Legal kit

August 2023

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 a 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.

Our legal kit includes a variety of resources, including

- our general terms and conditions, which outline the terms of service for the Dealfront platform (**A**);
- our data processing agreement governing the specific cases where we act as a data processor and our customer acts as a data controller (**B**);
- the **privacy notice** for our customers and website visitors, which details how we handle and protect your personal data (**C**); and
- a privacy information sheet for data subjects explaining how we collect and process data by web crawlers and other search engine technologies (**D**).

As part of our commitment to data privacy, transparency and compliance, we have also included a white paper on the balancing of interest test, providing you with additional guidance on how to assess data vendors (**E**). Finally, we understand that the EU General Data Protection Regulation (*GDPR*) is a top concern for many organisations. That is why we have included an overview of recent GDPR fines in order to enable your legal department to be in a better position to perform a risk assessment and to help you understand required compliance efforts (**F**).

We hope that our legal kit provides you with the information your legal department needs to make an informed decision about our services. Please don't hesitate to contact us if you have any questions or concerns.

A. General Terms And Conditions (GTC)

1. Definitions

Dealfront (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 Dealfront and Contracting Company and their respective User(s).

b) "Contracting Company" means the party to whom Dealfront 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) "Dealfront" 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 Dealfront web software, platform, products and any services which Dealfront 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 Dealfront 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 Dealfront, 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. Dealfront 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 Dealfront representative.

3. Content & Use of Services

3.1. Dealfront 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. Dealfront Services can be used without sharing personal data with us. However, if you (a) are implementing Dealfront 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://marketing.dealfront.com/inside-eea-data-processing-agreement-dealfront-en.pdf, "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, Dealfront processes personal data for its own purposes and not on behalf of you. Therefore, Dealfront 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 Dealfront's privacy notice (https://dealfront.com/privacy-notice/).

3.4. In the event Dealfront 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, Dealfront may expand, modify, or supplement its offering at any time and in Dealfront's sole discretion.

3.6. You acknowledge that all Results are compiled through automated systems at a large scale. Dealfront 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 Dealfront 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 Dealfront adds additional information to data provided by you as part of the Service, you acknowledge and agree that Dealfront 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. Dealfront is entitled, in each case, to reject specific Queries or the display of certain Results if Dealfront cannot reasonably execute or display these for technical and/or legal reasons.

4. License

4.1. Dealfront 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 Dealfront 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, Dealfront 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. Dealfront 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 Dealfront 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, Dealfront 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. Dealfront 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 Dealfront 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. Dealfront will inform you about such adjustments accordingly.

4.12. Dealfront 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 Dealfront'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 Dealfront and shall immediately report errors, bugs and any shortcomings relevant for IT security to Dealfront when Users become aware of such occurrences.

b) Users shall not unduly interfere with the Services or Dealfront'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 Dealfront 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 Dealfront.

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 Dealfront.

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 Dealfront 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, Dealfront 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. Dealfront 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 Dealfront 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 Dealfront, e.g. for the purpose of updating or enriching such data, you grant Dealfront a non-exclusive right to process such data as necessary, and to perform the Services pursuant to the Agreement.

6.3. Dealfront 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 Dealfront's Services pursuant to the Agreement. Dealfront 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

Dealfront will provide you with assistance and support in accordance with your Order and Plan selected. Dealfront’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 Dealfront 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. Dealfront 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). Dealfront 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, Dealfront 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.

Dealfront 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 Dealfront 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. Dealfront is entitled to involve third parties to provide the Services pursuant to the Agreement. Dealfront will ensure that such third parties comply with Dealfront's obligations under this Agreement, in particular with confidentiality and privacy obligations set forth in these GTC.

9.2. Without Dealfront'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 Dealfront 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. Dealfront shall only be liable to you for damages caused intentionally or with gross negligence. This shall not apply if Dealfront 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. Dealfront 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 Dealfront'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 Dealfront's employees, representatives, bodies and vicarious agents.

