



Front Privacy Notice

Effective as of June 5, 2024.

This Privacy Notice describes how FrontApp, Inc. ("**Front**," "**we**", "**us**" or "**our**") handles personal data that we collect through our websites and mobile applications that link to this Privacy Notice (collectively, the "**Service**"), as well as through our marketing and other activities described in this Privacy Notice. Use of the Service is subject to our [SaaS Services Agreement](#).

California residents: See our [California privacy notice](#) for information about your personal information and privacy rights.

Individuals in the EEA/UK/Switzerland: See our [Notice to European users](#) for information about your personal data and data protection rights.

If you have any questions or concerns about our use of your personal data, please contact us.

Index

You can click the links below to jump to specific sections, but we recommend that you read this Privacy Notice in its entirety.

- [Scope of this Privacy Notice](#)
- [Personal data we collect](#)
- [How we use your personal data](#)
- [How we share your personal data](#)
- [Your choices](#)
- [Other sites and services](#)
- [Security and retention](#)
- [International data transfers](#)
- [Children](#)
- [Changes to this Privacy Notice](#)
- [How to contact us](#)
- [California privacy notice](#)
- [Notice to European users](#)

Scope of this Privacy Notice

Front provides businesses with a cloud-based communication hub that their teams use for customer-related communications. The Service is not intended for use by individuals for personal, family, household, or other consumer purposes, and the personal data covered by this Privacy Notice pertains to individuals acting in a business or commercial capacity. This Privacy Notice does not apply to personal data about Front personnel or job candidates, or to personal data that Front processes on behalf of customers in our capacity as a processor or service provider.

Personal data we collect

The personal data we collect from you, either directly or indirectly, will depend on how you interact with us and with our Service. We collect personal data about you from the following sources:

Information you provide to us. Personal data you may provide to us through the Service, at our online or offline events, through our promotions and surveys, when visiting our offices, or otherwise includes:

- **Contact data.** Your full name, professional title, organization name, email address, mailing address, phone number, social media handle, and other contact details.
- **Account data.** Your full name, email address, the password for your Service account, your country, and any other information you choose to add to your Service profile or associate with your account, such as your avatar, industry, country, pronouns, birthdate, or hobbies.
- **Transaction data.** Any payment card data or banking details you chose to use to pay for the Service, and information about your transactions with us.
- **Communications data.** Information in your communications with us, including when you communicate with us through the Service, social media, events, or otherwise; respond to surveys; provide feedback; or post to our blogs/forums. This includes both the content of these communications and the contact details and metadata associated with it, such as social media handles, profile photos that you use with your social and email accounts, calendar appointment details; and the date/time of the communication. We and our service providers may monitor and record calls/videoconferences with our support or sales teams and other communications for training and quality assurance purposes and the other purposes described in the How we use your personal data section below.
- **Security data.** Security camera footage of our offices, facilities and event spaces.
- **Referral data.** Contact details of friends or contacts that you refer to us or that refer you, such as when you invite them or are invited by them to use the Service. You should your friends' or contacts' information with us unless you have permission to do so.

If we collect personal data not specifically listed above, we will use it consistent with this Privacy Notice or as otherwise explained at the time of collection.

Information automatically collected. As you navigate the Service, our communications, and other online services, we, our service providers, and our advertising partners may automatically collect information about you, your computer or device, and your browsing actions and usage activity, such as:

- **Device data.** Technical information about your computer or mobile device, including operating system type and version, manufacturer and model, browser type, screen resolution, RAM and disk size, CPU usage, device type (e.g., phone, tablet), IP address, unique device identification numbers or other identifiers (including identifiers used for advertising purposes), language settings, mobile device/cellular carrier, radio/network information (e.g., Wi-Fi, LTE, 3G), and general location information associated with IP address (e.g., city/town).
- **Usage data.** Page and screen views, search terms, authentication details, how long you spent on a page or screen, the website you visited before browsing to the Service, navigation paths between pages/screens, information about your activity on a page/screen, access times and duration of access, whether you have opened our emails or clicked links within them, and other functional information on Service performance (like diagnostics and crash logs).

Cookies and other technologies. Some of the information we collect automatically is captured using cookies and other technologies as described in our [Cookie Notice](#).

Third party sources. We combine personal data we receive from you or collect automatically when you use the Service with personal data we obtain from other sources, such as:

- Our business contacts who share details about their professional contacts and friends, including potential customers and partners.
- Public sources, including government records, information you submit in public forums, and information made publicly available on social media and company website bios (e.g., names, job titles, professional history and training/certifications).
- Data brokers who provide contact details and biographical details (e.g., professional/education history) about potential customers and help us keep the details in our database up to date.
- Authentication services you can use to log into the Service, such as those provided by Google, and Microsoft, which may share information about you to facilitate the authentication as described in the service's settings or privacy policy.
- Social media accounts that you connect to the Service, such as when you use a social media widget in the Service to "like" content in the Service. When you do this, the social platform may share your profile or other personal data about you with us. You may be able to limit the information shared with us in the settings of your social media account.

How we use your personal data

We use your personal data for the following purposes or as otherwise described in this Privacy Notice or at the time of collection:

Service delivery. We use your personal data to register your Service account, to manage and administer your Service account, provide the Service and to communicate with you about our Service (including support and administrative messages).

