Data Processing Agreement
in accordance with Art. 28 GDPR

between

Contracting Company (as indicated in the order or registration form)

hereinafter referred to as the "**Controller**"

and

Contracting Entity (as indicated in the order or registration form)

hereinafter referred to as the "**Processor**"
Processor and Controller collectively the "**Parties**"

Preamble

The Controller has selected the Processor to act as a service provider in accordance with Art. 28 of Regulation (EU) 2016/679 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, "**GDPR**").

This Data Processing Agreement, including all Annexes (hereinafter referred to collectively as the "**Agreement**"), specifies the data protection obligations of the parties from the underlying Order Form, the terms and conditions and/or the order descriptions (hereinafter referred to collectively as the "**Principal Agreement**").
The Processor guarantees the Controller that it will fulfil the Principal Agreement and this Agreement in accordance with the following terms:

Sect. 1 Scope and definitions

(1) The following provisions shall apply to all services of data processing provided by the Processor on behalf of the Controller under Art. 28 GDPR, which the Processor performs on the basis of the Principal Agreement, including all activities which may involve the processing of personal data by the Processor on behalf of the Controller.

(2) If this Agreement uses the term "data processing" or "processing" of data, this shall be generally understood to mean the use of personal data. Data processing or the processing of data shall mean any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(3) “Processor Affiliate” means an entity that owns or controls, is owned or controlled by or is under common control or ownership with Processor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

(4) Reference is made to further definitions set forth in Art. 4 GDPR.

(5) Consumer” shall have the meaning set forth under the US Privacy Laws, as applicable.

(6) The expression “US Privacy Laws” refers to applicable US state privacy laws, including, but not limited to, the: California Consumer Privacy Act, as amended by the California Privacy Rights Act, and relevant regulations issued by the California Privacy Protection Agency (“CCPA”), Virginia Consumer Data Protection Act (“VCDPA”), Colorado Privacy Act and relevant rules issued by the Colorado Attorney General (the “CPA”), Connecticut Data Privacy Act (the “CTDPA”) and Utah Consumer Privacy Act (the “UCPA”), as applicable.

Sect. 2 Subject matter and duration of the data processing

(1) The Processor shall process personal data on behalf and in accordance with the documented instructions of the Controller, unless required to do so by Union or EU member state law to which the Processor is subject, in such case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The Processor acknowledges that the Controller is disclosing personal data only in relation to the limited and specified business purposes identified in the Principal Agreement or this Agreement.

(2) The data processing may involve carrying out the following processing activities each as agreed and specified further in the Principal Agreement, among others:

- Online Lead Generation Service
- CRM Integration

(3) The duration of this Agreement corresponds to the duration of the Principal Agreement.

(4) The Controller may terminate this Agreement and the Principal Agreement at any time without prior notice in the event of a serious breach of this Agreement by the Processor, if the Processor fully or partially fails to execute instructions issued by the Controller, or if the Processor refuses to grant access to its business premises in breach of this Agreement. The use of the Controller’s data for purposes other than those specified in this Agreement (Sect. 2) or the breach of an essential obligation of this Agreement by the Processor (such as data loss or the possibility of unauthorized access to the data by third parties) shall be considered a serious breach.

(5) Furthermore, even when the prerequisites pursuant to subsection 4 are not met, the Controller shall be entitled to terminate this Agreement and the Principal Agreement without notice if the Processor repeatedly breaches the terms of this Agreement. Prior to the termination, the Controller shall notify the Processor about the breach in writing or in text form (by fax or email).

Sect. 3 Nature and purpose of the data processing

The nature and purpose of the processing of personal data by the Processor is specified in the Principal Agreement.

Sect. 4 Categories of data subjects

The categories of individuals affected by the processing of personal data under this Agreement ("data subjects") include:

- Controller's B2B clients and contact personnel of these clients
- Potential B2B clients and contact personnel of Controller
- Controller's website visitors

Sect. 5 Types of personal data

The following types of personal data shall be processed under this Agreement:

- Personal data (name, title)
- Contact details (email address, phone number, postal address)
- Contract data (contract details, services, Contracting Company's number)
- Contracting Company's history (phone calls, meetings, email)
- Website traffic and metadata

Sect. 6 Rights and duties of the Controller

(1) The Controller is solely responsible for assessing the lawfulness of the data processing and for safeguarding the rights of data subjects and is hence a controller within the meaning of Art. 4 (7) GDPR.