10.5. The Contracting Company shall indemnify Dealfront 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 Dealfront to defend itself against third-party claims. Dealfront shall inform the respective Contracting Company of any legal claim raised against Dealfront without undue delay. Dealfront shall, before entering into any settlement with such a third party, consult with the Contracting Company. If Dealfront decides to enter into a settlement without the Contracting Company's consent, Dealfront 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 Dealfront entity:

Contracting Dealfront affiliate is:	Governing law:	Courts with exclusive jurisdiction are located in	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

Dealfront has the right to amend these GTC, to adapt the GTC to changes of applicable laws, or to the services Dealfront offers. In this event, Dealfront 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, Dealfront reserves the right to terminate the Agreement extraordinarily with a notice period of one (1) month

B. 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.

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.

(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

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. 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.

(2) Data subjects' rights

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

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

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

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

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

(3) Monitoring duties

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

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

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

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

(4) Information duties

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

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

c. The Processor shall notify the Controller without any reasonable delay of any breach of data protection regulations, of the Principal Agreement and the Agreement and/or the instructions issued by the Controller, where such breach

occurs in the course of the processing of data carried out by the Processor, its employees or other third parties entrusted with the processing of data.

d. In the event that the Processor establishes, or if facts justify the assumption, that personal data processed by the Processor on behalf of the Controller have been unlawfully transmitted or otherwise unlawfully disclosed to third parties or that any other personal data breach has occurred, the Processor shall notify the Controller without delay and no later than 48 hours after becoming aware of the incident, providing information about

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

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

(5) Location of processing

a. The processing and use of the data shall take place exclusively 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. Any transfer to a third country requires the prior consent of the Controller and may only take place if the special requirements of Art. 44 et seqq. GDPR are fulfilled. This also applies to any data backups by Processor.

b. If the processing of personal data is carried out outside the European Union, the Processor guarantees that a lawful cross-border data transfer mechanism is in place. The Processor shall inform the Controller immediately in writing if the lawful cross-border data transfer mechanism no longer applies or if it is foreseeable for the Processor that the lawful cross-border data transfer mechanism will no longer apply before the end of this Agreement.

c. The Processor shall indemnify the Controller against all claims by third parties arising from the fact that

- the lawful cross-border data transfer mechanism no longer applies due to circumstances for which the Processor is responsible, and/or
- the Processor has failed to inform the Controller in due time about the omission of the lawful cross-border data transfer mechanism.

This indemnity obligation also includes, in particular, any fines and administrative fines as well as the Controller's reasonable legal fees.

d. If the Processor's lawful cross-border data transfer mechanism ceases to apply, the Controller shall be entitled, at its own discretion,

- to terminate the Principal Agreement immediately or
- to request that the Processor, by a specified deadline, provide another lawful cross-border data transfer mechanism or conclude Standard Contractual Clauses which meet the requirements of the data protection authority responsible for the Controller, whereby the Processor shall bear the costs incurred by this procedure.

  If the Processor fails to comply with the request on time, the Controller shall also be entitled to terminate the Principal Agreement. In the event of an extraordinary termination, the Processor shall, upon instruction by the Controller, assist the Controller at its own expense in transferring the personal data immediately to another processor named by the Controller.

e. If the processing of personal data takes place outside the EU, the Processor further guarantees that it has appointed a representative in the EU for the duration of the order, provided that this is necessary under the applicable data protection regulations. The representative shall be instructed to act as a contact point in addition to the Processor or in its place, in particular for supervisory authorities and data subjects, for all questions related to processing in order to ensure compliance with data protection regulations.

(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 in Annex III 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 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. The Processor shall provide the Controller with a copy of the subcontract upon request.

(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 addition, the Controller shall be granted control and verification rights in the subprocessing agreement in accordance with this Agreement. 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.

(7) Processor Affiliates shall process personal data only as subprocessors.

