INTROW DATA PROCESSING AGREEMENT

In the delivery of the Services and the Platform, and through the Customer's use of the Services, Introw may have access to some data which qualifies as Personal Data and for which Introw acts as a Processor. This Data Processing Agreement, entered into between Introw and the Customer, governs the Processing of Personal Data in this context.

This Data Processing Agreement applies in addition to the other provisions as set out in the Contract which shall continue to apply also to the activities as contemplated herein.

Capitalized notions used throughout this Data Processing Agreement shall have the meaning attributed to them as set out in the Terms and Conditions, unless as otherwise expressly specified in this Data Processing Agreement.

1. Additional definitions

1.1. "**Data Protection Legislation**" means any applicable legislation in force regarding the processing and protection of Personal Data, including the European GDPR Regulation 2016/679 and the Belgian implementation thereof.

1.2. "**Data Controller**", "**Data Processor**", "**Data Subject**", "**Personal Data**", "**Data Breach**", "**Transfer**", and "**Processing**" / "**Processed**" / "**Process**" shall have the same meanings as set out in the Data Protection Legislation.

1.3. "**Customer Personal Data**" means Personal Data Processed (such as stored, uploaded, accessed, sent, communicated, amended, etc.) through use of the Platform / Services, including CDS Data, but excluding Introw Platform Usage Data and data as referred to in clause 2.1 of this Data Processing Agreement (including without limitation customer contact information, business details and transaction details).

2. Processing as a Data Controller

2.1. Any Personal Data in relation to which Introw acts as a Data Controller (such as Introw Platform Usage Data and Customer business representative Personal Data, including addresses, email, telephone number and other information which is shared generally and necessarily as a result of the (potential) business relationship between Introw and the Customer and their respective representatives) shall be Processed in accordance with the Privacy Statement. Please refer to this document for further information.

3. Processing as a Data Processor

3.1. Nature and purposes of Processing the Personal Data

(a) As a result of the nature of the Platform and Services supplied, Introw may have access to and Process certain Customer Personal Data which are stored on or are connected to the Platform / Services. Introw will only process Customer Personal Data on behalf of and under the documented and lawful instructions of Customer, for the purposes of the Contract and as set out herein.

(b) Introw may Process these Customer Personal Data for purposes of providing the Platform and Services, hence for the performance of the Contract. The parties acknowledge that the execution and performance of the Contract and the use of the Platform and the Services constitute the documented instructions of Customer. **The Processing activities are further described in clause 14 below**.

(c) Any additional Processing of Customer Personal Data requires the written consent of the Customer, and Introw may evaluate (and refuse) such additional Processing activities. Introw may also inform

the Customer in the event any Processing instruction may constitute a breach of Data Protection Legislation.

3.2. Roles of the Parties

1. In respect of what is set out in clause 3.1:
   (a) Introw shall in such capacity act solely as a Data Processor, not as a Data Controller, and respect the obligations imposed on it as set out in Data Protection Legislation.
   (b) The Customer agrees and acknowledges that the Processing activities referred to in this clause 3 are an integral part of the standard Services offering of Introw and are thus performed on the instruction of the Customer, who wishes to make use of the same. The Contract (including this Data Processing Agreement) and its provisions are Customer's documented instructions to Introw for Processing Customer Personal Data. Additionally, where Introw is obliged by applicable law to Process Personal Data, it shall have the right to do so.
   (c) The Customer shall at all times act as a Data Controller in relation to Customer Personal Data. As a result, the Customer shall comply with all of its obligations as a Data Controller under Data Protection Legislation, including without limitation obtaining and maintaining all necessary and valid consents and providing sufficient transparency. Without limiting the generality of the foregoing, the Customer shall (i) have sole responsibility for the accuracy, quality, integrity, legality and reliability of Customer Personal Data and of the means by which it acquired Customer Personal Data and (ii) comply with all applicable Data Protection Legislation in collecting, compiling, storing, sharing, transferring, accessing and using Customer Personal Data when making use of the Services.

4. Duration

4.1. This Data Processing Agreement enters into force together with the Contract and shall remain in force during the term of the Contract.

4.2. After termination of the Contract, Introw shall have no right to Process Customer Personal Data, unless (a) where anonymised or aggregated and/or in statistical form, and (b) except for Processing necessary for compliance with its own legal, regulatory, accounting and tax obligations.

4.3. Without prejudice to clause 4.2, where after termination of the Contract any Customer Personal Data would remain on any of Introw's systems, the Customer has the right to request the deletion or return of such Customer Personal Data in Introw's standard data format. Any such request must be submitted to Introw in writing.

5. Sub-processors

5.1. Customer acknowledges and agrees that Introw may rely on sub-Processors to support the provision of the Platform and Services, when strictly necessary for the performance of the Contract.

5.2. Introw maintains an up-to-date list of its sub-Processors, which it updates on a regular basis. The list of Introw's sub-Processors can be provided upon written request by the Customer.