(2) The Controller is entitled to issue instructions concerning the nature, scale and method of data processing. Such instructions are also considered to be issued by the Controller when using and configuring the Processor's services and platform. Upon request by the Controller, the Processor shall confirm verbal instructions immediately in writing or in text form (e.g., by email).

(3) The Controller shall notify the Processor of any errors or irregularities detected in relation to the processing of personal data by the Processor.

Sect. 7 Duties of the Processor

(1) <u>Data processing</u>

a. The Processor shall process personal data exclusively in accordance with this Agreement and/or the underlying Principal Agreement and in accordance with the Controller's documented instructions, unless required to do so by Union or EU Member State law or

US Privacy Laws to which the Processor is subject (if applicable). In such case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Any processing of data by the Processor other than in the manner described herein or in the Principal Agreement is prohibited. The Processor shall not process data provided for data processing for other purposes, in particular not for its own purposes. Copies or duplicates may not be made, unless this is part of the order, necessary in order to fulfil the Principal Agreement or unless the Controller has given its prior express written consent.

b. The Processor shall comply with all requirements set forth in the US Privacy Laws, as applicable, and to provide the same level of privacy protection that they impose on the Controller in relation to the processing of Consumers' personal data.

c. The Processor shall not sell nor share any Consumers' personal data.

d. The Processor shall not retain, use, or disclose personal data outside of the direct relationship with the Controller.

e. The Processor shall not combine the personal data it receives from the Controller with personal data it receives from or on behalf of another person(s) or entity(ies) or that it collects from its own interaction with the Consumer, provided that the Processor may combine Personal Data to perform any business purpose identified by the US Privacy Laws, as applicable.

(2) Data subjects' rights

a. The Processor shall, within its capabilities, assist the Controller in complying with the rights of data subjects, particularly with respect to rectification, restriction of processing, deletion of data, notification and information. The Processor shall take appropriate technical and organizational measures for this purpose.

b. If instructed accordingly by the Controller, the Processor shall rectify, delete or restrict the processing of personal data processed on behalf of the Controller. The same applies if this Agreement stipulates the rectification, deletion or restriction of the processing of data. The Processor shall not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Controller, but only on documented instructions from the Controller (e-mail sufficient).

c. If a data subject contacts the Processor directly to have his or her data rectified, deleted or the processing restricted, the Processor shall forward this request to the Controller within a reasonable time upon receipt.

d. Controller instructs Processor to respond to data subject access requests directly (including providing information about the Controller). If Processor is unable to respond directly, Processor shall forward this request to the Controller within a reasonable time upon receipt.

Contact point for Data Subject Access Requests is the email privacy@dealfront.com

(3) Monitoring duties

a. The Processor undertakes to ensure, by means of appropriate controls, that the personal data processed on behalf of the Controller are processed solely in accordance with this Agreement and/or the Principal Agreement and/or the relevant instructions.

b. The Processor shall organize its business and operations in such a way that the data processed on behalf of the Controller are secured to the extent necessary in each case and protected from unauthorized access by third parties. The Processor will agree in advance with the Controller any changes in the organization of data processing on behalf of the Controller that are significant for data security.

c. The Processor confirms that it has appointed a Data Protection Officer in accordance with Art. 37 GDPR and that the Data Protection Officer shall monitor compliance with data protection and security laws. The appointed Data Protection Officer is:

Henri Markkanen
dpo@dealfront.com

In the event of a change of Data Protection Officer, the Processor will notify the Controller of this change in writing or in text form, naming the new Data Protection Officer.

(4) Information duties

a. The Processor shall inform the Controller immediately if, in its opinion, an instruction issued by the Controller violates legal regulations. In such cases, the Processor shall be entitled to suspend execution of the relevant instruction until it is confirmed or changed by the Controller.

b. The Processor shall assist the Controller in its maintenance of Records of Processing Activities pursuant to Art. 30 GDPR and provide the Controller with the necessary information in an appropriate manner. Furthermore, the Processor shall keep its own Record of Processing Activities with respect to all processing activities carried out on behalf of the Controller, as required in Art. 30 (2) GDPR.

c. The Processor shall notify the Controller without any reasonable delay of any breach of data protection regulations, of the Principal Agreement and the Agreement and/or the instructions issued by the Controller, where such breach occurs in the course of the processing of data carried out by the Processor, its employees or other third parties entrusted with the processing of data.

d. In the event that the Processor establishes, or if facts justify the assumption, that personal data processed by the Processor on behalf of the Controller have been unlawfully transmitted or otherwise unlawfully disclosed to third parties or that any other

personal data breach has occurred, the Processor shall notify the Controller without delay and no later than 48 hours after becoming aware of the incident, providing information about

- time, nature and extent of the incident, including the number of datasets and data categories presumably affected,
- possible detrimental consequences and
- measures that have been taken by the Processor in order to prevent further personal data breaches in the acute case.

