

Legal Kit

February 2026

We understand that when it comes to choosing a business intelligence solution for your organisation's data needs, there are many factors to consider, especially with regard to legal compliance.

That's why we've put together this comprehensive legal kit to provide your legal department with all the information they need to vet our services and products and to make an educated decision.

Please note that we do not provide legal advice. This document is solely meant to provide a comprehensive overview of the respective terms and regulations governing our relationship with our customers.

What's inside

- A. [General Terms and Conditions \(GTC\)](#)
 - B. [Data Processing Agreement – Inside EEA](#)
 - C. [Privacy Notice for Customers and Users of Leadfeeder](#)
 - D. [Privacy Information for Data Subjects](#)
 - E. [AI Features at Leadfeeder](#)
-

A

**General Terms and Conditions
(GTC)**

General Terms and Conditions (GTC)

1. Definitions

Leadfeeder (as defined below) offers lead generation tools and sales intelligence services for B2B companies. In these General Terms and Conditions ("GTC"):

- a) "Agreement" means the Order, these GTC, the Data Processing Agreement (if applicable) and all and any specification agreed upon (e.g., selected Plan) between Leadfeeder and Contracting Company and their respective User(s).
- b) "Contracting Company" means the party to whom Leadfeeder is to provide its products or services pursuant to the Order. If a Contracting Company includes more than one legal or natural person, the obligations imposed upon each shall be joint and several.
- c) "Leadfeeder" means Dealfront Group GmbH and its affiliates, including but not limited to Dealfront Germany GmbH and Dealfront Finland Oy, (in the following also referred to as "we", "our", or "us")
- d) "Order" means any registration (either paid subscription or free trial), signed quote, order confirmation or sign-up through a web interface indicating the products and services ordered, to be ordered or currently used by Contracting Company and respective User(s).
- e) "Queries" means queries, searches, API-calls or any specific configuration Users employ within our Services in order to get Results.
- f) "Result" means any company data, contact information, lead or other information or data provided by the Services as an outcome to a Query.
- g) "Services" means the Leadfeeder web software, platform, products and any services which Leadfeeder provides to Contracting Companies and Users, through its websites, portals, interfaces (APIs), integrations and further internet based services.
- h) "Sources" may include but are not limited to company websites, news portals, online media and public databases, such as commercial registers, blogs, forums, consumer portals or social networks.
- i) "User" means the natural person(s) who are using the Services after (i) either registering themselves as well as a Contracting Company, or (ii) being invited on behalf of or by a Contracting Company.

2. Scope of Application and Definitions

- 2.1. These GTC apply to all Services which Leadfeeder provides to Contracting Companies and Users ("you"). By purchasing, using or otherwise accessing any of the Services, you agree to be bound by the Agreement.
- 2.2. These GTC take effect the earlier of (a) the use or access of the Services, or (b) the execution of an Order and supersede all prior communications between you and Leadfeeder, unless expressly agreed otherwise in writing (text form sufficient).
- 2.3. The Services are offered for professional purposes only, i.e. for natural or legal persons who or which, when entering into a legal transaction, act in exercise of a business. You confirm that the use of the Services is intended for commercial or professional purposes only.
- 2.4. Leadfeeder does not accept any other terms (e.g., additional and ancillary provisions such as guarantee commitments, procurement terms or assurances) with regard to the provision of the Services, unless agreed in writing (text form sufficient) by an authorized Leadfeeder representative.

3. Content & Use of Services

- 3.1. Leadfeeder provides its Services to Contracting Companies and Users in accordance with the Agreement. The Services will be provided as they exist and may be updated and amended throughout the Term (as defined below in section 8).
- 3.2. Leadfeeder Services can be used without sharing personal data with us. However, if you (a) are implementing Leadfeeder technologies in your systems or website by means of which you share personal data with us, or (b) share personal data with us in order to be processed on your behalf, the data processing agreement (accessible under <https://www.leadfeeder.com/privacy/>, "Data Processing Agreement")) accompanies these GTC and sets forth additional terms of our Agreement that apply solely to personal data processed on your behalf as part of providing the Services to you.
- 3.3. With regard to any other Services, Leadfeeder processes personal data for its own purposes and not on behalf of you. Therefore, Leadfeeder does not enter into a data processing agreement with regard to all other processing activities not subject to Sec. 3.2 and performed as part of our Services. Additional information can be found here in Leadfeeder's privacy notice (<https://www.leadfeeder.com/privacy/>).

- 3.4. In the event Leadfeeder offers specialized or third party Services to you, the provision of such Services may be dependent on your consent to additional terms and conditions prior to the activation of such Services.
- 3.5. You acknowledge and understand that the content and scope of Services and Results, including the selection of Sources, are subject to change and are expected to change over time. To improve the swiftness and efficiency of certain Services, Leadfeeder may expand, modify, or supplement its offering at any time and in Leadfeeder's sole discretion.
- 3.6. You acknowledge that all Results are compiled through automated systems at a large scale. Leadfeeder is not responsible for the completeness, relevance or correctness of the Results and does not have any influence on or control over the Results which are served from Sources.
- 3.7. As Leadfeeder processes and delivers Results automatically without manual checks, you acknowledge that the Results may contain incorrect, harmful, illegal, offensive, or otherwise inappropriate or unsuitable texts, images, or works. Such content shall not be considered a defect of the Services.
- 3.8. To the extent Leadfeeder adds additional information to data provided by you as part of the Service, you acknowledge and agree that Leadfeeder is not responsible for ensuring that the Results are fit for your intended purpose or use. It is your own responsibility to ensure the accuracy and suitability of the respective Results provided to you.
- 3.9. Leadfeeder is entitled, in each case, to reject specific Queries or the display of certain Results if Leadfeeder cannot reasonably execute or display these for technical and/or legal reasons.

4. License

- 4.1. Leadfeeder grants to the Contracting Company a non-exclusive, non-transferable license to use the Services in accordance with Agreement, determining, in particular, the type of use, the number of Users, and the scope of access granted to Users.
- 4.2. With the exception of the following, the Contracting Company is not entitled to lease, resell, or otherwise transfer the Services or Results to third parties:
 - a) Use of the Services may only take place within the Contracting Company's organization. Use for or within any other enterprises (including affiliated companies) and/or publishing of Results is only permitted with prior consent of Leadfeeder in text form.
 - b) Transmission of Results or granting access to the Services to external service providers (agencies, call centers, etc.) is only permitted for uses where these providers directly support the Contracting Company for its own purpose and their use is restricted by means of time, access and region to the Contracting Company's project.
- 4.3. Contracting Company shall be entitled to assign any User that is a natural person or employed by or working for the Contracting Company a named user license ("Seat") up to the number indicated in the Order. For the avoidance of doubt, Leadfeeder is not required to provide its Services to unlicensed Users, i.e., if the number of Users exceeds the number of available Seats.
- 4.4. Leadfeeder provides all Users with an online working environment, which Users may a) access directly by entering their login and password or b) use indirectly via a software interface permitting authorized access.
- 4.5. Contracting Company acknowledges and agrees that Leadfeeder offers different service packages ("Plans"), composed of different data sets, products, features and actions ("Actions") that can be performed within such Plans by Users.
- 4.6. Actions include (but are not limited to) the download/export of data, revealing of leads or contact details, syncing data to an external system or sending API calls.
- 4.7. Depending on the Agreement and number of Results affected, Contracting Company acknowledges that certain Actions a) might be performed with or without cost or b) will consume credits ("Credits"). In case of any additional charge, Leadfeeder will inform the Contracting Company accordingly.
- 4.8. As per its Order the Contracting Company will be entitled to a certain number of Credits to be used by its Users during the Term. If all Credits have been used, certain Actions might not be available anymore until the renewal of the Term. Unused Credits will expire at the end of each Term.
- 4.9. Overuse of Credits or Seats above the limits of the Order can result in additional charges. Leadfeeder will inform the Contracting Company about such overuse and additional charges accordingly.
- 4.10. The Contracting Company will choose a restrictive set of configurations and inform its Users accordingly so that it will be able to avoid unintended Credit consumption or charges.

- 4.11. Contracting Company acknowledges and agrees that Leadfeeder may upon renewal adjust the applicable Plan to reflect overuse (according to Section 4.9) which has occurred during the Term or can be reasonably expected during the upcoming Term. Leadfeeder will inform you about such adjustments accordingly.
- 4.12. Leadfeeder provides the Services on all calendar days and ensures that the Services have an availability of 99% in the annual average. The operating time shall exclude periods in which maintenance activities take place, provided that such maintenance has been announced at least 24 hours prior to commencement. Operational disruptions beyond Leadfeeder's control (e.g., disruptions caused by *force majeure* or unrelated third-parties) are excluded from the operating times. Exclusions from operating times in accordance with Section 4.12 shall not be treated as the Services being unavailable.

