotler ('**Processor**').

Controller and Processor shall hereinafter jointly also be referred to as '**Parties**' and each individually as a '**Party**'.

CONSIDERATIONS:

I. Based on the Agreement, Processor shall perform services for Controller.
II. The intended services entail that Processor will process personal data for which Controller is responsible (hereinafter**: the Personal Data**) and which Processor shall not process for its own purposes or other purposes.
III. Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 (hereinafter: **GDPR**) applies to this processing of personal data.
IV. The Parties have laid down the agreement and conditions regarding this processing of the Personal Data in this data processing agreement (hereinafter: **the Data Processing Agreement**).

THE PARTIES HAVE AGREED AS FOLLOWS:

1. The Data Processing Agreement

1.1. Terms beginning with a capital letter in the Data Processing Agreement shall have the meaning assigned to them in Article 4 of the GDPR unless terms have been defined in this article.
1.2. The Data Processing Agreement pertains to the processing of the Personal Data by Processor on behalf of Controller in the context of implementing the Agreement.
1.3. The following annexes are part of the Data Processing Agreement:
  1.3.1. Annex 1: Processing Activities
  1.3.2. Annex 2: Security Measures
  1.3.3. Annex 3: Subprocessors
  1.3.4. Annex 4: Contact Information regarding processing
1.4. The Data Processing Agreement is an integral part of the Agreement. To the extent that the provisions in the Data Processing Agreement conflict with the provisions in the rest of the Agreement, the provisions in the Data Processing Agreement shall prevail.
1.5. Unless unambiguously stated otherwise, references in the Data Processing Agreement are to the articles of and annexes to the Data Processing Agreement.
1.6. In the Data Processing Agreement, references to legal provisions shall be construed as references to legal provisions at the time of entering into the Data Processing Agreement.

2. Processing execution

2.1. Processor guarantees that it shall process the Personal Data on behalf of Controller to the extent that:
  2.1.1. this is in the context of implementing the Agreement (as specified in Annex 1);
  2.1.2. Controller has given additional written instructions for such processing.

2.2. Processor shall follow all reasonable instructions from Controller regarding the processing of the Personal Data. Processor shall immediately inform Controller if, in its opinion, instructions conflict with applicable legislation regarding personal data processing.

2.3. Notwithstanding the provisions in the first paragraph of this article, Processor is permitted to process the Personal Data if a legal provision (including judicial or administrative orders based thereon) obligates him to such processing. In such a case, Processor shall notify Controller of the intended processing and the legal requirement prior to the processing, unless such legislation prohibits such notification. Processor shall, where possible, enable Controller to oppose to this mandatory processing and shall limit the mandatory processing to the strictly necessary.

2.4. Processor shall process the Personal Data properly and with due care and in accordance with its obligations as Processor under the GDPR.

2.5. Controller shall ensure that no special categories of personal data as referred to in Article 9 of the GDPR shall be provided to Processor so that Processor does not need to process such personal data.

3. Confidentiality

3.1. Processor shall ensure that confidentiality has been agreed upon with its employees regarding the processing of personal data.

4. Personal Data Security

4.1. Processor shall implement appropriate and effective technical and organizational security measures that – taking into account the state of the art, the cost of implementation, the nature, scope, context, and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of Data Subjects – are aligned with the nature of the Personal Data to be processed (as specified in Annex 1). This is to protect the Personal Data against loss, unauthorized access, corruption, or any form of unlawful processing, as well as to guarantee the (timely) availability and integrity of the data.

4.2. Processor holds an ISO-27001 certification and has, pursuant to paragraph 1 of this article, implemented appropriate security policies for the processing of personal data.

4.3. Processor shall, upon first request from Controller, provide a (copy of a) valid certificate issued by an independent and competent third party, along with the statement of applicability, demonstrating that Processor complies with the obligations in this article.

4.4. The security measures taken by Processor as referred to in this article are described in Annex 2. Controller accepts that the organizational and technical security measures taken by Processor are sufficient to ensure an appropriate security level.