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

Sect.16 Miscellaneous

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

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

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

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

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

Schedule of Annexes

Annex I List of Acceding Parties

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

Annex III Subprocessors pursuant to Sect. 10 of this Data Processing Agreement

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:

   Address:

   Contract person's name, position and contact details:

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

1. Company name:

   Address:

   Contract person's name, position and contact details:

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

3. **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

Annex III

Subprocessors pursuant to Sect. 10 Data Processing Agreement

The Processor currently works with the following subcontractors and the Controller hereby agrees to their appointment. The processing and use of personal data shall take place exclusively 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. Any transfer to a third country requires the prior consent of the Controller and may only take place if the special requirements of Art. 44 et seqq. GDPR are fulfilled. This also applies to any data backups by Processor.

If data processing takes place outside the European Economic Area (EEA) or if access is made from outside the EEA, the following overview must also list the measures and guarantees that ensure an appropriate level of data protection during processing in accordance with Art. 44 GDPR ff. (e.g. EU Standard Contractual Clauses, Binding Corporate Rules or other arrangements by the European Commission).

Company: Amazon Web Services
Data processing activity: Hosting/Cloud Service Provider
Location: EU/EEA

Company: Dealfront Finland Oy
Data Processing activity: Data Infrastructure and IT security
Location: Finland

Company: Dealfront Germany GmbH
Data processing activity: Data Infrastructure and IT security
Location: EU/EEA

C. Privacy Notice for customers And users of Dealfront pursuant to Article 13 of the EU General Data Protection Regulation (GDPR)

May 2023

Introduction

Dealfront Group GmbH and its affiliates, including but not limited to Dealfront Germany GmbH and Dealfront Finland Oy, (in the following "Dealfront", “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.

Dealfront 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 https://marketing.dealfront.com/privacy-information-for-data-subjects-en.pdf?_gl=1*1e5gbno*_ga*Njk4NDU1MTc3LjE2ODEyOTc5NDY.*_ga_BKMK057R5F*MTY4MTMwMjAyNy4yLjEuMTY4MTMwMjcyNy4zNy4wLjA.)

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)** .

Dealfront has implemented numerous measures to ensure the protection of personal data. For more information, visit our **online privacy centre** at: https://www.dealfront.com/privacy-center.

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 Dealfront 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@dealfront.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 Dealfront at any time by email: dpo@dealfront.com.

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

Dealfront 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 Dealfront website or use Dealfront's services (for additional information see here: https://www.dealfront.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 you provide us ab**out 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

a) 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.

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

Insofar as Dealfront 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 Dealfront 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 Dealfront 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 at: privacy@dealfront.com.

If you want to lodge a complaint with the official data protection authority, please visit the website https://www.baden-wuerttemberg.datenschutz.de/ for more information.

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. Dealfront 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.dealfront.com/cookies-and-tracking/.

B2) Information provided by you

If you contact Dealfront, 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 testing software or an app and sharing your data with us.

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) Dealfront 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://marketing.dealfront.com/essential-content-of-the-joint-controller-agreement-en.pdf.

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

Dealfront 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

  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.

C1.4) 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

Dealfront 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@dealfront.com.

D) 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

May 2023

Dealfront Group GmbH (in the following "Dealfront", “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.dealfront.com/privacy-notice/.

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@dealfront.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 Dealfront at any time by email: dpo@dealfront.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 Dealfront 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
- 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, Dealfront 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. Dealfront 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://marketing.dealfront.com/essential-content-of-the-joint-controller-agreement-en.pdf.
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

While Dealfront operates globally, our servers and main data processing activities are exclusively done in the European Union. On rare occasions, 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. Dealfront 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@dealfront.com.

If you want to lodge a complaint with the official data protection authority, please visit the website https://www.baden-wuerttemberg.datenschutz.de/ for more information.

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. Dealfront does not use such profiling.

10. 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. Whitepaper

dealfront

Why most data vendors fail the Balancing of Interest Test.

Disclaimer: Before reading this, please note that this is not legal advice but an opinion piece and that it is your responsibility to ensure that any products and services you use are in compliance with the relevant laws and regulations.