5. User Obligations

- 5.1. Users are responsible for the confidentiality of their authentication credentials, such as logins, passwords, tokens, or API keys and shall not pass these on to third parties. They are responsible for misuse of such credentials resulting from a failure to comply with these obligations.
- 5.2. Contracting Companies and Users shall exercise due care during their use. This means, in particular that:
- a) Users shall not exploit any potential programming errors to the detriment of Leadfeeder and shall immediately report errors, bugs and any shortcomings relevant for IT security to Leadfeeder when Users become aware of such occurrences.
 - b) Users shall not unduly interfere with the Services or Leadfeeder's infrastructure.
 - c) Users must not use Services for illegal purposes.
 - d) Users shall ensure not to spread viruses, worms, or other malicious code via the Services.
 - e) Users shall not access Services and databases of Leadfeeder by means of automated scripts (e.g., through "screen scraping"), except if such access has been expressly provided for in the Agreement and is done via interfaces designed and/or made available for such a purpose by Leadfeeder.
 - f) Users shall not mislead other Users or attempt to gain access to profile and personal data of other Users or otherwise jeopardize the privacy and security of any data stored by Leadfeeder.
 - g) Users shall not permit direct or indirect access to or use of any Services in a way that circumvents a usage limit included in the Agreement.
 - h) Users shall not copy a Leadfeeder Service or any part, feature, function, or user interface thereof or frame or mirror any part of any Services.
 - i) Users shall not access any Services or monitor the availability, performance or functionality of these Services in order to build a competitive product or service, or for any other benchmarking for competitive purposes.
- 5.3. If there is evidence or a serious suspicion that a User has committed a breach of Sections 5.1. or 5.2., or has attempted a breach, Leadfeeder may, with immediate effect, exclude the User from the further use of the Services until the matter has been reasonably resolved or, if the matter cannot be reasonably resolved, suspend such User and/or the respective Contracting Company's account.
- 5.4. You acknowledge and understand that you are solely responsible for complying with the laws, rules and regulations applicable to your use of the Results, e.g. data protection and e-privacy regulations. Leadfeeder is in no position to legally assess and/or influence your use of Results (e.g., if and how to use address or contact data).

6. Rights and Ownership

- 6.1. You agree and acknowledge that certain Results may be subject to third-party rights and licenses (e.g., copyright or trademark protected) and that Leadfeeder does not grant or manage such third-party rights or licenses. Copyrights, patent rights, trademark rights and all other intellectual property rights related to the provision of the Services itself shall remain with the respective owners of such rights. .
- 6.2. If you provide data to Leadfeeder, e.g. for the purpose of updating or enriching such data, you grant Leadfeeder a non-exclusive right to process such data as necessary, and to perform the Services pursuant to the Agreement.
- 6.3. Leadfeeder will keep any personal data and other information provided by the Contracting Company (such as User details) confidential, and will only make the data available as necessary to complete or perform Leadfeeder's Services pursuant to the Agreement. Leadfeeder will undertake reasonable effort to delete the received data and information upon your request.
- 6.4. You acknowledge and agree that aggregated and anonymized data may be used in order to improve or develop our Services.

7. Support

Leadfeeder will provide you with assistance and support in accordance with your Order and Plan selected. Leadfeeder's Customer Support personnel will be available from 9:00 a.m to 6:00 p.m. (Central European Time) (Monday - Friday, except for bank holidays) in order to swiftly respond to inquiries. Different support schedules may be available to you depending on your time zone and region.

8. Orders, Payment, Term and Termination

- 8.1. The initial duration of the Agreement with Contracting Company, as set forth in the Order, or any subsequent renewal period(s) are herein referred to as "Term".
- 8.2. The Contracting Company may only terminate the Agreement with effect at the end of each Term. Extraordinary termination rights and the right to termination for just cause remain unaffected. For any Agreement with a Term of one (1) year or longer, a cancellation of the renewal has to be received by Leadfeeder at least 30 days prior to the last day of the Term. Any Agreement that has not been canceled in time will automatically renew for another Term equal to the length of the last Term.
- 8.3. The fees for the initial Term apply as set forth in the Order. All prices are quoted in EUR or USD (as the case may be) and exclude statutory VAT or sales tax (as applicable). With regard to any subsequent Terms, any increase of prices will be limited to a maximum of 5% per year. Leadfeeder will inform the Contracting Company about such an increase accordingly.
- 8.4. The fees for every Term are due annually up front (unless otherwise stated in the Order). Leadfeeder will issue an invoice upon the earlier of (a) receipt of payment or (b) order confirmation. Payment of any (open) amount is due within fourteen (14) days of receipt of the invoice.
- 8.5. If Contracting Company fails to pay in time, Leadfeeder may, in its sole discretion, take any or all of the following actions:
 - a) restrict or suspend User access to the Services until all past-due payments are made,
 - b) terminate the Agreement, or
 - c) engage a third party to collect the outstanding amounts.Leadfeeder shall provide Contracting Company with prior notice (email sufficient) (at least one (1) week) before a suspension or termination in accordance with lit. a) or b) above. Restriction or suspension of access to the Services shall have no effect on the Term of the Agreement nor Contracting Company's obligation to pay the respective fees.
- 8.6. You will provide accurate, current and complete information about the legal entity who is the contractual party when placing an Order (all information necessary to identify the legal entity, billing information, bank details and contact persons). You will inform Leadfeeder without undue delay of any relevant changes (e.g., address, billing information and bank details or the relevant contact person).

9. Provision of Services, Assignment of Rights

- 9.1. Leadfeeder is entitled to involve third parties to provide the Services pursuant to the Agreement. Leadfeeder will ensure that such third parties comply with Leadfeeder's obligations under this Agreement, in particular with confidentiality and privacy obligations set forth in these GTC.
- 9.2. Without Leadfeeder's prior written consent (text form sufficient), subject to the provisions section 354a German Commercial Code (HGB) , you may not assign, delegate or otherwise transfer the Agreement (or any rights or obligations under or in connection therewith) to any third parties.
- 9.3. You may only set off claims uncontested or recognized in writing by Leadfeeder or ordered by a court of law.
- 9.4. You may withhold payment or retain possession only to secure claims that are uncontested or ordered by a court of law.

10. Liability and Indemnification

- 10.1. Leadfeeder shall only be liable to you for damages caused intentionally or with gross negligence. This shall not apply if Leadfeeder breaches essential obligations of the Agreement. Essential contractual obligations are those whose fulfillment makes the proper execution of the Agreement possible in the first place and on whose compliance the contractual partner regularly relies and may rely. The liability for a breach of essential obligations shall be limited for each contractual year to the remuneration owed by the Contracting Company in the respective year in which the breach has occurred, this limitation shall not apply if the damage is foreseeable and typical for the Agreement and is typically higher than the annual remuneration.

- 10.2. Leadfeeder assumes no liability for lost profits, consequential or indirect damages, reductions in value of Contracting Company's brand or of its business, frustrated expenses or similar costs.
- 10.3. Any statutory strict liability - in particular liability under the German Product Liability Act as well as statutory warranty liability - shall remain unaffected by the above limitations of liability. The same shall apply to Leadfeeder's liability in case of culpable injury to life, body or health.
- 10.4. The limitations or exclusions of liability according to Sections 10.1. to 10.3. shall also apply to the personal liability of Leadfeeder's employees, representatives, bodies and vicarious agents.
- 10.5. The Contracting Company shall indemnify Leadfeeder from any third party claims arising from an infringement of third-party rights caused by the Contracting Company (e.g., as a consequence of an infringement of Section 6). This includes the reimbursement of reasonable legal costs incurred by Leadfeeder to defend itself against third-party claims. Leadfeeder shall inform the respective Contracting Company of any legal claim raised against Leadfeeder without undue delay. Leadfeeder shall, before entering into any settlement with such a third party, consult with the Contracting Company. If Leadfeeder decides to enter into a settlement without the Contracting Company's consent, Leadfeeder shall bear its own costs resulting from such settlement and in connection with the dispute.

11. Final Provisions

- 11.1. The law governing the Agreement, as well as the jurisdiction in which disputes shall be adjudicated are set forth below, in each case based on the respective contracting Leadfeeder entity:

Contracting Leadfeeder affiliate is:	Governing law:	Courts exclusive jurisdiction located in	with are	Arbitration Proceeding
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		Arbitration Rules of the Finland Chamber of Commerce
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		None

- 11.2. Amendments to the Agreement (including termination notices) must be made in text form; this also applies to a waiver of this text form requirement. Verbal amendments, including ancillary agreements, are invalid.
- 11.3. Should any provisions of the Agreement be or become totally or partially invalid or unenforceable, or if the Agreement contains gaps, the validity or enforceability of the other provisions of the Agreement shall not be affected thereby. In place of the invalid, unenforceable or missing provisions a valid and enforceable provision which the parties to the Agreement would have agreed upon taking into account of the economic purpose of the Agreement if they had, at the conclusion of the Agreement, been aware of the invalidity, unenforceability or the absence of the relevant provisions, shall be deemed to be agreed between the parties.

12. Right to make amendments to the GTC

Leadfeeder has the right to amend these GTC, to adapt the GTC to changes of applicable laws, or to the services Leadfeeder offers. In this event, Leadfeeder will inform Contracting Company of the

amendment in text form reasonably in advance. The amendment is incorporated and applies unless Contracting Company objects in text form within two (2) weeks of receipt of the notification about the amendment. If the Contracting Company exercises its right of objection, the contract will continue to apply based on the GTC without the amendment. In this case, any rights of the parties to terminate the contract remain unaffected. In case of a timely objection, Leadfeeder reserves the right to terminate the Agreement extraordinarily with a notice period of one (1) month.