5. Data breach

5.1. Processor shall actively monitor Security Breaches and will report on the results of the monitoring to Controller in accordance with this Article 5.

5.2. When a breach concerning Personal Data occurs or has occurred, Processor shall notify Controller immediately, but no later than 24 hours after Processor has become aware of it, unless the Breach is very likely to result in little to no risks for Controller and the Data Subjects. Processor shall provide all relevant information about: (a) the nature of the Breach; (b) the Personal Data potentially affected; (c) the observed and suspected consequences of the

Breach; and (d) the measures that have been or will be taken to address the Breach or to minimize its consequences and/or damage as much as possible.

5.3. Processor shall, notwithstanding the other obligations in this article, take measures that can reasonably be expected to remedy the Breach as soon as possible or minimize its further consequences. Processor shall consult with Controller as soon as possible to make further arrangements thereon.

5.4. Processor shall at all times provide its cooperation to Controller and shall follow Controller's instructions and conduct proper investigation of the Breach.

5.5. Any necessary notification of a Breach regarding the Personal Data to the Data Protection Authority and/or Data Subjects shall be made by Controller. Processor shall not provide any information about Breaches to Data Subjects or other third parties, except to the extent Processor is legally required to do so or the Parties have agreed otherwise.

5.6. Notifications regarding Breaches shall be made to the contact person of Controller as described in Annex 4.

5.7. If and insofar the Parties have agreed that Processor maintains direct contact with authorities other than the Data Protection Authority, or other third parties in relation to a Breach, Processor shall keep Controller informed thereof unless Processor is not permitted to do so.

6. Audit and cooperation

6.1. With the certification mentioned in Article 4.2, Processor principally demonstrates that it complies with and can comply with the provisions in paragraphs 1 through 4 of Article 28 of the GDPR. If, notwithstanding this, Controller has reasonable grounds for substantial doubt as to whether Processor has or can comply with the obligations under the Data Processing Agreement and the GDPR, and the Parties have not been able to eliminate this doubt through mutual consultation, then Controller shall have the right to have the compliance with the measures mentioned in Article 4 and compliance with paragraphs 1 through 4 of Article 28 GDPR verified (hereinafter: **an/the Audit**). Processor and Controller shall jointly determine when and by which independent third party the Audit will be conducted. An Audit shall exclusively be carried out by an independent registered accountant or EDP auditor.

6.2. During the term of the Data Processing Agreement, Controller may conduct one Audit per calendar year, which does not include any investigation initiated by a competent supervisory authority. Controller shall ensure that the persons conducting the Audit sign a confidentiality statement in advance that is acceptable to Processor. Processor shall cooperate with an Audit.

6.3. Processor shall reasonably cooperate with competent supervisory authorities such as the Netherlands Authority for the Financial Markets (NL: *De Autoriteit Financiële Markten*) and the Data Protection Authority with their investigation. Processor shall therefore follow the duly given instructions from these authorities that relate to the services to be provided by Processor under the Agreement, provide all requested information and grant access to relevant documents and data. All of this shall be to the extent reasonably possible and subject to confidentiality obligations under the law or towards third parties.

6.4. If, despite the certification mentioned in Article 4.2, Controller has reasonable grounds to require additional information about the processing of Personal Data - for example, due to a required compliance procedure - Processor shall, upon request from Controller, provide all materially relevant information to Controller so that Controller can demonstrate, inter alia on the basis of that information, that it complies with the applicable (privacy) legislation.

6.5. Furthermore, Processor shall, upon Controller's request, provide all necessary assistance to Controller in fulfilling Controller's other legal obligations under applicable privacy legislation, such as conducting a Data Protection Impact Assessment (DPIA).

6.6. The GDPR and other legislation grant certain rights to the Data Subject. Processor shall cooperate with Controller in fulfilling Controller's obligations arising from these rights.