The Processor shall assist the Controller in the comprehensive and timely fulfilment of any reporting obligations.

(5) Location of processing

a. The processing and use of the data shall take place primarily in the territory of the Federal Republic of Germany, in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Data may also be processed in third countries, in particular to provide certain features, if the special requirements of Art. 44 et seqq. GDPR are fulfilled.

b. If the processing of personal data is carried out outside the European Union, the Processor ensures that a lawful cross-border data transfer mechanism is in place.

(6) Other obligations of support and cooperation

The Processor shall assist the Controller within its possibilities in ensuring compliance with the obligations pursuant to Art. 32 – 36 GDPR.

(7) Deletion of personal data after order completion

After termination of the Principal Agreement, the Processor shall be obliged to hand over to the Controller all personal data, documents and work results that are associated with the contractual relationship, as well as to delete them in compliance with data protection and data security regulations and in accordance with the instructions of the Controller. This also applies to any data backups made by the Processor.

Sect. 8 Monitoring rights of the Controller

(1) The Controller shall at all times be entitled to monitor compliance with the provisions on data protection and the contractual agreements to the extent necessary, and may perform the inspections itself or using third parties, in particular by obtaining information and inspecting the stored data and systems as well as other on-site checks. The Parties shall agree on the time of the inspection or auditing and other details ahead of time and at latest fourteen (14) days before the inspection. The auditing shall be carried out in a way that does not impede the obligations of Processor or its subcontractors in regard to third parties. The representatives of the Controller and the auditor must sign conventional non-disclosure commitments.

(2) The Processor will assist the Controller in carrying out inspections and contribute to the complete and speedy processing of the inspections. Controller shall be responsible for its own and Processor's expenses caused by the auditing.

(3) The Processor shall be obliged to provide the Controller with information insofar as this is necessary for carrying out the inspection.

Sect. 9 Docking Clause

(1) Any entity that is not a party to this Agreement may, with the prior written consent (email sufficient) of all Parties, accede to this Agreement at any time as a controller or a processor by completing the Annexes and signing Annex I.

(2) Once the Annexes mentioned in Sec. 9 (1) above are completed and signed, the acceding entity shall be treated as a Party to this Agreement and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(3) The acceding entity shall have no rights or obligations from this Agreement from the period prior to becoming a Party.

Sect. 10 Subprocessing

(1) The Controller authorizes the Processor to make use of other processors in accordance with the following subsections in Sect. 10 of this Agreement. This authorization shall constitute a general written authorization within the meaning of Art. 28 (2) GDPR. For the avoidance of doubt, subprocessing for the purpose of this Agreement means involving a third party appointed by or on behalf of the Processor to perform and conduct services which relate directly to the provisions of the Principal Agreement. This does not include ancillary services, such as telecommunication services, postal/transport services or maintenance (unless specifically covered as a service under the Principal Agreement).

(2) The Processor currently works with the subcontractors specified under https://dealfront.notion.site/sub-processor-list-dealfront and the Controller hereby agrees to their appointment.

(3) The Processor shall be entitled to appoint or replace other processors. The Processor shall inform the Controller in advance of any intended change regarding the appointment or replacement of another processor. The Controller shall register under https://www.dealfront.com/privacy-center/#section8 to receive information on planned changes of the subprocessors. The Controller may object to an intended change on reasonable grounds. If the parties are unable to reach an agreement concerning the use of a new subcontractor, the Controller is entitled to terminate the Agreement with thirty (30) days' notice, insofar as the change of subcontractor affects the Processing of Personal Data.

(4) A level of protection comparable to that of this Agreement must always be guaranteed when another processor is involved. The Processor is liable to the Controller for all acts and omissions of other processors it appoints. The Controller has the right to convince itself of the suitability of the other processor.