B

**Data Processing Agreement –
Inside EEA**

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) Data processing

- 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@leadfeeder.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@leadfeeder.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.leadfeeder.com/privacy/> 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 dba Leadfeeder Finland	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 dba Leadfeeder Group

- (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: Leadfeeder entity listed in the applicable order or registration form

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

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



**Privacy Notice for Customers
and Users of Leadfeeder**

Privacy Notice for customers and users of Leadfeeder pursuant to Article 13 of the EU General Data Protection Regulation (GDPR)

(February 2026)

Introduction

Dealfront Group GmbH dba Leadfeeder Group and its affiliates, including but not limited to Dealfront Germany GmbH and Dealfront Finland Oy, (in the following "Leadfeeder", "we", "our", "us") takes the protection of your personal data very seriously. With this privacy notice ("**Privacy Notice**"), we want to inform the public and data subjects about the nature, extent, and purpose of the personal data collected, used, and processed by us pursuant to **Article 13 of the GDPR** and inform data subjects about their rights.

Leadfeeder also operates one of the largest search engines/crawlers in the world for the provision of its services. Data and information that are publicly available on the Internet are thereby automatically collected. This processing may also affect personal data that is not collected directly from the data subject. Therefore, we have also developed the document "**Privacy Information for Data Subjects**" to inform data subjects pursuant to **Article 14 of the GDPR**.

(see privacy information for data subjects available here <https://www.leadfeeder.com/privacy/> .

This Privacy Notice is structured as follows: In the **overview (A)** we provide an overview of our privacy practices related to our services and our platform as well as your rights. In the second part, we explain in detail the **processing operations** carried out by us (**B**), their respective data scope, purpose, and associated legal bases. In the third part you receive information about how and when we share data with third parties (**C**) .

Leadfeeder has implemented numerous measures to ensure the protection of personal data. For more information, visit our **online privacy centre** at: <https://www.leadfeeder.com/privacy/>).

A) Overview

In this Privacy Notice, we use the terms defined in Article 4 of the GDPR: personal data, data subject, processing, restriction of processing, pseudonymisation, controller, processor, recipient, third parties, and consent. Since Leadfeeder is a company specialising in data processing in the Business-to-business (B2B) sector, we have also defined other terms that are intended to help you understand the following explanations:

Publicly available data means all data, information, and entries which are accessible or viewable for everyone via **public sources** directly (e.g. by a link) or indirectly (e.g. by a query). Examples of public sources are: websites, news portals, press or blog articles, publicly shared posts and profiles from social media, as well as public databases of specialist portals, job boards, forums, the commercial register, the Federal gazette, or Wikipedia.

Business related data is data that is associated with a business or an organisation. For example, a change of management notification may include the name of the company and the manager; a press release may include the contact of the press representative; include a public social media profile (e.g. LinkedIn or XING) with the name of the employer and mention a product rating of the manufacturer concerned.

A1) The controller / data protection officer

For the purposes of this Privacy Notice, the data controller of the personal data collected, processed and stored through the platform, or through the communication platforms related thereto, is Dealfront Group GmbH, with registered office at Durlacher Allee 73, D-76131 Karlsruhe, Germany (hereinafter "Data Controller").

You can always contact the Data Controller by e-mail at: privacy@leadfeeder.com

For any questions regarding the data processing carried out in the context of using the platform or our services and products, may also contact the group data protection officer ("DPO") designated by Leadfeeder at any time by email: dpo@leadfeeder.com

A2) How and when do we obtain personal data from you?

Leadfeeder may collect personal data from you in the following circumstances:

- Data collected by automated means such as cookies or similar technologies when you visit the **Leadfeeder website or use Leadfeeder's services** (for additional information see here: <https://www.leadfeeder.com/cookies-and-tracking/>).
- Data collected from you when you **create an account, complete a form, contact us directly or subscribe to our services**
- Data submitted when using our services (e.g., prompts or parts of prompts that you enter while using our AI features)
- Data you provide us **about others** in your organisation or data that others have provided about you.

A3) Legal bases for data processing?

We process personal data in accordance with the applicable data protection regulations, namely the GDPR:

a) for the fulfilment of contractual obligations pursuant to Article 6 para. 1 lit. b of the GDPR

We process your personal data in the context of the performance of our contracts with our customers, users and/or applicants or for the implementation of pre-contractual measures. The purposes of the data processing are based primarily on the specific product and may include, but are not limited to, general communication about our services, analysis and consulting for the purpose of creating an offer, support or consulting, the provision of online software, or the processing of application documents.

b) if we have a legitimate interest pursuant to Article 6 para. 1 lit. f of the GDPR

If necessary, we may process your personal data prior to the initiation or fulfilment of a contract or beyond if we have a legitimate interest in doing so. Legitimate interests include:

- Operation of our website and optimisation of our offers on the Internet
- Analysis and optimisation of customer journeys and procedures
- Advertising, marketing, and sales, insofar as you have not objected to the use of your data for this purpose
- Market and opinion research, insofar as you have not objected to the use of your data for this purpose
- Asserting legal claims and defence in legal disputes

- Ensuring IT security and IT operations; elimination of errors and malfunctions
- Prevention of crime
- Measures for business and risk management and controlling
- Further development of services and products
- Event management

c) on the basis of your consent pursuant to Article 6 para. 1 lit. a of the GDPR

Certain processing activities (e.g. the receipt of newsletter, downloads of whitepapers or other materials) are based on your consent. Consent given can be revoked at any time.

d) in case we are legally required to process your data (Art. 6 para. 1 lit. c of the GDPR)

Insofar as Leadfeeder is required by law to process certain data, personal data may also be affected.

A4) Deletion and retention periods

We process and store your personal information as long as it is necessary for the fulfilment of our contractual and legal obligations. It should be noted that our business relationship is a continuing obligation, which is intended for several years. If the data are no longer required for the fulfilment of contractual or legal obligations, these are regularly deleted unless the consent given also extends beyond the end of the contract or a balance of interests comes to the conclusion that a legitimate interest of Leadfeeder exists for further storage which outweighs the interests of the data subject.

A5) How do we share the data?

We may share data as follows:

- within the Leadfeeder group in order to provide you the requested services and products
- with service providers that perform services or handle transaction on our behalf
- other parties when we are required to do so by law or as necessary to protect our rights, or in the context of corporate transactions.

A6) Rights of data subjects

You may be entitled to exercise some or all of the following rights:

1. require (i) information as to whether your personal data is retained and (ii) access to and/or duplicates of your personal data retained, including the purposes of the processing, the categories of personal data concerned, and the data recipients as well as potential retention periods;
2. request rectification, removal or restriction of your personal data, e.g. because (i) it is incomplete or inaccurate, (ii) it is no longer needed for the purposes for which it was collected, or (iii) the consent on which the processing was based has been withdrawn;
3. refuse to provide and – without impact to data processing activities that have taken place before such withdrawal – withdraw your consent to processing of your personal data at any time;
4. **object, on grounds relating to your particular situation, that your personal data shall be subject to a processing. In this case, please provide us with information about your particular situation. After the assessment of the facts presented by you we will either stop processing your personal data or present you our compelling legitimate grounds for an ongoing processing;**

5. take legal actions in relation to any potential breach of your rights regarding the processing of your personal data, as well as to lodge complaints before the competent data protection regulators;
6. require (i) to receive the personal data concerning you, which you have provided to us, in a structured, commonly used and machine-readable format and (ii) to transmit those data to another controller without hindrance from our side; where technically feasible you shall have the right to have the personal data transmitted directly from us to another controller; and/or
7. not to be subject to any automated decision making, including profiling (automatic decisions based on data processing by automatic means, for the purpose of assessing several personal aspects) which produce legal effects on you or affects you with similar significance.

You may (i) exercise the rights referred to above or (ii) pose any questions or (iii) make any complaints regarding our data processing by contacting us under: privacy@eadfeeder.com.

A7) Non-use of "profiling"

Profiling describes a type of automated processing of personal data that consists in assessing, analysing, or predicting certain personal aspects such as health or personal preferences and which produces legal effects on the data subject. Leadfeeder does not use such profiling.

B) Comprehensive Privacy Notice

When you visit our platform, use our services or contact us directly, we obtain various types of data related to you and your use of our services. This data may include information that directly identifies you such as your name or contact details as well as identifiers (e.g. your IP address) or cookie-level data that may indirectly identify you. The information we obtain generally consists of (B1) automatically collected data about your interactions with our platform and our services or (B2) data you provide us about yourself or we directly collect from you or (B3) data you provide us about others in your organisation or (B4) data that others have provided us with about you.

B1) Information automatically collected

If you are visiting our websites or accessing our applications, we collect the following information provided by your browser or mobile device: pages accessed, time of visit and time of last visit, frequency of recurring visits, IP address, name of the owner of the IP address, domain or provider of IP address, referrer (site/service/queries that led you to our website), browser information, device information.