6.7. Any request received by Processor from a Data Subject concerning the processing of Personal Data shall be forwarded by Processor to Controller as soon as possible, but within 2 working days.

6.8. In the context of all cooperation requested under this Article 6, Controller shall ensure that Processor's business operations are not excessively disrupted.

6.9. Processor may charge Controller for reasonably incurred costs made in connection with the Articles 6.1 through 6.6.

6.10. If the final report of an Audit establishes that Processor has attributably breached the obligations under the Data Processing Agreement, then the costs incurred and to be incurred by Processor (for example, for the remedy of the breach) will remain for Processor's account. The costs of third parties incurred by Controller for or in connection with the Audit and the compensation payable to third parties by Controller in this regard will under no circumstances be for the account of Processor.

7. Engaging subprocessors

7.1. The subprocessors engaged by Processor for the implementation of the Agreement at the time of closing this Data Processing Agreement are listed in Annex 3. By entering into the Agreement, Controller consents for these subprocessors.

7.2. Controller hereby also gives general consent for further engagement or replacement of subprocessors. Processor shall inform Controller of the intended engagement of new subprocessors.

7.3. Processor shall inform Controller about any intended addition or replacement of subprocessors, whereby Controller shall be given the opportunity to object to such changes within 30 days.

7.4. Processor shall be responsible for the subprocessors it has engaged and shall impose the same type of conditions, obligations, and responsibilities on them as apply to Processor itself under this Data Processing Agreement. If Controller has objections against a new subprocessor, Processor shall make reasonable efforts to resolve Controller's objections. If Processor cannot resolve Controller's objections, Controller may suspend the Agreement.

7.5. Processor shall not transfer the Personal Data to a country outside the European Economic Area without an appropriate level of protection unless this has been agreed upon under the Agreement with Controller or unless 'standard contract clauses' have been agreed with the subprocessor in the third country.

8. Retention periods, Return and destruction of Personal Data

8.1. Controller shall determine, taking into account the statutory retention periods applicable to Controller, how long data must be retained. Controller shall be responsible for storing and removing data as it has direct access to the application provided by Processor.

8.2. If Controller has not taken care of removal of the Personal Data in accordance with Article 8.1, Processor shall, upon written request from Controller or - if applicable - at the end of the agreed retention periods, for a reasonable compensation, at Controller's discretion: either

definitively destroy (or cause to be destroyed) the Personal Data or return it to Controller. Upon Controller's request, Processor shall provide evidence that the data has been irretrievably destroyed or deleted. Any return of data shall take place electronically in a commonly used, structured, and documented data format. If return, definitive destruction, or deletion is not possible, Processor shall immediately inform Controller. In such a case, Processor guarantees that it shall treat the Personal Data confidentially and shall no longer process it.

9. Limitation of liability

9.1. The (total) liability of Processor in the event of attributable breach of this Data Processing Agreement or on any other grounds shall at all times be limited in accordance with the provisions set forth in the Agreement.

10. Duration and termination

10.1. This Data Processing Agreement shall enter into force simultaneously with the Agreement and its duration shall be equal to the duration of the Agreement, including any extensions thereof.

10.2. Termination of the Agreement, on whatever grounds (termination / dissolution), shall result in the termination of this Data Processing Agreement on the same grounds unless Parties agree otherwise in that specific case.

10.3. Obligations which by their nature are intended to continue after termination of the Data Processing Agreement shall remain in force after termination. These obligations include, those arising from provisions concerning confidentiality, liability, dispute resolution, and applicable law.

10.4. Controller shall be entitled to terminate this Data Processing Agreement and the Agreement with immediate effect if Processor indicates that it cannot or can no longer comply with the reliability requirements imposed by law and/or case law regarding the processing of Personal Data.

10.5. The obligations under this Data Processing Agreement shall continue as long as Processor processes Personal Data of Controller, even after Processor has ceased to provide the care, services, and/or facilities assigned in the Agreement.

