

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.