Such data is collected and processed for different purposes such as:

- to deliver the contents of our websites and apps correctly,
- to optimise the content of our website, enhance user experience and to advertise our services and products,
- to ensure the permanent functioning of our systems and the technology of our website,
- to provide law enforcement with information necessary for prosecution in the event of a cyber-attack, and
- to facilitate the access to and the use of our services.

The legal basis for the processing of the data collected in this way is Article 6 para. 1 lit. f (legitimate interest in aforementioned purposes) as well as Art. 6 (1) lit. b GDPR (performance of

a contract if such processing is necessary in order to provide you access to our services and products via the platform).

To collect such data, we use cookies and similar technologies. For more information about cookies and other technologies used by us please see here: <https://www.leadfeeder.com/cookies-and-tracking/>

B2) Information provided by you

If you contact Leadfeeder, if you send us an email or inquiry, or if you wish to use certain offers and services of our company, the processing of your personal data may be necessary. Examples include:

- You request a whitepaper, a price list, or another document.
- You sign up to receive our newsletter.
- You contact our service team or our sales team.
- You apply for one of our job advertisements.
- You contact us during a lecture, trade fair or similar event.
- You are using software or an app provided by us and sharing your data with us in the course of using the software or app.

In such cases, the following personal data may be collected directly from you:

- name, job title, affiliation
- email address, phone number or other contact details
- billing and payment information
- user information from integrated tools
- messages with our support and sales teams
- metadata related to your request or inquiry
- search queries and results of such queries
- other data uploaded by you to our systems

In these cases, we process your personal data for the following purposes:

B2.1) To provide you with our services and products (Art. 6 (1) lit. b GDPR)

Such services may include:

- processing your requests and inquiries on our platform,
- deliver platform/website content to you
- providing customer assistance and IT support, and/or
- providing online learning content to you.

B2.2) To communicate with you

We may communicate with you via different means, such as by post, email, personal contact, messenger or chat systems or social media. The communication purposes may include:

- sending you service-related messages and notifications (Art. 6 (1) lit. f GDPR (our legitimate interest in marketing and sales of our products and services));
- sending you our newsletter (Art. 6 (1) lit. a GDPR);
- responding to your questions or addressing your requests (Art. 6 (1) lit. b GDPR);
- sending you materials you have requested (Art. 6 (1) lit. b GDPR);

- sending you payment or billing related information (Art. 6 (1) lit. b GDPR) and to fulfil our legal obligations regarding accounting and bookkeeping (Art. 6 (1) lit. c GDPR in conjunction with Sec. 257 (4) of the German Commercial Code)
- in conjunction with job applications and the application procedure (Art. 6 (1) lit. b GDPR and Art. 6 (1) lit. c GDPR).

B2.3) To protect our rights or the rights of others

This may include activities like:

- Detecting and preventing fraud or illegal activities or misuse of our services (Art. 6 (1) lit. f GDPR);
- Backing up our systems (Art. 6 (1) lit. f GDPR (our legitimate interest in IT security and recovery of our data));
- Performing audits, testing, assessments or other troubleshooting activities (Art. 6 (1) lit. f GDPR (our legitimate interest in IT security and recovery of our data));
- Complying with and enforcing applicable legal requirements (Art. 6 (1) lit. c GDPR);
- Collecting and recovering money owed to us (Art. 6 (1) lit. b GDPR).

B2.4) For advertising and marketing activities (Art. 6 (1) lit. f (legitimate interest in marketing our products and services) GDPR

These activities include:

- Developing, managing and executing advertising and marketing campaigns, promotions and offers related to our services, products and our platform;
- Interest-based advertising. We use online and offline information obtained from you for interest-based advertising and marketing activities. To learn more about this, please also refer to our cookie notice.

B3) Information provided by you about third parties

You may provide information about other people, such as the name and email of a contact who you want to invite as a user to our services and products. These third parties may include team members or colleagues in your organisation or external agencies with whom you are, in accordance with our terms and conditions, authorised to give access to our services. Such information may include the name, job title and contact information. Do not give us information about others unless you are authorised or have their permission to do so. We will use their information for the purposes described in this Privacy Notice.

B4) Information provided about you by third parties

Others may have provided us with information about you, such as your name and contact details either because they wanted to invite you as a user to our services or products or in the context of verifying your information for the use of or in the context of our services. We inform and ask anyone sharing information with us not to give us such information about others unless they are authorised or have the respective data subjects permission and knowledge to do so. We will use your information for the purposes described in this Privacy Notice.

C) Data Sharing

C1) Recipients

We may share data with the following recipients:

C1.1) Leadfeeder group

In order to offer you comprehensive support and to ensure an ongoing high quality of our services and products, Dealfront Group GmbH relies on the assistance of Dealfront Germany GmbH and Dealfront Finland Oy (each a "Joint Controller" and together the "Joint Controllers"). The legal basis for such processing is Art. 6 (1) lit. b as well as Art. 6 (1) lit. f (legitimate interest in providing and improving our services). In accordance with Art. 26 of the GDPR, the Joint Controllers have entered into a Joint Controller Agreement stipulating in a transparent manner their respective responsibilities with regard to compliance with their obligations under the GDPR. The essential content of the Agreement is available here: <https://www.leadfeeder.com/privacy/>.

In addition, we may share data with other affiliates for marketing or customer support purposes. Such processing activity is based on Art. 28 GDPR in conjunction with a data processing agreement concluded with the respective affiliates.

C1.2) Service Providers

Leadfeeder doesn't sell your data to our service providers. We may share some data with some companies that help us provide our services (for example accounting or job application tools). The legal basis for this data transfer and processing activity is Art. 28 GDPR in conjunction with a data processing agreement concluded with the respective service provider. These service providers are only allowed to use the data shared with them for the specific task they've been hired to do.:

- Web analysis service providers
- Advertising service providers
- Map Services / Maps
- CDN / Content Delivery Networks
- Video Player
- Screensharing / Video Chats
- Tools for communication
- Contact data management / CRM tools
- Job application tools
- Accounting tools
- Cloud Storage and Hosting Providers
- Online learning systems and tools

- Other service and system providers that are necessary for the provision of our services (e.g. tools for the evaluation of data)

As our business operates globally, the service providers mentioned above may occasionally reside outside the jurisdiction where you are based. Further details on this matter can be found below (see C2).

C1.3) Legal Disclosure

We may disclose your personal data to comply with legal requirements and obligations, including court orders or to comply with legitimate requests from law enforcement agencies or regulators.

C.1.4) Change of ownership

We may disclose your personal data in the event of an acquisition, merger or other transaction to the new owner

C2) Cross Border Data Transfers

Leadfeeder operates globally, however, data provided by you and processed by us in the context of providing our services to you is exclusively stored and processed on servers within the European Union.

We also strive to have all our service providers be based within the EEA/EU. Thus, only in rare cases and as part of our data sharing activities mentioned above (see (C)), we may need to transfer your personal data to other countries, including those outside the European Economic Area (EEA), which may have different data protection standards than your country of residence. We will ensure that your personal data is adequately protected when shared with such service providers.

In the event of a transfer outside of the EEA, we use EU Standard Contractual Clauses or (where applicable) rely on adequacy decisions as a safeguard in compliance with Article 46 of the GDPR. For more information on these safeguards, please visit

https://ec.europa.eu/info/law/law-topic/data-protection_en or contact our Group Data Protection Officer at dpo@leadfeeder.com

D) Integration Disclosure

You may choose to use Leadfeeder's Google Ads integration in order to enable you to gain valuable insights into your advertising campaigns and track and improve their effectiveness. We use the Google OAuth protocol for authentication without requiring you to share your login credentials with us. OAuth also allows secure access to the user's data.

Leadfeeder's use and transfer to any other app of information received from Google APIs will adhere to [Google API Services User Data Policy](#), including the Limited Use requirements. Leadfeeder does not transfer information received from Google APIs to any third party or app without your consent. Provided that you have consented, the non-personal data received from Google APIs will be used to provide you with the services as well as for security (e.g. fraud prevention) and analytical purposes.

E) Additional Privacy Disclosures for U.S. Residents

E0) Data Broker Registrations

Dealfront is registered as a data broker with the California Privacy Protection Agency pursuant to California Civil Code SS 1798.99.80 and is in the process of registering as a data broker in the following states: Oregon, Texas and Vermont.

THE ENTITY MAINTAINING THIS WEBSITE IS A DATA BROKER UNDER TEXAS LAW. TO CONDUCT BUSINESS IN TEXAS, A DATA BROKER MUST REGISTER WITH THE TEXAS SECRETARY OF STATE (TEXAS SOS). INFORMATION ABOUT DATA BROKER REGISTRANTS IS AVAILABLE ON THE TEXAS SOS WEBSITE.

The entity maintaining this website is a data broker under Texas law. To conduct business in Texas, a data broker must register with the Texas Secretary of State (Texas SOS). Information about data broker registrants is available on the Texas SOS website.

This section supplements the information contained in this Privacy Notice and applies solely to individuals who reside in the United States (“U.S. Residents”). It is provided to comply with applicable U.S. state privacy laws, including the **California Consumer Privacy Act of 2018 (CCPA)** as amended by the **California Privacy Rights Act (CPRA)**, and similar laws in other U.S. states.