(5) In the subprocessing agreement with the other processor, the Processor must ensure that the provisions agreed between the Controller and the Processor and, if applicable, supplementary instructions from the Controller also apply in full to the other processor. This includes, in particular, the obligation to maintain confidentiality pursuant to Sect. 11 of this Agreement, the guarantee of technical and organizational measures to ensure an appropriate level of processing security, participation in the processing of inquiries from data subjects and the fulfilment of the agreed documentation obligations. In the subprocessing agreement, the details specified in Sect. 2,3,4 and 5 of this Agreement shall be specified in such a way that the responsibilities of the Processor and the other processors are clearly delimited. If more than one other processor is used, this also applies to the responsibilities between these other processors.

(6) The Processor shall regularly verify the other processor's compliance with its obligations. In particular, the Processor shall check in advance and on a regular basis during the term of the agreement that the other processor has taken the guaranteed and required technical and organizational measures to protect personal data. The result of the control must be documented by the Processor and transmitted to the Controller upon request.

Sect. 11 Confidentiality

(1) The Processor is obliged to maintain confidentiality when processing data for the Controller.

(2) The Processor guarantees that it is aware of the applicable data protection regulations and familiar with their application.

(3) In fulfilling its obligations under this Agreement, the Processor undertakes to employ only employees or other agents who are committed to confidentiality in the handling of personal data provided and who have been appropriately familiarized with the requirements of data protection. Upon request, the Processor shall provide the Controller with evidence of the confidentiality commitments.

(4) Insofar as the Controller is subject to other confidentiality provisions, it shall inform the Processor accordingly. The Processor shall oblige its employees to observe these confidentiality rules in accordance with the requirements of the Controller.

Sect. 12 Technical and organizational measures, Sensitive Data

(1) The technical and organizational measures described in **Annex II** are agreed upon as binding.

(2) The Processor shall observe the principles of due and proper data processing in accordance with Art. 32 in conjunction with Art. 5 (1) GDPR. It guarantees the contractually agreed and legally prescribed data security measures. It will take all necessary measures to safeguard the data and the security of the processing, in particular taking into account the state of the art, as well as to reduce possible adverse consequences for the affected parties. Measures to be taken include, in particular, measures to ensure appropriate pseudonymization and encryption, measures to protect the confidentiality, integrity, availability and resilience of systems and measures to ensure continuity of processing after incidents. In order to ensure an appropriate level of processing security at all times, the Processor will regularly evaluate the measures implemented and make any necessary adjustments. The Processor will notify the Controller in advance of any significant changes to the technical and organizational measures.

Sect. 13 Deletion and Return of Personal Data

(1) Copies or duplicates of the data processed on behalf of the Controller shall never be created without the knowledge of the Controller, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work and upon request by the Controller, at the latest upon termination of the Principal Agreement, the Processor shall hand over to the Controller or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

Sect. 14 Remuneration

The Processor's remuneration is specified in the Principal Agreement.

Sect. 15 Liability/Indemnification/Contractual penalty

(1) The Processor shall be liable to the Controller for any and all loss or damage culpably caused in the performance of the services under the Principal Agreement or by a breach of applicable statutory data protection obligations on the part of the Processor, its employees or parties commissioned by it to implement the Principal Agreement.

(2) Within the context of their contractual relationship under the Principal Agreement, the Controller and the Processor shall be obligated to compensate data subjects for damage caused by them arising from the unlawful or improper processing of their data within the meaning of the GDPR or other data protection provisions as stipulated in Art. 82 GDPR. As regards the parties inter se, the Processor shall indemnify the Controller against any and all claims for damages asserted against the Controller based on the Processor's culpable breach of its own obligations under data protection regulations or on non-observance of instructions lawfully issued by the Controller. The Controller shall bear the burden of proof for non-compliance of Processor with Processor's

obligations under data protection regulations and for non- compliance with instructions lawfully issued by the Controller. The Controller shall also bear the burden of proof that the damages are due to the Processor's breach of duty and that Processor was responsible for such breach.

Sect. 16 Miscellaneous

(1) In case of contradictions between the provisions contained in this Agreement and provisions contained in the Principal Agreement, the provisions of this Agreement shall prevail.

(2) Amendments and supplements to these provisions must be in writing and expressly declare that the provisions in this Agreement are being changed and/or supplemented. The foregoing also applies to the formal requirement itself.