Preamble

At Dealfront we care deeply about data privacy, transparency and compliance with data protection laws. However, data privacy is a complex topic, specifically when it comes to its application in sales and marketing. In addition, we have observed a lot of misleading and conflicting information online. We strive to enable our customers and users to make educated decisions and ask the right questions, which is why we have prepared this document.

As you may be aware, under most modern data privacy regulations like GDPR, a company needs to have a legal basis for processing personal data. If they don't have a legal basis for processing personal data but do it anyway, such processing is unlawful and (if found out) may result in fines, lawsuits and other negative consequences.

Regular data processing of your customer or soon-to-be customers (e.g. in your CRM) typically falls under Article 6 (1) lit. b GDPR as you are fulfilling a contract with a known customer. In this case, the data subjects have actively engaged you and expect their data to be processed in exchange for the services you provide to them.

However, in the case of data vendors that sell data on millions of contacts, it's obvious that there is no direct customer relationship or consent (opt-in) present for everybody in their databases. Therefore these vendors (including Dealfront) rely on "legitimate interest" as defined in Article 6 (1) lit. f GDPR as a legal basis when collecting, storing and selling personal data.

What do they mean by relying on “legitimate interest”?

Calling upon "legitimate interests" means that a company can collect and process personal data if:

a) they have a legitimate reason to do so AND
b) their interest/claim to process the data is stronger than the individuals interest of protecting their own privacy (the “balancing test”)

While the GDPR explicitly mentions sales and marketing activities as an example for legitimate use (see recital 47 GDPR), the balancing test has to be made on a per person basis and cannot be generalized.

Examples where the balancing test works:

- **Processing data about managers and directors taken from a trade register**
  That data was made public by law to be able to identify owners and decision makers and enable trade and business within a country

- **Processing data about hiring managers or press contacts which have themselves published their data on the internet**
  The data was made available with the knowledge and consent of these people in order to be contacted for specific requests related to their job or business

- **Processing business contact data from a companies website**
  The data was put their with the knowledge of these people and the company and their employees know and expect their data to be used in the context of the company’s business

- **Marketing Communications**
  While stricter laws may apply regarding the means on how to contact your business contacts, processing their data for such purposes is in line with market standards and expectations of the respective business contact

Examples where the balancing test fails:

- **Data taken from a private conversation or phone book**
  If I email you, I don’t want a 3rd party to read that conversation and take out details from this and resell it online

- **Processing private phone numbers and personal emails**
  People have a right to separate their private life from business life. Nobody wants unsolicited emails or calls on their personal phone or email address. (In addition and apart

from data protection laws, you also need to respect strict e-privacy laws when using private contact details for marketing purposes.)

- **Processing data from unknown sources as this data might be stolen or acquired in other unlawful ways in the first place**
  Data acquired in such a way can never be subsequently used based on your legitimate interests as the interests of the data subjects to not have their stolen/unlawfully acquired data processed always have to override any sales or marketing interests

- **Storing and processing data for an indefinite period of time or processing outdated data**
  GDPR requires that personal data is not kept for no longer than necessary for the purposes for which it was collected and that data needs to be accurate. This is why it is important to have regular updates of your data on file.

To generalize the examples above:

- It is ok if the data was made public before
- It is problematic if personal data **that was collected unlawfully** or **without the data subject's knowledge or control or if you process outdated data or very old data**

Typical Data subject	
Agrees with / can reasonably expect	**Does not agree / is not ok with**
✓ Processing their data that was made public before	✗ Processing their data that collected from a private context
✓ Processing their data if they actually are aware of you as a controller as well as the scope of processing	✗ Processing their data without any knowledge or possibility to be aware of such processing activity
✓ Processing their data in line with their role in a company	✗ Processing of their private contact data or data that is outdated for business purposes
✓ Processing their data related to	✗ Contacting them on their private

their job or business for business purposes	email address/ private phone number for business related purposes outside of business hours
✓ Processing non-sensitive data relating to business activities	✗ Processing sensitive or highly personal data for business purposes
✓ Processing data that was published in public contact directories with the knowledge of the data subject	✗ Processing data of data subjects that are registered in a public Do-not-contact list

What can you do to assess a data vendor?