In the event of a conflict between this Section and other parts of this Privacy Notice, this Section shall apply to U.S. Residents.

E1) Definitions

Certain terms used in this Section have the meanings given in applicable U.S. privacy laws:

Personal Information (PI)

Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. This corresponds broadly to the term *personal data* under the GDPR.

Sensitive Personal Information (SPI)

A subset of Personal Information that includes, for example, precise geolocation, account log-in credentials, financial account information, and other categories defined under California law.

Consumer

A natural person who resides in California or another U.S. state with an applicable privacy law.

Sale

The disclosure of Personal Information to a third party for monetary or other valuable consideration.

Sharing

The disclosure of Personal Information to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration.

E2) Sources and Categories of Personal Information

We collect Personal Information from the sources described in Sections A2 and B of this Privacy Notice, including:

- Directly from you (e.g. when creating an account, contacting us, or using our services)
- Automatically from your device or browser when you interact with our platform
- From third parties, such as third-party licensed data providers, publicly available sources including company websites, business partners or other users who provide your details in a business context

In may collect the following categories of Personal Information:

Category of Personal Information	Examples	Business or Commercial Purposes
Identifiers	Name, business email address, phone number, IP address, account identifiers	Providing services, account management, communication, security
Professional or Employment Information	Job title, employer, business contact details	Providing B2B services, customer management, analytics
Commercial Information	Records of services purchased, transaction history	Contract performance, billing, service improvement
Internet or Network Activity	Device data, log data, browsing activity on our platform	Platform functionality, analytics, security, marketing
Geolocation Data (approximate)	Country or region derived from IP address	Security, localisation, analytics
Audio, Electronic or Similar Information	Communications with our support or sales teams	Customer support, quality assurance
Inferences	Business interests or preferences derived from use of our services	Service improvement, analytics, marketing

E3) Sharing of Personal Information / Third Parties to Whom Personal Information is Sold or Disclosed

As described in Section C) Data Sharing of this Privacy Notice, we share Personal Information with our customers, partners, service providers, certain third parties, and where required by law in order to operate our business and provide our services.

E4) Privacy Rights

U.S. Residents, and specifically California Consumers, as well as residents of Oregon, Texas and Vermont have the following rights regarding their Personal Information, subject to certain exceptions:

1. **Right to Know/Access:** The right to request disclosure of the specific pieces of PI we have collected about you, the categories of sources, the business purpose for collecting or selling/sharing it, and the categories of third parties with whom we disclose it.
2. **Right to Delete:** The right to request the deletion of your Personal Information that we have collected, subject to legally recognized exceptions.

3. Right to Correct: The right to request that we correct inaccurate Personal Information we maintain about you.
4. Right to Opt-Out of the Sale or Sharing of PI: The right to direct us not to Sell or Share your Personal Information (including for targeted advertising).
5. Right to Limit Use and Disclosure of Sensitive Personal Information: The right to limit the use of your SPI. As noted above (F3), Leadfeeder already limits the use of SPI to permitted purposes and therefore, does not offer a separate right to limit its use.
6. Right to Non-Discrimination: The right not to receive discriminatory treatment for exercising any of your privacy rights.
7. Right to data portability (receive a copy in a portable format).

We honour opt-out preference signals including the Global Privacy Control (GPC). If your browser or device sends a GPC signal when you interact with our website or services, we treat it as a valid request to opt out of the sale, sharing of your personal information and opt out of the sale and use of your personal data for targeted advertising. This applies automatically, no additional action is required on your part.

We respond to rights requests within 30 calendar days of receipt. We may extend the response period by an additional 30 days where reasonably necessary, and we will notify you of any extension within the initial 30-day period.

We do not sell sensitive personal information as defined under applicable law, including racial or ethnic origin, religious beliefs, mental or physical health data, information about sex life or sexual orientation, biometric data, precise geolocation data, or personal data of minors, regardless of consent. US residents have the right to request that we refrain from processing such sensitive data. To the extent we process (but do not sell) sensitive personal information about US residents, we obtain specific and informed consent, we do not rely on broad, pre-ticked, or buried consent.

E5) How to Exercise Your Rights and Contact Information

To opt out of the sale or sharing of your personal information, you may click the 'Do Not Sell or Share My Personal Information' link in the footer of our homepage, or use the methods listed below. We do not require you to create an account to submit an opt-out request.

You may exercise your privacy rights, especially but not limited to your right to opt out of sale, sharing or licensing of your personal information, by contacting us through one of the following methods:

- **Email:** privacy@leadfeeder.com
- **Online tool:** privacycockpit.leadfeeder.com

You may designate an authorized agent to make a request on your behalf where permitted by law. We may take reasonable steps to verify your identity (and, where applicable, the authority of your agent) before processing your request.

Dealfront participates in California's Data Broker Registry Operating Platform (DROP). California residents may submit deletion requests directly through DROP. Starting August 1, 2026, Dealfront

accesses DROP at least every 45 days to process consumer deletion requests. Upon matching a request, Dealfront deletes the matched personal information and instructs its service providers to do the same. Dealfront does not contact consumers to verify DROP-submitted requests.

E6) Children's Privacy

Leadfeeder's Site and Services are designed for business use and are not intended for or directed to individuals younger than 16 years of age. We do not knowingly collect, maintain, sell, share or process Personal Information from anyone under 16.

We ask that individuals under 16 do not provide any Personal Information through our Site or Services. If we discover that we have inadvertently received Personal Information from a person under 16, we will take prompt steps to delete the information in accordance with applicable legal requirements.

If you believe that a child under 16 may have provided Personal Information to us, please contact us at privacy@leadfeeder.com so that we can investigate and take appropriate action.

E7) Security Program

We have implemented and maintain a comprehensive information and data privacy security program including: (a) administrative, technical, and physical safeguards appropriate to the volume and sensitivity of data we process; (b) employee training on data security and data privacy; (c) oversight and assessment of service providers with access to personal data; (d) procedures to detect, prevent, and respond to security incidents; and (e) annual review and update of the program.

E8) Do NOT Track Signals

Some web browsers offer a "Do Not Track" (DNT) feature that, when enabled, sends a signal to websites requesting that your browsing activity not be tracked. Our technology (Leadfeeder/Dealfront Web Visitor) relies on first-party data collection methods such as our own tracking script and IP address-based company lookups rather than third-party cookies that follow individuals across multiple websites. Our technology is designed to identify the companies visiting a specific website, not to track individuals across the web.

As DNT signals are primarily intended to address cross-site behavioral tracking by third parties, and as there is currently no industry-wide standard for how such signals should be interpreted or honored, we do not alter our data collection practices in response to DNT signals.

You may still exercise your privacy rights as described in this Privacy Notice, including the right to opt out of the sale or sharing of your personal information where applicable under state law.

F) Changes to our Privacy Notice

We reserve the right to amend this Privacy Notice to ensure continued compliance with legal requirements or to reflect changes to our services in the Privacy Notice.

D

**Privacy Information for Data
Subjects**

Privacy Information for Data Subjects

(February 2026)

Dealfront Group GmbH (in the following "Leadfeeder", "we", "our", "us") operates a search engine/web crawler that automatically collects and processes publicly available data and information on the Internet. Our web crawlers visit millions of web pages daily to discover business information relevant to our clients. In certain cases, they may also collect personal information, for example, if your name appears on a public website of your company, then our web crawlers may index that page and display the information on our platform to our customers if they search your company or information in connection with your company.

This Privacy Information for Data Subjects ("Privacy Information") explains how we collect, use and protect your personal data. We are committed to protecting your privacy and ensuring that your personal data is processed in accordance with the European General Data Protection Regulation (GDPR) and applicable data privacy laws.

For information on how we process personal data on our platform or in connection with our services, please refer to <https://www.leadfeeder.com/privacy/>

1. Who is responsible for the data processing and who can I contact?

For the purposes of this Privacy Information, the data controller of the personal data collected, processed and stored by and in conjunction with our search engine is Dealfront Group GmbH, with registered office at Durlacher Allee 73, D-76131 Karlsruhe, Germany (hereinafter "Data Controller").

You can always contact the Data Controller by e-mail at: privacy@leadfeeder.com.

For any questions regarding the data processing carried out in the context of using the platform or our services and products, may also contact Henri Markkanen, the group data protection officer ("DPO") designated by Leadfeeder at any time by email: dpo@leadfeeder.com.

2. Which sources and data do we use?

Similar to popular search engines, we process **publicly available sources** on the Internet, for example,

- Company websites
- Social media platforms
- Public records databases (such as government websites, commercial and trade registers and databases)
- News websites and archives (such as newspapers and news channels)
- Blogs and forums
- Consumer portals and marketplaces
- Special interest sites, job boards or listings
- Directories for patents, trademarks, grants, etc.
- Publicly available online phone directories
- Publicly available academic and research databases
- Publicly available data sets (such as those published by government agencies or academic institutions).

Whenever possible we try to (for each record) store and display a deep-link to the individual sources we may find.