11. Applicable Law and Disputes

11.1. This Data Processing Agreement and its implementation shall be governed by Dutch law.

11.2. Any disputes relating to this Data Processing Agreement that cannot first be resolved through mutual consultation shall be submitted exclusively to the District Court of The Hague.

12. Final provisions

12.1. In the event of nullity or voidability of one or more provisions of this Data Processing Agreement, the remaining provisions shall remain in full force and effect.

12.2. This Data Processing Agreement replaces all previous data processing agreements between Parties.

Annex 1: Processing activities

Purpose of processing: Implementing of the Agreement, consisting of: making the Platform available and performing Platform-related services, such as providing support and consultancy.

Type of processing: Processing in a designated system. This may include: requesting, consulting, forwarding, viewing, combining, screening, securing, destroying data.

Categories of Personal data: Personal data entered by the Controller into the Platform. The Controller determines which (type of) personal data are entered and to which personal data a Processor employee may gain access during the aforementioned services.

This may include the following categories of personal data:

- Name
- Address
- Postcode
- Place of residence
- Telephone number(s)
- Bank account number
- Email address(es)
- Social media contact details
- Date of birth
- Place of birth
- Gender
- Marital status
- Nationality
- Profession
- Chamber of Commerce number
- Household composition
- Policy number
- Relationship number
- Risk address
- Claims data
- Source
- Role/Function
- Debtor and creditor data
- Invoices
- Payments
- Insurance history
- Complaints
- Cancellation data
- Payment arrangements
- Academic/professional qualifications
- CV/work experience
- Passport photo/profile photo
- Language proficiency
- Financial data (income, expenditure, assets)
- Signature
- Vehicle data (registration number, make, model)
- IP address
- Location data
- Username/login credentials
- Communication preferences
- Attendance register

Special categories of personal data shall not be made available by the Controller to the Processor. The Controller is fully responsible for correctly categorising all personal data provided and the lawfulness of the processing in accordance with applicable legislation.

Annex 2: Security measures

Spotler has made documents describing appropriate technical and organizational security measures available in the Spotler account of the Controller.

The Processor implements, among other things, the following appropriate technical and organizational measures to ensure a security level appropriate to the risk. The overview below is not exhaustive but indicative.

Organizational measures:
Some of the organizational measures implemented by the Processor include:

- Assigning responsibilities for information security.
- Increasing security awareness among existing and new employees.
- Establishing procedures to periodically test, assess, evaluate, and, if necessary, improve security measures.
- Regularly monitoring log files.
- Signing confidentiality agreements and data processing agreements.
- Regularly assessing whether the same objectives can be achieved with fewer personal data. Restricting access to personal data to the minimum necessary.

Technical measures:
Some of the technical measures implemented by the Processor include:

- Logical and physical (access) security of systems and premises.
- Digital security of systems and applications.
- Hardware and software measures.
- Update measures.
- Virus scans and malware protection.
- Firewalls.
- Logging measures.
- Password management.
- Authorization management.
- Encryption.

Standards:
Spotler Group has established its information security management system based on the ISO/IEC 27001:2022 standard and is committed to obtaining and maintaining ISO 27001 certification. A complete overview of the implemented security measures is included in the Statement of Applicability.

Annex 3: Subprocessors

De Subprocessors of Spotler are devided into the following categories:

1. **Data centres & Cloud providers** *(ISO 27001 certified secure data centres)*
2. **AI providers**
3. **Supporting software**
4. **SMS providers**

Of the Subprocessors listed below, only those Subprocessors that relate to the product procured by the Controller shall apply.