5.3. For the avoidance of doubt, use of sub-Processors will not relieve, waive or diminish any obligation Intro has under this Data Processing Agreement. In that sense, Introw shall only use sub-Processors offering a sufficient level of appropriate technical and organisational measures to meet the requirements of Data Protection Legislation and

it shall agree on contractual provisions with such sub-Processor which are similar to those as stated herein.

6. Data Subject rights and Customer assistance

6.1. During the term of the Contract, Introw shall, to the extent possible for Introw and to the extent the Customer (who shall at all times be the first contact point of its own customers or business relations) has no other means to meet its obligations under Data Protection Legislation, provide the Customer with reasonable assistance to meet its obligations under Data Protection Legislation and as provided for in Data Protection Legislation (particularly to assist the Customer in ensuring compliance with the obligations resulting from Articles 32 to 36 of the European GDPR Regulation 2016/679). The Customer shall reimburse Introw for any reasonable costs incurred as a result of such assistance.

6.2. In the event Introw would receive any request from a Data Subject (of whom Customer Personal Data is Processed under this Contract) or business relation of the Customer to access, delete, correct, block or otherwise Process Personal Data Processed under the Contract, the Parties agree that Intro shall inform the Customer of the same and hand over all relevant communications to the Customer without first responding to it directly.

7. Security

7.1. The Customer, as a Data Controller, is entirely and solely responsible for the security of its own data (including Customer Personal Data).

7.2. With respect to Processing Customer Personal Data and to minimize risks of any misuse thereof, and more in general in relation to the Processing of Personal Data: (i) Introw shall ensure that access to Customer Personal Data by personnel of Introw is limited to that of its personnel who require such access to perform the Contract and that such personnel to whom it grants access to such Customer Personal Data are directed to keep such Customer Personal Data confidential; (ii) Introw shall maintain appropriate administrative, physical, technical and organizational safeguards for protection of Customer Personal Data having regard its role; (iii) to the extent relevant and required under Data Protection Legislation, and unless notification is delayed by the actions or demands of a law enforcement agency, Introw shall report to the Customer the unauthorized acquisition, access, use, disclosure or destruction of Personal Data, (a "**Breach**") within seventy-two (72) hours following determination by Introw that a Breach occurred on its systems and Introw shall reasonably assist the Customer with the investigation and mitigation of the impact of any such Breach as well as any notification obligation towards a supervisory authority that may be necessary.

8. Transfers

8.1. In the event of a Transfer of Customer Personal Data to a third country outside the EU and outside the EEA (each a "**Third Country**"), the Parties acknowledge that steps must be taken to ensure that such data transfers comply with Data Protection Legislation. In this sense, Introw shall comply with the provisions of Data Protection Legislation allowing Transfers, such as Transferring to a Third Country offering an adequate level of protection, use of the European Commission's standard contractual clauses, etc.

9. Audit

9.1. Upon the Customer's reasonable request, Introw shall provide such information to the Customer necessary to demonstrate its compliance with Data Protection Legislation. The Customer can also request an independent third-party auditor, to be approved in writing by Introw, to conduct an audit. The contract with such auditor shall require the auditor to respect Introw's confidentiality obligations, trade secrets and confidential information and shall solely relate to compliance with Data Protection Legislation.

Notwithstanding the foregoing and for the avoidance of doubt, the foregoing may in no way materially impede the Customer, or a third party auditor, from conducting an audit as described herein.

9.2. An audit can only be required taking into account reasonableness and for a maximum of once (1) per two (2) years unless Data Protection Legislation or guidance by a competent supervisory authority would dictate otherwise. Audits shall be conducted at a time agreed with Introw in writing, and in each event during normal business hours and without interruption to Introw's normal business operations.

9.3. The audit report shall be provided to Introw by the auditors before it is finalised, so that Introw can make any comments it may have, and the final report should take account of and respond to these comments. The audit report will then be sent to Introw and discussed in a meeting between the Parties.

9.4. In the event the final audit report reveals breaches of the commitments made in the performance of this Data Processing Agreement, Introw shall propose a corrective action plan within a maximum of twenty (20) working days from the meeting between the Parties.

9.5. The Customer shall bear all costs related to such audits, unless a substantial breach of Data Protection Legislation attributable to Introw results from such audit.

10. Costs

10.1. Services and assistance rendered by Introw to the Customer hereunder shall be charged at Introw's then-current hourly rates, unless where stated otherwise in this Data Processing Agreement.

11. Notice of default

11.1. When Introw fails to comply with its obligations under this Data Processing Agreement, the Customer shall first send a registered notice of default. This notice shall clearly mention the defaults that occurred, and, if redress is possible, a proposal of remedial measures and a reasonable term for their implementation.

12. Liability

12.1. The provisions in relation to liability as set out in the Terms and Conditions are applicable to this Data Processing Agreement and all services provided by Introw in respect of this Data Processing Agreement.

12.2. Introw shall in any event only be liable for direct damages caused by a Processing activity of Introw which beaches this Data Processing Agreement and subject to the terms as set out herein.