In addition to publicly available data, we also query publicly available data from **open interfaces and services** such as:

- Companies' email servers (MX records)
- Domain databases (Whois records)
- IP databases (e.g. DNS, ripe.net, etc.)
- Geolocation services (e.g. nominatim)

While such services may not produce deep-links we try to indicate if possible when we last fetched a full or partial record.

As a third basis we also **derive additional information** by combining datasets using heuristics, AI and machine learning systems. For example, we may guess your email address, using a combination of publicly available data such as your first and last name with a known pattern for your company's email domain. If we do so, we have implemented accuracy checks in order to ensure the correctness of such data. We are also using data collected through the usage of our systems to optimise such algorithms, e.g. removing data that other users flagged as inaccurate or showing a last seen date for certain records.

Lastly we do act as a data processor for some of our customers with regard to personal data contained in their CRM systems. While we may use such data in an aggregated and anonymized form, such data itself will only be available to a limited subset within the authorised group. As our customer is the data controller, the information duties under the respective data protection laws lie with them. However, if a customer has agreed that we should fulfil certain information duties on their behalf, we may provide the required information to the data subjects concerned.

3. Which personal data do we collect?

Like all search engines Leadfeeder is built to process public unstructured information. So whatever data is accessible about you on the public web may also end up in our indexes. However since the purpose of our service is B2B sales and marketing, we only create structured records of a very specific format. This may result in the following personal data processed about you:

- name
- birth dates
- job title
- departement
- business email address
- other contact details (e.g. business phone, social media profile link)
- affiliated company name and details
- your IP address

Please note that we are on purpose NOT extracting or processing any data regarding sensitive information like financial data, medical details, political affiliations, private demographic information (e.g. number of children), etc.

Our search index is a fully automated and dynamic system, meaning that if the original data source disappears or is no longer publicly available, the system will also automatically update or delete the piece of personal data after a reasonable amount of time (see Section 7 below).

4. For what purpose do we process your data?

Unlike any of the popular search engines, Leadfeeder isn't free to use for anyone. We only process data and display search results to our registered customers and users within a controlled and secure environment for the following purposes:

- To help our clients gain relevant information for marketing and sales purposes.
- To help our clients update and improve their own databases and data correctness
- To improve and develop our services and products.

5. Legal bases, balancing of interests

The legal basis for processing personal data obtained through our systems is our legitimate interests (Art. 6 (1) lit. f GDPR) in providing and marketing our services to our users and clients, improving our products and services and growing our business. We believe that our legitimate interests are not overridden by the rights or interests of the data subjects, since the vast majority of data we process has already been made publicly available.

You can, of course object at any time to the processing of your personal data. For more information please see section 8 below.

6. Who are the recipients of the processed data?

We may share data with the following recipients:

a. Leadfeeder group

In order to offer you comprehensive support and to ensure an ongoing high quality of our services and products, Dealfront Group GmbH relies on the assistance of Dealfront Germany GmbH and Dealfront Finland Oy (each a "Joint Controller" and together the "Joint Controllers"). The legal basis for such processing is Art. 6 (1) lit. b as well as Art. 6 (1) lit. f (legitimate interest in providing and improving our services). In accordance with Art. 26 of the GDPR, the Joint Controllers have entered into a Joint Controller Agreement stipulating in a transparent manner their respective responsibilities with regard to compliance with their obligations under

the GDPR. The essential content of the Agreement is available:
<https://www.leadfeeder.com/privacy/>

In addition, we may share data with other affiliates for marketing or customer support purposes. Such processing activity is based on Art. 28 GDPR in conjunction with a data processing agreement concluded with the respective affiliates.

b. Service Providers

We may share some data with some companies that help us provide our services (for example hosting providers). The legal basis for this data transfer and processing activity is Art. 28 GDPR in conjunction with a data processing agreement concluded with the respective service provider. These service providers are only allowed to use the data shared with them for the specific task they've been hired to do:

- Contact data management / CRM tools
- Cloud Storage and Hosting Provider
- Data accuracy and data analysis tools
- Data analytics providers
- other service and system providers that are necessary for the evaluation of data

While Leadfeeder operates globally, our servers and main data processing activities are primarily done in the European Union. For some features, we may, however, transfer your personal data to third-party service providers located outside of the European Economic Area (EEA). In such cases, we will ensure that appropriate safeguards are in place to protect your personal data, such as standard contractual clauses approved by the European Commission.

c. Leadfeeder users and clients

We may display your data to our clients and users who have subscribed to our services and who have a legitimate interest in the data (Art. 6 (1) lit. f GDPR) in order to promote their business and market their services. Please note that our clients act as data controllers with regard to such data. Thus, they are solely responsible for their data processing activities and handle their processing operations and data subject rights requests independently from us.

d. Legal Disclosure

We may disclose your personal data to comply with legal requirements and obligations, including court orders or to comply with legitimate requests from law enforcement agencies or regulators

e. Change of ownership

We may disclose your personal data in the event of an acquisition, merger or other transaction to the new owner

7. Data Retention

When processing and storing personal data, we make sure that data is only stored for as long as is necessary for the intended purpose.

If the personal data are stored in our search index, the data is kept as follows: In case data can be found by our web crawlers in several different sources (e.g. in the commercial register, in the website's imprint, and on a public social media profile), the **storage period** depends on the last successful access to the respective data in one of the related public sources. If this was more than 12 months ago for all available sources, the data will no longer be displayed in our search index. The data are also deleted if the data subject asserts their right to have the data deleted by us.

8. How can I obtain information and what are my rights?

You may be entitled to exercise some or all of the following rights:

1. require (i) information as to whether your personal data is retained and (ii) access to and/or duplicates of your personal data retained, including the purposes of the processing, the categories of personal data concerned, and the data recipients as well as potential retention periods;
2. request rectification, removal or restriction of your personal data, e.g. because (i) it is incomplete or inaccurate, (ii) it is no longer needed for the purposes for which it was collected, or (iii) the consent on which the processing was based has been withdrawn;
3. refuse to provide and – without impact to data processing activities that have taken place before such withdrawal – withdraw your consent to processing of your personal data at any time;
4. **object, on grounds relating to your particular situation, that your personal data shall be subject to a processing. In this case, please provide us with information about your particular situation. After the assessment of the facts presented by you we will either stop processing your personal data or present you our compelling legitimate grounds for an ongoing processing;**
5. take legal actions in relation to any potential breach of your rights regarding the processing of your personal data, as well as to lodge complaints before the competent data protection regulators;

6. require (i) to receive the personal data concerning you, which you have provided to us, in a structured, commonly used and machine-readable format and (ii) to transmit those data to another controller without hindrance from our side; where technically feasible you shall have the right to have the personal data transmitted directly from us to another controller; and/or
7. not to be subject to any automated decision making, including profiling (automatic decisions based on data processing by automatic means, for the purpose of assessing several personal aspects) which produce legal effects on you or affects you with similar significance.

You may (i) exercise the rights referred to above or (ii) pose any questions or (iii) make any complaints regarding our data processing by contacting at: privacy@leadfeeder.com.

9. No automated profiling

Profiling describes a type of automated processing of personal data that consists in assessing, analysing, or predicting certain personal aspects such as health or personal preferences and which produces legal effects on the data subject. Leadfeeder does not use such profiling.

10. Additional Privacy Disclosure for U.S. Residents

Dealfront is registered as a data broker with the California Privacy Protection Agency pursuant to California Civil Code SS 1798.99.80 and is in the process of registering as a data broker in the following states: Oregon, Texas and Vermont.

THE ENTITY MAINTAINING THIS WEBSITE IS A DATA BROKER UNDER TEXAS LAW. TO CONDUCT BUSINESS IN TEXAS, A DATA BROKER MUST REGISTER WITH THE TEXAS SECRETARY OF STATE (TEXAS SOS). INFORMATION ABOUT DATA BROKER REGISTRANTS IS AVAILABLE ON THE TEXAS SOS WEBSITE.

The entity maintaining this website is a data broker under Texas law. To conduct business in Texas, a data broker must register with the Texas Secretary of State (Texas SOS). Information about data broker registrants is available on the Texas SOS website.

This section supplements the information contained in this Privacy Information and applies solely to individuals who reside in the United States ("U.S. Residents"). It is provided to comply with applicable U.S. state privacy laws, including the California Consumer Privacy Act of 2018 (CCPA) as amended by the California Privacy Rights Act (CPRA), and similar laws in other U.S. states.

In the event of a conflict between this Section and other parts of **this Privacy Information**, this Section shall apply to U.S. Residents.

a. Definition

Certain terms used in this Section have the meanings given in applicable U.S. privacy laws:

Personal Information (PI)

Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. This corresponds broadly to the term personal data under the GDPR.

Sensitive Personal Information (SPI)

A subset of Personal Information that includes, for example, precise geolocation, account log-in credentials, financial account information, and other categories defined under California law.

Consumer

A natural person who resides in California or another U.S. state with an applicable privacy law.

Sale

The disclosure of Personal Information to a third party for monetary or other valuable consideration.