Product	Subprocessor	Service Location	Description	Categories	Data classification
Spotler Engage	Iron Mountain Data Centers AMS-1	The Netherlands (EU)	Datacenter for hosting and data storage	1	Private – (Regular PII)
	Amazon Web Services (AWS)	Germany (EU)	Cloud data storage of video and images (not text or other content).	1	Private – (Regular PII)
	Pusher (Bird)	Ireland (EU)	Processing of chat conversations for Engage Chat	3	Private – (Regular PII)
	OpenAI	United States of America (USA)	PostOptimizer (outbound publishing)	2	No PII
	Google Cloud Platform	Ireland (EU)	Cloud hosting and data storage	1	Private – (Regular PII)
Spotler Chat+	Google Cloud Platform (GCP)	Ireland (EU)	Cloud hosting and data storage	1	Private – (Regular PII)
	Amazon Web Services (AWS)	Germany (EU)	Storing assets in S3 buckets	1	Private – (Regular PII)
	OpenAI	United States of America (USA)	Processing of messages for Chatbot	2	Private – (Regular PII)
	Zenrows	Spain (EU)	Scraping content from websites	1	Private – (Regular PII)
	Pusher (Bird)	Ireland (EU)	Sending notifications from our async services (e.g., model training)	1	Private – (Regular PII)
Spotler Activate	Velia	Germany (EU)	Hosting	1	Private – (Regular PII)
	TransIP	The Netherlands (EU)	Storage of back-ups (encrypted)	1	Private – (Regular PII)

	Cloudflare	Worldwide	HTTP Requests & Events	1	Private – (Regular PII)
	Sentry	Germany (EU)	System Monitoring	3	Private – (Regular PII)
	DigitalOcean	Internationally available (POPs)	Product images	1	No PII
	Thoughtspot	Germany (EU)	Analytics	2	No PII
	Spotler Connect	European Union	Data synchronisation	2	Private- (Regular PII)
Spotler Activate Pro	DigitalOcean	The Netherlands (EU)	Hosting (client data)	1	Private – (Regular PII)
	Velia	Germany (EU)	End to end monitoring	3	Private – (Regular PII)
	Amazon Web Services (AWS)	Germany (EU)	Hosting Mongo DB (Feed & Analytics)	1	Private – (Regular PII)
	Cloudflare	The Netherlands (EU)	HTTP Requests & Events	1	Private – (Regular PII)
	Telekom	Germany (EU)	Email Templates, S3	3	Private – (Regular PII)
Spotler Activate Search	Amazon Web Services (AWS)	Germany (EU)	Datacenter for hosting and data storage	1	Private – (Regular PII)
	Cloudflare	Worldwide	Nameservers + DNS / CDN	1	Private – (Regular PII)
Spotler CRM	Google Cloud Platform (GCP)	Belgium (EU)	Database storage for customer data, file storage for customer data	1	Private – (Regular PII)
	Amazon Web Services (AWS)	France (EU)	Webservers	1	Private – (Regular PII)
	Velia	Germany (EU)	Hosting	1	Private – (Regular PII)
Spotler Mail+	Equinix AM3	The Netherlands (EU)	Datacenter for hosting and data storage	1	Private – (Regular PII)
	ProServe	The Netherlands (EU)	Management of VMware platform	1	Private – (Regular PII)

	Spotler Message	EU	SMS service provider	4	Private – (Regular PII)
	TransIP	The Netherlands (EU)	Storage of back-ups (encrypted)	1	Private – (Regular PII)
	OpenAI	United States of America (USA)	Artificial Intelligence (AI) service provider	2	No PII
	BackBlaze	The Netherlands (EU)	Storage of back-ups	1	Private – (Regular PII)
	ElasticSearch	The Netherlands (EU)	Statistics & logging	3	Private – (Regular PII)
Spotler MailPro	BackBlaze	The Netherlands (EU)	Storage of back-ups	1	Private – (Regular PII)
	BIT NL	The Netherlands (EU)	Data storage	1	Private – (Regular PII)
	Spotler Message	European Union	Telecom service provider	4	Private - (Regular PII)
Spotler SendPro	Equinix AM2	The Netherlands (EU)	Hosting and data storage	1	Private – (Regular PII)
	Iron Mountain Data Centers AMS-1	The Netherlands (EU)	Hosting and data storage	1	Private – (Regular PII)
	Digital Realty	The Netherlands (EU)	Hosting and data storage	1	Private – (Regular PII)
	Spotler Message	EU	Telecom service provider for SMS messages	4	Private – (Regular PII)
Spotler Connect	Amazon Web Services (AWS)	Germany (EU)	Datacenter for hosting and data storage	1	Private – (Regular PII)
	ProServe	The Netherlands (EU)	Managed Kubernetes Platform	1	Private – (Regular PII)
	ElasticCloud (Runs on AWS)	Germany (EU)	Search	1	No PII
Spotler Leads	Equinix AM3	The Netherlands (EU)	Datacenter for hosting and data storage	1	Private – (Regular PII)
	ProServe	The Netherlands (EU)	Management of VMware platform	1	Private – (Regular PII)
Spotler Message*	CM	The Netherlands (EU)	Telecom service provider for SMS messages	4	Private – (Regular PII)