Don't blindly trust the marketing material of data vendors. Here are a couple of questions you may ask a data vendor in order to be able to properly assess them:

1. **Where is the personal data coming from? / What data sources do you rely on?**
   if they are compliant - why would they not tell you?

2. **Do you source personal data from your community members?**
   if yes, this is problematic as in the context of the community tools, data vendors identify personal data in your CRM, emails and contact books and use this data for their own databases. Thus, the data subjects concerned never know when, how and for what purpose their data is extracted from your systems.

3. **If I install you tools / plugins, will you be able to read my email?**
   if yes, this is a big concern as you will lose control of the personal data stored in your systems

4. **Do you have personal phone numbers or private email addresses in your database?**
   if yes is there a way to filter these out? Generally, higher data protection standards apply to private contact details of a person

5. **Where do you host your data?**
   EU data subjects are probably not ok with US hosting or outside of the EEA/EU hosting as these countries have different data protection standards than the EEA/EU

Other Arguments by vendors and how to interpret those:

- **“But we have notified everybody in our database according to Art. 14 about our data processing”**
  - *Sending out an email is not sufficient to fulfill the information rights*
  - *It is unclear if the data subject has even received the email - most of those end up in spam folders*
  - *Many data subjects don’t even have an email on their record - and data vendors aren’t sending out letters*

- **“We make it really easy to opt out”**
  - *While this is a necessity, it’s already too late if the data ended up in their database unlawfully*

- **“But we are ISO certified”**
  ISO, SOC or any other certifications do not legitimize lawful processing or proof compliance with the GDPR or other privacy laws. These certificates typically test the framework governance within the defined scope: how the processes work and how those are documented (i.e. IT security policies, how technical infrastructure is secured), and not the personal data that is flowing within the systems.

- **“We only process B2B / business data”**
  While this is good - it still is personal data.

- **“We are audited under Trust-e or ePrivacy Seal”**
  These are badges that organizations like to display on their website in order to show that they comply with certain privacy standards. However, these seals are issued by private third-party providers against a fee, creating a financial incentive to actually issue them rather than carefully vetting the respective organizations and eventually denying their issuance. Thus, these seals create a false sense of security.

- **“The GDPR does not apply to us”**
  Even if it may not apply to a US company it applies without any doubt to their EU customers using their services. If a service sells only data about non-EU data subjects and only to non-EU customers, that is true. But as soon as there is any data about EU data subjects involved, GDPR applies.

- **“We are registered data-brokers”**
  This is a requirement under certain US privacy laws and has no meaning with regard to GDPR compliance.

- **“Are you fully COMPLIANT or just ALIGNED?”**
  Using sentences like “adhere to GDPR principles” or “GDPR aligned” show that instead of being confident that they are compliant they just try to be as compliant as possible.

- **“We have successfully performed a data privacy impact assessment (DPIA)”**
  This is mandatory under the GDPR for certain high risk or large scale processing activities. The fact that they performed such a DPIA does not mean anything with regard to the lawfulness of their processing activity or their data.

  As a result:

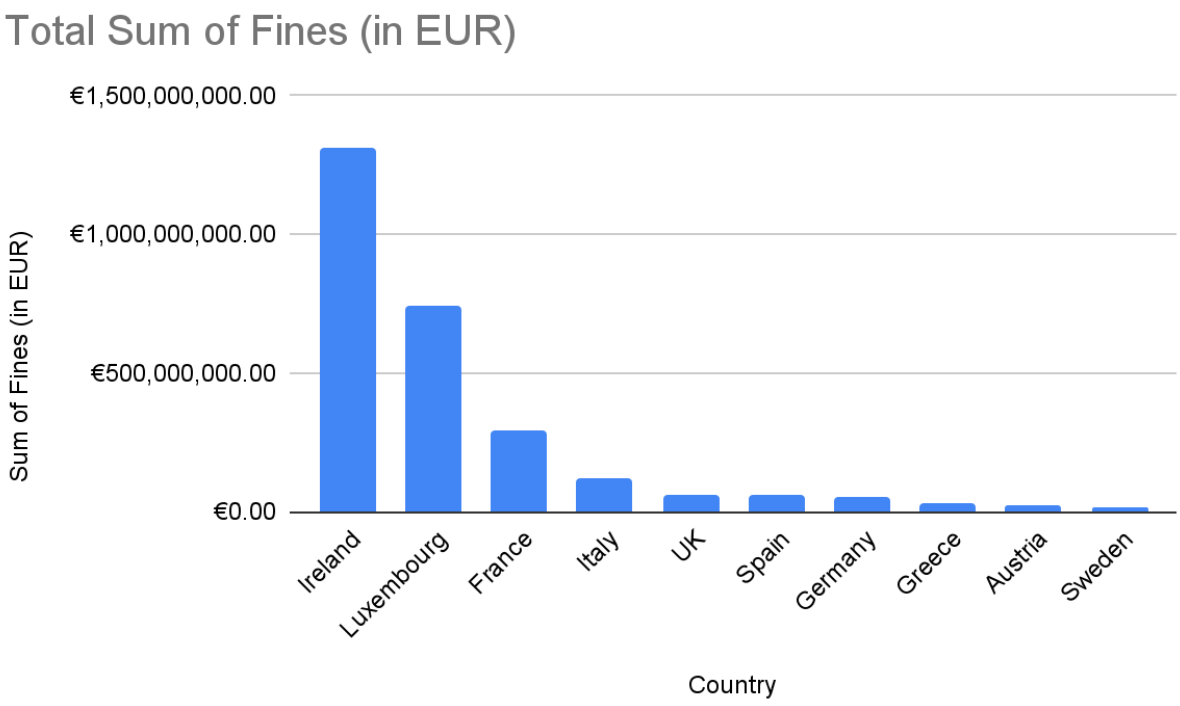
  You are responsible for data privacy as soon as you acquire data from data vendors. Don’t blindly trust their marketing materials.

  Make sure that a data vendor:
- predominantly relies on personal data from publicly available sources;
- disclose personal data only either with the explicit consent and/or knowledge of the data subject concerned or for reasons of public interest and in accordance with the law (e.g. commercial registers);
- carefully vets all data sources to ensure the quality and reliability of the data;
- never acquires data from data sources that have questionable data processing practices or cannot explain and provide comprehensive documentation with regard to their data sources;
- never shares your personal data and the personal data that you share with with other parties, unless you explicitly asked them to do so