Sharing

The disclosure of Personal Information to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration.

b. Sources and Categories of Personal Information

We collect Personal Information set forth and from the sources described in **Section 2 ("Which sources and data do we use?")** of this Privacy Information, including:

- Directly from you (e.g. when creating an account, contacting us, or using our services)

- Automatically from your device or browser when you interact with our platform
- From third parties, such as third-party licensed data providers, publicly available sources including company websites, business partners or other users who provide your details in a business context

We may collect the following categories of Personal Information:

- (a) Identifiers: name, business email address, business phone number, IP address;
- (b) Professional and employment information: job title, department, employer name;
- (c) Internet or network activity: website visits via Dealfront's visitor-identification technology;
- (d) Geolocation data: country and region derived from IP address;
- (e) Inferences: professional attributes and purchase propensity derived from the above;
- (f) Publicly available information: data indexed from public websites, company registers, directories, and open databases as described in Section 2 of this Privacy Information.

C. Sharing of Personal Information / Third Parties to Whom Personal Information is Sold or Disclosed

As described in **Section 6 ("Who are the recipients of the processed data?")** of this Privacy Information, we share Personal Information with our customers, partners, service providers, certain third parties, and where required by law in order to operate our business and provide our services.

d. Privacy Rights

U.S. Residents, and specifically California Consumers, as well as residents of Oregon, Texas and Vermont have the following rights regarding their Personal Information, subject to certain exceptions:

1. **Right to Know/Access:** The right to request disclosure of the specific pieces of PI we have collected about you, the categories of sources, the business purpose for collecting or selling/sharing it, and the categories of third parties with whom we disclose it.
2. **Right to Delete:** The right to request the deletion of your Personal Information that we have collected, subject to legally recognized exceptions.
3. **Right to Correct:** The right to request that we correct inaccurate Personal Information we maintain about you.
4. **Right to Opt-Out of the Sale or Sharing of PI:** The right to direct us not to Sell or Share your Personal Information (including for targeted advertising).
5. **Right to Limit Use and Disclosure of Sensitive Personal Information:** The right to limit the use of your SPI. As stated in **Section 3 ("Which personal data do we collect?")** of this Privacy Information, Leadfeeder does not extract or process sensitive personal information, and therefore, does not offer a separate right to limit its use.
6. **Right to Non-Discrimination:** The right not to receive discriminatory treatment for exercising any of your privacy rights.
7. **Right to data portability** (receive a copy in a portable format).

We honour opt-out preference signals including the Global Privacy Control (GPC). If your browser or device sends a GPC signal when you interact with our website or services, we treat it as a valid request to opt out of the sale, sharing of your personal information and opt out of the sale and use of your personal data for targeted advertising. This applies automatically, no additional action is required on your part.

We respond to rights requests within 30 calendar days of receipt. We may extend the response period by an additional 30 days where reasonably necessary, and we will notify you of any extension within the initial 30-day period.

We do not sell sensitive personal information as defined under applicable law, including racial or ethnic origin, religious beliefs, mental or physical health data, information about sex life or sexual orientation, biometric data, precise geolocation data, or personal data of minors, regardless of consent. US residents have the right to request that we refrain from processing such sensitive data. To the extent we process (but do not sell) sensitive personal information about US residents, we obtain specific and informed consent, we do not rely on broad, pre-ticked, or buried consent.

e. How to Exercise Your Rights and Contact Information

To opt out of the sale or sharing of your personal information, you may click the 'Do Not Sell or Share My Personal Information' link in the footer of our homepage, or use the methods listed below. We do not require you to create an account to submit an opt-out request.

You may exercise your privacy rights, especially but not limited to your right to opt out of sale, sharing or licensing of your personal information, by contacting us through one of the following methods:

- Email: privacy@leadfeeder.com
- Online tool: privacycockpit.leadfeeder.com

You may designate an authorized agent to make a request on your behalf where permitted by law. We may take reasonable steps to verify your identity (and, where applicable, the authority of your agent) before processing your request.

Dealfront participates in California's Data Broker Registry Operating Platform (DROP). California residents may submit deletion requests directly through DROP. Starting August 1, 2026, Dealfront accesses DROP at least every 45 days to process consumer deletion requests. Upon matching a request, Dealfront deletes the matched personal information and instructs its service providers to do the same. Dealfront does not contact consumers to verify DROP-submitted requests.

f. Children's Privacy

Leadfeeder's products and services are designed for business use and are not intended for or directed to individuals younger than 16 years of age. We do not knowingly collect, maintain, sell, share, or process Personal Information from anyone under 16. We ask that individuals under 16 do not provide any Personal Information through our Site or Services. If we discover that we have inadvertently received Personal Information from a person under 16, we will take prompt steps to delete the information in accordance with applicable legal requirements. If you believe that a child under 16 may have provided Personal Information to us, please contact us at privacy@leadfeeder.com so that we can investigate and take appropriate action.

g. Security Program

We have implemented and maintain a comprehensive information and data privacy security program including: (a) administrative, technical, and physical safeguards appropriate to the volume and sensitivity of data we process; (b) employee training on data security and data privacy; (c) oversight and assessment of service providers with access to personal data; (d) procedures to detect, prevent, and respond to security incidents; and (e) annual review and update of the program.

h. Do NOT Track Signals

Some web browsers offer a "Do Not Track" (DNT) feature that, when enabled, sends a signal to websites requesting that your browsing activity not be tracked. Our technology (Leadfeeder/Dealfront Web Visitor) relies on first-party data collection methods such as our own tracking script and IP address-based company lookups rather than third-party cookies that follow individuals across multiple websites. Our technology is designed to identify the companies visiting a specific website, not to track individuals across the web.

As DNT signals are primarily intended to address cross-site behavioral tracking by third parties, and as there is currently no industry-wide standard for how such signals should be interpreted or honored, we do not alter our data collection practices in response to DNT signals.

You may still exercise your privacy rights as described in this Privacy Information, including the right to opt out of the sale or sharing of your personal information where applicable under state law.

11. Changes to this Privacy Information

We reserve the right to amend this Privacy Information to ensure continued compliance with legal requirements or to reflect changes to our services in the Privacy Notice.

E

AI Features at Leadfeeder

Leadfeeder AI Features

Our approach to responsible AI

1. Purpose and Scope of this Document

At Leadfeeder we offer you AI Features that make it even easier to find what you are looking for. Whether you are looking for companies, contacts or other insights, by using the power of popular Large Language Models (LLMs) our AI Features understand your intent and deliver the results you were hoping for.

We've built these features with **security and compliance at their core**, so that your data stays protected and you stay compliant. Our AI Features do not expose confidential or personal data to externally hosted LLMs. The LLMs only see the information you include in your prompt together with the information required to answer your request.

This document gives you an overview of how our AI Features work and how they are designed to meet data-protection and AI-regulatory standards. If you'd prefer not to use them, you can easily turn the AI Features off at any time by reaching out to our support teams.

2. Overview of AI Features

2.1 AI List Enrichment

Our AI List Enrichment tool helps you add valuable insights to the companies that matter most to you. Simply select a list of companies and ask the AI to generate a new data point on a specific topic you are interested in. The AI enriches your list of companies with the desired information.

For example, if you are interested in environmentally friendly companies, select the companies most relevant to you and ask the AI: "How environmentally friendly are the companies?". The result could look as follows:

Company A, Score: 9 / 10, Explanation: Company A operates on 100 % renewable electricity, publishes audited sustainability reports, and has achieved a verified 40 % reduction in CO₂ emissions since 2020.

Company B, Score: 2 / 10, Explanation: Company B has no publicly available sustainability targets, relies heavily on coal-based energy, and has been fined for environmental non-compliance.

The feature works with data from our global Leadfeeder database, including publicly available sources such as company websites and signals. It does **not** access or use your

customer data. The AI List Enrichment tool will access the global Leadfeeder database to retrieve information on each selected company and forward it to the LLM to generate the results.

2.2 AI Target Filter Generation

The AI Target Filter Generation makes it easier than ever to discover the companies or contacts most relevant to you. Simply describe what you're looking for in natural language. The tool will take on retrieving the relevant information from the database by having the LLM transpose your natural language request into a powerful database query.

For example, if you ask the AI to show all German companies with at least 100 employees that have Data Science teams, the AI automatically converts your request into matching filters such as country (DE), employee count (100+), and job titles (Data Science, AI, Data Engineering). The tool applies these filters to our database and delivers the results instantly. Additionally, the tool will provide feedback to help you understand if your prompt needs refinement to retrieve better results.

To make this work, none of your customer data is exposed to the LLM. Only your prompt will be forwarded to the LLM together with tool specific instructions. The query provided by the LLM will be applied to the Leadfeeder database without any further involvement of AI.

2.3 AI Signal Alerts

AI Signal Alerts help you stay up to date with the companies that matter most to you. Set up customized alerts based on specific topics or events for a selected list of companies and let the tool inform you about updates on a regular basis (e.g. daily, weekly, or monthly).

For example, you could create an alert for companies in your list announcing the construction of new office buildings. The output might include entries such as "Siemens AG is building a new office in Munich [link to source]" or "Volkswagen AG plans a new office complex in Wolfsburg to be completed in 2028 [link to source]."