	Essendex	The United Kingdom (UK)	Telecom service provider for SMS messages	4	Private – (Regular PII)
	IT1 / IT Jedan	Croatia (EU)	Telecom service provider for SMS messages	4	Private – (Regular PII)
	Sinch	Sweden (EU)	Telecom service provider for SMS messages	4	Private – (Regular PII)
	Syniverse	Luxembourg (EU) / United States of America (USA)	Telecom service provider for SMS messages	4	Private – (Regular PII)
	Tyntec	Germany (EU)	Telecom service provider for WhatsApp message	4	Private – (Regular PII)
	Dataplace (data center Rotterdam)	The Netherlands (EU)	Hosting and data storage	4	Private – (Regular PII)
	Bird	The Netherlands (EU)	Telecom service provider for SMS messages	4	Private – (Regular PII)
	Infobip	United Kingdom (UK)	Telecom service provider for SMS messages	4	Private – (Regular PII)
	Sinhro	Slovenia (EU)	Telecom service provider for SMS messages	4	Private – (Regular PII)
	Vonage	United States of America (USA)	Telecom service provider for SMS messages	4	Private – (Regular PII)
	Twilio	United States of America (USA)	Telecom service provider for SMS messages	4	Private – (Regular PII)
	Tyntec	The Netherlands (EU)	Telecom service provider for SMS messages	4	Private – (Regular PII)
Momice	Amazon Web Services (AWS)	Germany (EU)	Datacenter for hosting and data storage	1	Private – (Regular PII)
	SendPro	The Netherlands (EU)	Mail Service Provider (only use data for sending mails, short storage, for their use only)	1	Private – (Regular PII)
	Adyen	The Netherlands (EU)	Payment Service Provider	3	Private – (Regular PII)
	Brevo	France (EU)	Mail Service Provider (only use data for sending mails, short storage, for their use only)	1	Private – (Regular PII)
Spotler	Thoughtspot	Germany (EU)	Analytics	2	No PII

Analytics	ProServe	The Netherlands (EU)	Managed Kubernetes Platform	1	Private – (Regular PII)
	Spotler Connect	European Union	Data synchronisation	2	Private- (Regular PII)
Spotler ID	ProServe	The Netherlands (EU)	Managed Kubernetes Platform	1	Private – (Regular PII)
	Spotler Connect	European Union	Data synchronisation	2	Private- (Regular PII)

* *For SMS messages, the processing of personal data is handled in accordance with standard telecommunications protocols. When messages are sent within the EU, sub-processors located within the European Economic Area (EEA) are used by default. If an SMS message is sent to a recipient outside the EEA, e.g. the United States, the delivery is handled by the recipient's local telecommunications provider. In such cases, data may be routed through or processed by providers outside the EEA solely for the purpose of message delivery.*

Annex 4: Contact information regarding processing

Contact Information of Controller:

- See signed agreement

Contact Information of Processor:

- Privacy officer Spotler | privacyofficer@spotler.nl | +31 (0)88 103 09 09