F. Overview of Recent GDPR Fines

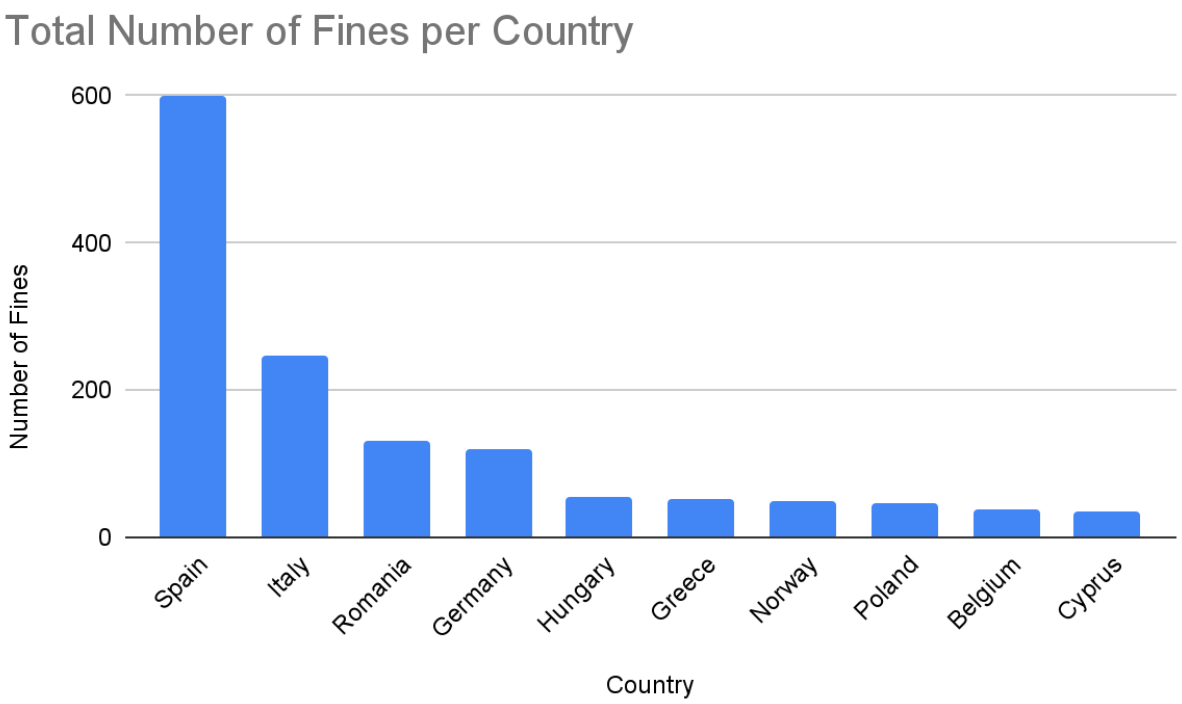
The General Data Protection Regulation (GDPR) has been in effect since May 2018, and since then, data protection authorities (DPAs) in the European Union have been actively enforcing it.

The following statistics show how many fines and what sum of fines have been imposed per country to date (April 2023) (only top 10 countries) as well as sectors:



Data Source: https://www.enforcementtracker.com/

In terms of recent GDPR fines, there have been several notable cases. In 2021, Luxembourg's DPA issued the largest fine under the GDPR to date to Amazon Europe in the amount of € 746 million for non-compliance with general data protection principles regarding processing of customers' data. In the last three (3) years, Ireland's DPA issued several high fines to Meta Ireland as well as Meta's US entity and WhatsApp Ireland (in total €1 billion 60 million) in the last three years.



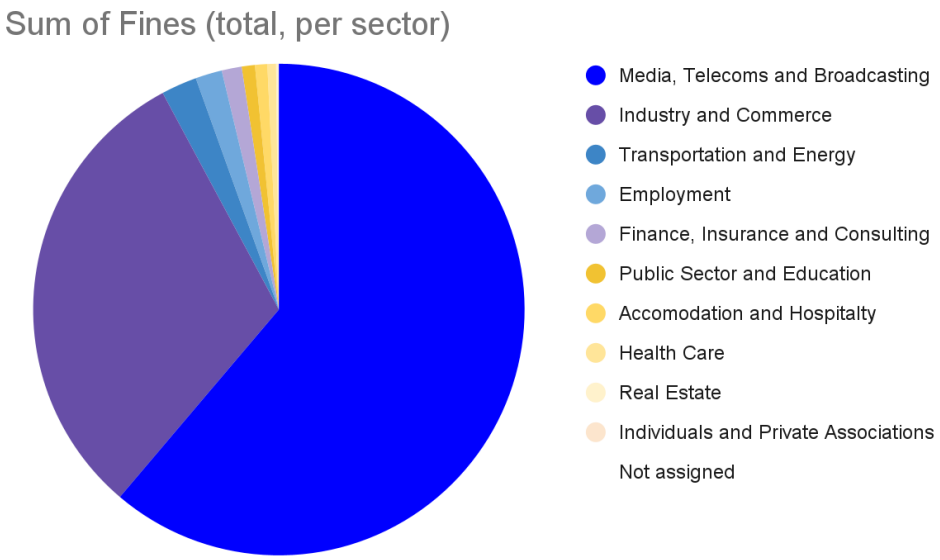
Data Source: https://www.enforcementtracker.com/