To generate these insights, the AI Signal Alerts searches the Leadfeeder global database for relevant signals related to your selected companies. The identified information, along with your prompt, is then processed by the LLM to compile the results. Aside from the user prompt, no user or customer data is sent to the LLM.

2.4 AI Company Insights

With AI Company Insights, you can quickly generate tailored insights about a specific company. Simply select a company of interest and ask a question in natural language. The

tool will retrieve information on the company from the Leadfeeder global database, collect information from the internet and send this information to the LLM. The LLM will analyze the information and provide the answer to your question.

2.5 AI Contact Recommendations

AI Contact Recommendations helps you identify the most relevant contacts for your needs. Start with a selected list of contacts from the Leadfeeder database and describe in natural language which profiles you want to find. Your prompt will be forwarded to the LLM which interprets your request and returns the necessary filters. The filter will be applied to your list of contacts to return the matching contacts.

For example, you might ask to find all members of Data Science teams based in Germany or Austria. Contact Recommendations will translate this prompt into filters such as location and job title, apply them to your pre-selected contact list, and deliver the relevant results.

Only your prompt together with system instructions is sent to the LLM to define the filters. No other user or customer data is shared. The generated filters are then applied to the chosen subset of the Leadfeeder database to identify matching contacts.

2.6 AI Web Visitor Summary

AI Web Visitor Summary gives you instant, AI-powered summaries of how companies engage with your website. Simply enter a prompt, for example, “Show me a summary of this company’s engagement” and you’ll receive a clear, conversational overview of their activity.

Your summary might read something like:

“Company XYZ visited your website 50 times in the past 90 days, mainly from Berlin, Germany. Six unique visitors viewed 77 pages in total, spending the most time on your pricing pages — a strong indicator of buying intent.”

Behind the scenes, a LLM analyzes your tracked website events (such as page visits, sources, time spent, and visitor IDs) to generate insights tailored to your question.

All personal identifiers are pseudonymized before data is sent to the AI model, and then safely restored internally once the response is received. This ensures that no identifiable visitor data ever leaves the Leadfeeder environment.

The result: an at-a-glance, privacy-safe view of each company’s engagement, directly in the Leadfeeder App, helping you spot your most interested prospects faster.

3. Compliance

Our AI Features do not expose customers to compliance risks. In particular, the only user or customer data that is processed are the respective user prompts.

3.1 Data Protection

Protecting your personal and confidential data is a core element of our AI Feature design and a key part of complying with European and global digital regulations. We know that generative AI brings new challenges for privacy because LLMs may, in rare cases, reproduce information contained in their training data. To avoid this risk, we built our AI Features with data protection in mind and have taken the necessary legal safeguards to protect your data.

To eliminate the risk of a model reproducing your confidential information, your customer data is not forwarded to the LLM. With the exception of AI Web Visitor Summary, the only individualized data the LLM will see is your prompt. Otherwise, we only provide the LLM with data from our global database which is collected from publicly available sources on the internet.

As an additional safeguard, we only use LLM providers that contractually commit not to use customer prompts or outputs for model training. Thus, even if personal or confidential data is included in a user prompt, it will not be stored or reused by the external LLM provider for model training. This ensures that your data remains private and protected at all times.

Prompts and AI-generated outputs are only retained for as long as necessary to provide the requested functionality and to ensure service quality. Once not needed anymore, prompts and outputs are anonymized or deleted from our systems and the systems of the LLM providers.

To comply with regulation on data transfers to third party recipients, we have concluded data processing agreements with our LLM providers. Where external LLM providers process data outside the EU/EEA, we rely on appropriate safeguards such as the European Commission's adequacy decisions or Standard Contractual Clauses (SCCs) to ensure an equivalent level of protection.

Finally, our AI Features are designed purely as assistive tools. They do not make automated decisions or create user profiles that produce legal or similarly significant effects.

3.2 AI Act

We design and operate our AI Features in full alignment with the principles and requirements of the EU AI Act. As part of our compliance approach, we regularly assess our AI systems to ensure that they meet applicable obligations and reflect the spirit of responsible and trustworthy AI.

Our AI Features do not qualify as high-risk AI systems under the EU AI Act. They are assistive tools that support users in retrieving information. They are not intended for use cases that are classified as high-risk under the EU AI Act.

Even though the strict requirements for high-risk systems do not apply, we take the AI Act's key principles of transparency, accuracy, fairness and non-discrimination seriously. To uphold these values, we continuously monitor and test our AI Features to identify potential risks or compliance issues early. That said, AI may occasionally generate incomplete or inaccurate results. Our AI Features are designed to assist your work, not to replace human judgment. We therefore recommend verifying AI-generated information for accuracy and suitability before using it in your specific context.

4. Turning off AI Features

If you feel uncomfortable with the AI Features, the administrator of your Leadfeeder account can always disable the AI Feature by setting the `disable_ai_features` flag. This will disable all AI Features described above and hide any onboarding messages and other information that could be perceived by users as a nudge to use AI Features.

5. FAQ

5.1 Which large language models are used?

All providers are carefully selected and contractually bound to comply with data protection and security requirements.

5.2 How does AI contribute to the AI Features?

We use **Large Language Models (LLMs)** to make our services more intuitive and efficient. Depending on the specific feature, the LLM helps interpret what you are looking for, generate search filters, or summarize relevant information.

The general process works as follows: You describe your request in natural language (the *prompt*). This prompt, along with limited contextual information from our global Leadfeeder database and predefined instructions, is sent to the LLM. The model generates a response, which our system then uses to produce the final result, sometimes involving additional data

processing within our own systems. With the exception of the prompt you enter and the AI Web Visitor Summary, your customer data is never forwarded to the LLM.

5.3 Will my data be used to train AI models?

No. We have contractually agreed with all LLM providers that neither your prompts nor the output generated are used for model training. In addition, our AI Features do not access or process your customer data.

The only individual data ever seen by the AI model is the text you include in your prompt. All other information required for the AI Feature to function is handled within our systems under strict data protection and security controls. We apply robust internal safeguards to prevent unauthorized access or use and to ensure full compliance with applicable data protection laws.

5.4 How does Leadfeeder ensure data protection compliance for its AI Features?

We ensure data protection compliance through a combination of contractual, technical, and organizational safeguards. All LLM providers we work with act as our data processors under dedicated Data Processing Agreements (DPAs). The LLM providers have contractually committed not to use any prompts or outputs for future model training. This prevents the risk of personal or confidential information being memorized and reproduced by the model.

In addition, our AI Features never access your internal or customer-specific data. They operate solely on data from our global Leadfeeder database, which is available to all customers. The only individual data element ever seen by the model is the text you include in your prompt.

5.5 How can I protect confidential information when using the AI Features?

Our AI Features are designed so that your confidential information is not exposed to the LLM. The only personal data ever seen by the model is what you actively include in your prompt.

If you prefer not to share certain information, simply avoid entering it in the prompt. However, even if a prompt contains personal or confidential data, this does not create a compliance issue. All LLM providers act as data processors and are bound by Data Processing Agreements as required by applicable law. They have contractually committed not to use prompts or outputs for model training or any other purpose.

In short: Your data remains protected at all times and you stay in control.

5.6 Can I rely on the AI Output?

We design our AI Features to be as accurate and reliable as possible. Their performance benefits from the quality of our underlying databases, and we continuously monitor and test the features to maintain consistency and precision.

That said, AI models can occasionally produce incomplete or inaccurate information and may sometimes generate statements that do not fully reflect the facts. For this reason, we recommend reviewing AI-generated results for accuracy and suitability before relying on them in your specific use case.

5.7 Can I turn the AI Features off?

Yes. You have full control over whether you use the AI Features. Please refer to [section 4](#) for instructions. Turning them off does not affect your access to the rest of the Leadfeeder platform.

5.8 Does Leadfeeder use AI for automated decision-making or profiling?

No. Our AI Features are designed purely as assistive tools. They help you find and interpret information more efficiently but do not make automated decisions or create profiles that produce legal or similarly significant effects. All decisions and interpretations remain fully under your control.

5.9 Where is my data processed, and does it leave the EU/EEA?

Your data is primarily processed within the EU. However, as we use popular LLM providers, data sent to the LLM may leave the EU. The effect is limited, though, because your prompt is the only data individualized by you that is transferred to the LLM. We do not process your customer data with LLMs.

5.10 How does Leadfeeder ensure compliance with the EU AI Act?

Our AI Features are fully aligned with the principles of the EU AI Act. They are assistive tools helping users to identify information and do not qualify as high-risk systems. We ensure transparency and accuracy and continuously test and document our AI Features.

5.11 What happens to my prompt and AI-generated output after I use an AI Feature?

Prompts and AI-generated outputs are only stored as long as necessary to deliver the requested result or perform the requested service and maintain service quality. Afterwards, they are automatically deleted or anonymized. None of this information is used for model training or shared with third parties.

5.12 Can I report an issue or concern with an AI-generated result?

Yes. We encourage feedback to help us continuously improve our AI Features. If you notice an inaccurate, biased, or otherwise concerning result, you can report it directly through your account interface or contact our support team at support@Leadfeeder.com. Our team reviews all submissions and, where appropriate, adjusts the feature to prevent similar issues in the future.