13. General

13.1. The provisions of the Terms and Conditions shall also apply *mutatis mutandis* to this Data Processing Agreement, unless explicitly stated otherwise herein.

14. Description of the Processing activities

2.	**Subject**	3.	See our Services description on Introw's website
4.	**Nature**	5.	Collection, organization, structuring, storage, consultation, use, disclosure by transmission, alignment or combination, restriction, modification and amendment, erasure or destruction
6.	**Purpose**	7.	Performance of the Contract
8.	**Duration**	9.	Term of the Contract
10.	**Personal Data**	11.	Identification data, contact data, professional data
12.	**Data Subject**	13.	Customer partnerships and business contacts, including personal data on related data subjects

Annex 1 - Sub-processor list

Provider	Purpose of processing	Data Processing Territory
Amazon Web Services (AWS)	Cloud hosting and infrastructure	Ireland (EU)
Cloudflare	Content delivery network (CDN) and security	EU
Stripe	Payment processing	EU
HubSpot	Customer relationship management (CRM)	EU
Intercom	Customer support and helpdesk software	EU
Postmark	Transactional email services	USA (GDPR compliant)
Google Analytics	Product and user analytics	Globally Distributed (GDPR Compliant)
OpenAI	LLM Provider	USA (GDPR Compliant), Zero data retention usage only.
Sentry	Performance monitoring and logging tool	USA (GDPR compliant)
Anthropic	LLM Provider	USA (GDPR Compliant), Zero data retention usage only.
Slack	Internal communication and collaboration tools	USA (GDPR compliant
Zenleads Inc. (dba Apollo.io)	Data Enrichment	USA (GDPR compliant)
Tinybird	Analytics database	EU
Vercel	AI Gateway	USA (GDPR Compliant), Zero data retention usage only.
Aikido	Aikido automatically performs a wide range of security checks. Allowing us to implement security-first safeguards in our development cycle	EU
Vanta	Compliance ISMS	EU
Cohere	LLM Provider	USA (GDPR Compliant), Zero data retention usage only.

DeepL	Translation provider	Germany
Brightdata	Data enrichment provider	USA
Brandfetch	Brand enrichment provider	Switzerland
Langfuse	LLM Observability platform	USA (GDPR Compliant)
Exa	LLM Content provider	USA

Annex 2- Technical and Organisational measures

At Introw, we are ISO 27001 and SOC 2 Type 2 compliant, meaning we have established policies and measures to mitigate technical and organizational risks. We adhere to industry best practices to enforce strong security controls. Additionally, we leverage Vanta to streamline governance and compliance across our organization.

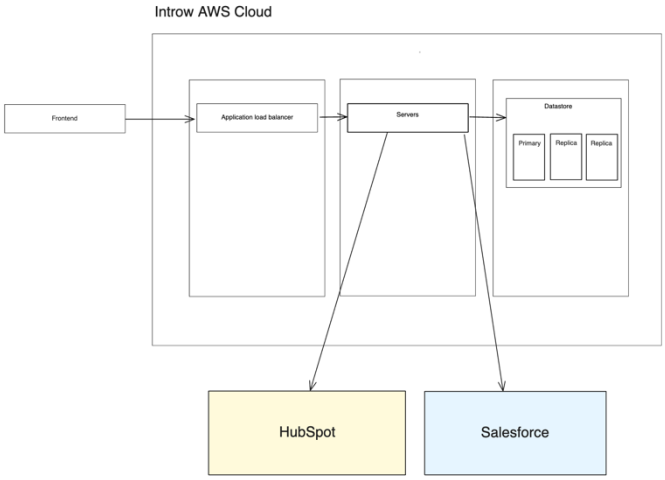
Technical Measures:

- Encryption: All databases are encrypted both in transit and at rest using TLS 1.3.
- Continuous Monitoring: We utilize real-time monitoring tools to oversee critical infrastructure and maintain an integrated incident response mechanism.
- Backup Strategy: Daily backups are performed, with additional backups scheduled during deployments to ensure data integrity and availability.
- Network Security: We employ AWS Virtual Private Cloud (VPC) with Identity and Access Management (IAM) to enforce the principle of least privilege, restricting access to essential components.

Organizational Measures:

- Governance: Our security governance framework is based on ISO 27001 and SOC 2, supported by well-defined policies, risk management procedures, and both internal and external audits.
- Training: All Introw employees undergo regular security awareness training to maintain a strong security culture.
- Risk Management: We conduct thorough vendor risk assessments to ensure third-party compliance and security.
- Incident Response: A formalized incident response plan is in place, aligned with industry best practices to ensure rapid mitigation of security threats.
- Data Protection Policies: We enforce strict policies on data retention, processing, and privacy impact assessments to ensure compliance with relevant regulations.
- These measures are continuously reviewed and improved as part of our ongoing commitment to security and compliance.

Annex 3- Data Flow


Introw AWS Cloud
Frontend
Application load balancer
Servers
Datastore
Primary
Replica
Replica
HubSpot
Salesforce

14.