(3) This Agreement is exclusively subject to the laws as set forth below:

Contracting Entity is:	**Governing law:**	**Courts with exclusive jurisdiction are located in**
Dealfront Finland Oy	the laws of Finland under exclusion of the UN Sales Convention and without giving effect to any principles of conflicts of law	Helsinki, Finland
All other contracting entities	laws of the Federal Republic of Germany under exclusion of the UN Sales Convention and without giving effect to any principles of conflicts of law	place of the registered office of Dealfront Group GmbH

(4) In the event that access to the data which the Controller has transmitted to the Processor for data processing is jeopardized by third-party measures (measures taken by an insolvency administrator, seizure by revenue authorities, etc.), the Processor shall notify the Controller of such without undue delay.

Schedule of Annexes

Annex I List of Acceding Parties

Annex II Technical and organizational measures taken by the Processor to ensure the security of processing

Annex I

List of Acceding Parties

Controller(s) (Identity and contact details of the controller(s) and, where applicable, of the respective controller's data protection officer

1. Company name: Customer listed in the applicable order or registration form

   Address: Address listed in the applicable order or registration form

   Contract person's name, position and contact details: Contact person listed in the applicable order or registration form

This Annex I shall automatically be deemed executed when the customer agrees to the applicable order or registration form.

Processor(s) (Identity and contact details of the processor(s) and, where applicable, of the respective processor's data protection officer

1. Company name: Dealfront entity listed in the applicable order or registration form

   Address: Dealfront address listed in the applicable order or registration form

   Contract person's name, position and contact details: Henri Markkanen, DPO, dpo@dealfront.com

Annex II

Technical and organizational measures to ensure the security of processing

The Processor guarantees that the following technical and organizational measures have been taken:

A. Encryption measures

Measures or operations in which a clearly legible text/information is converted into an illegible, i.e. not easily interpreted, character string (secret text) by means of an encryption method (cryptosystem).

Description of the encryption measure(s):

- Data Encryption in transit and at-rest

B. Measures to ensure confidentiality

1. **Physical access control**

Measures that physically deny unauthorized persons access to IT systems and data processing equipment used to process personal data, as well as to confidential files and data storage media.

Description of physical access control:

- Individual access control on need-to-know basis
- All workstations are encrypted, antivirus software and screenlock in place
- Monitoring the entrances to the facilities
- Doors to the server rooms/cabinets and other security areas are always closed and access is regulated
- Visitors or external service providers are admitted individually
- The disposal or reusing of equipment is regulated
- Guidelines for clean desk and screen locking are implemented and observed

2. **Logical access control**

Measures to prevent unauthorized persons from processing or using data which is protected by data privacy laws.

Description of logical access control system:

- Detailed access and actions logging in all application infrastructure
- Technical monitoring 24/7

3. **Data access control**

Measures to ensure that persons authorized to use data processing systems can only access personal data according to their access rights, so that data cannot be read, copied, changed or removed without authorization during processing, use and storage.

Description of data access control:

- Detailed access and actions logging in all application infrastructure
- All workstations are encrypted, antivirus software and screen lock in place
- Individual access control on need-to-know basis
- Password policy in place, MFA enforced where applicable, SSO used widely

4. **Separation rule**

Measures to ensure that data collected for different purposes are processed separately and separated from other data and systems in such a way as to preclude the unplanned use of such data for other purposes.

Description of the separation control process:

- Authorization concepts
- Encrypted storage of personal data

C. Measures to ensure integrity

1. **Data integrity**

Measures to ensure that stored personal data cannot be corrupted by means of a malfunctioning of the system.

Description of data integrity:

- Continuous vulnerability scanning and penetration testing
- Technical monitoring 24/7

2. **Transport control**

Measures to ensure that the confidentiality and integrity of data is protected during transmission of personal data and transport of data carriers.

Description of transport control:

- Transmission of data via encrypted data networks or tunnel connections (VPN)
- Comprehensive logging procedures

4. **Input control**

Measures to ensure that it can be subsequently verified and ascertained whether and by whom personal data have been entered or modified in data processing systems.

Description of the input control process:

- Logging of all system activities

D. Measures to ensure availability and resilience

1. **Availability control**

Measures to ensure that personal data are protected against accidental destruction or loss.

Description of the availability control system:

- Data backup procedure
- Uninterrupted power supply
- Fire alarm system
- Air conditioning
- Alarm system
- Emergency plans
- No water-bearing pipes above or near server rooms

2. **Quick recovery**

Measures to ensure the ability to quickly restore the availability of and access to personal data and used systems in the event of a physical or technical incident.

Description of the measures for quick recovery:

- Data backup procedure
- Regular tests of data recovery
- Emergency plans