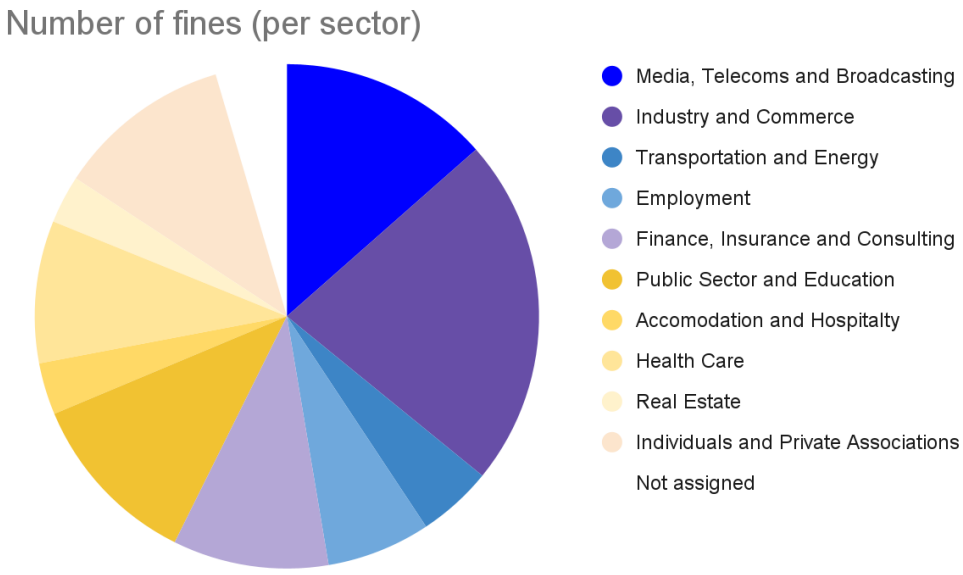
As can be seen from the data, there are certain high profile cases where DPAs have issued substantial fines to companies. However, in general, DPAs tend to take a cooperative approach when it comes to the enforcement of GDPR requirements.

Before imposing fines for GDPR violations, DPA consider several factors such as:

- Cooperation;
- Financial impact;
- Proportionality of fine relating to scope of violation;
- Whether the violation was made intentionally or unintentionally.

DPAs are encouraged to work with private companies and individuals to achieve GDPR compliance. In most cases, smaller fines are more appropriate and effective in achieving compliance with GDPR requirements.





Summary:
The General Data Protection Regulation (GDPR) has been in effect since May 2018, and since then, data protection authorities (DPAs) in the European Union have been actively enforcing it. In recent years, several high-profile GDPR fines have been issued, with companies in various sectors being penalised for data protection violations.

However, it is important to note that in most cases,

- DPAs have chosen to take a cooperative approach to GDPR enforcement, with a focus on resolving issues and finding solutions rather than immediately issuing fines or enforcing GDPR provisions;

- most GDPR enforcement actions have resulted in lower penalties, with fines typically ranging from a few thousand euros to a few hundred thousand euros;
- companies that have been found to violate the GDPR have been able to avoid fines or reduce their penalties by showing that they have made good faith efforts to comply with the regulation;
- **DPAs are generally more lenient towards companies that show a willingness to cooperate and address compliance issues.**

  In conclusion, while GDPR fines can be substantial, DPAs tend to take a cooperative approach to enforcement, with a focus on finding solutions and resolving issues rather than immediately imposing penalties, provided that companies are able to demonstrate good faith efforts to comply with GDPR requirements. This includes implementing and enforcing internal privacy guidelines, providing regular training to staff on data protection requirements and **carefully vetting any third-party with whom personal data is shared**.