Business operations. We use your personal data to administer and maintain our Service and our IT systems (including monitoring, troubleshooting, data analysis, testing, system maintenance, repair and support, reporting and hosting of data) and to operate our business.

Research and development. We use your personal data for research and development purposes, including to analyze and improve the Service and our business in an informed way. As part of these activities, we may create aggregated, de-identified and/or anonymized data from personal data we collect. We make personal data into de-identified or anonymized data by removing information that makes the data personally identifiable to you. We may use this aggregated, de-identified or otherwise anonymized data and share it with third parties for our lawful business purposes, including to analyze, improve and promote the Service and our business.

Marketing. As permitted by applicable law, we may collect and use your personal data to send you marketing emails or contact you by phone about our and/or our partners' products, services or events. You may opt-out of our marketing communications as described in the [Opt-out of marketing](#) section below.

Targeted advertising. Our third-party advertising partners may use cookies and similar technologies to collect information about your use of the Service (including the device data and usage data described above), our communications, and other online services over time and with different browsers and devices. Our advertising partners use that information to show you ads online that they think will interest you and measure the ads' performance. We may also share individuals' contact data with our advertising partners to facilitate interest-based advertising on their platforms (e.g., social media platforms) to those individuals or others with similar traits.

Compliance and protection. We use your personal data to comply with applicable laws, lawful requests, and legal process, such as to respond to subpoenas or requests from government authorities. We also use your personal data to protect our, your or others' rights, privacy, safety, or property (including by establishing and defending legal claims), including by conducting internal audits against our policies; enforcing the terms and conditions that govern the Service; and taking steps to prevent, investigate and deter fraud, cyberattacks or other unauthorized, unethical, or illegal activity.

We, our service providers and the third parties we work with may use artificial intelligence (AI) and machine learning technologies, including generative AI, to facilitate the processing of personal data described above.

How we share your personal data

We may share your personal data with the following categories of recipients, at your direction, and as otherwise described in this Privacy Notice or at the time of collection.

Affiliates. We may share all categories of personal data with FrontApp SARL (France), FrontApp Ireland Limited (Ireland), and other corporate affiliates that we control, are controlled by, or with which we are under common control, for purposes consistent with this Privacy Notice.

Service providers. We may share all categories of personal data with third parties that provide services on our behalf or help us operate the Service or our business (such as hosting, information technology and software, customer support, email and telephone communications, call recording, marketing, advertising, payment processing, user authentication, market/survey research, data brokerage, generative artificial intelligence, and analytics).

Payment processors. Third party payment processors, such as [Stripe](#), that collect your payment card data and other transaction data to process your payment card transactions when you pay for the Service. You can learn about how Stripe handles your personal data in its privacy policy available here: <https://stripe.com/privacy>. We also give you the option to use third party services such as [Plaid](#) to gather your account and banking details from your bank. By using Plaid to gather this data, you grant us and Plaid the right, power, and authority to act on your behalf to access and transmit your personal financial information from the relevant financial institution. You agree to your personal and financial information being transferred, stored, and processed by Plaid as described in Plaid's privacy policy currently available at <https://plaid.com/legal/#end-user-privacy-policy> and you expressly agree to its terms and conditions.

Authentication services. When you log into the Service by using your credentials on a third party service, such as Google and Microsoft, the service will collect contact data, device data and usage data from you to facilitate the authentication as described in the service's relevant settings or privacy policy.

Advertising partners. Third party advertising companies collect, and we share with them, personal data for targeted advertising purposes as described above, including the companies placing third party advertising cookies identified in our Cookie Notice. Their use of personal data is subject to their own privacy policies.

Other users and the public. Other users of our blogs and forums to which you post content visible to them, such as community.front.com, parts of which are publicly accessible.

Professional advisors. We may share all categories of personal data with professional advisors, such as lawyers, auditors, and bankers, where necessary in the course of the professional services that they render to us.

Authorities and others. We may share all categories of personal data with law enforcement, government authorities, and private parties, as we believe in good faith to be necessary or appropriate for the [compliance and protection purposes](#) described above. See our [Law Enforcement Data Request Guidelines](#) for details on how we handle law enforcement requests.

Business transferees. Parties (and their advisors) to business transactions involving a corporate divestiture, merger, consolidation, acquisition, reorganization, sale or other disposition of all or any portion of the business or assets of, or equity interests in, Front or our affiliates (including, in connection with a bankruptcy or similar proceedings) may acquire all categories of personal data that we handle in connection with such transactions or we may share it with them in the context of negotiations of or due diligence for such transactions.

Your choices

This section applies to all users. Some users may also have additional rights under applicable privacy laws, as described in the relevant region-specific sections below. If you do not provide information we identify as required or mandatory, we may not be able to provide features or services that require that information.

Access or update your information. You may review and update certain Service account information by logging into your account.

Opt-out of marketing communications. You may opt-out of marketing emails at any time by following the opt-out or unsubscribe instructions at the bottom of the email, or by [contacting us](#). Please note that if you opt-out of promotional emails, you may continue to receive service-related and other non-marketing emails.

Request deletion. California residents may request deletion of their personal information as described in the [California privacy notice](#) below and European users may request deletion as described in the [notice to European users](#) below. Individuals in other jurisdictions may request deletion of their information by [contacting us](#) with their request. We may need to verify your identity and place of residency to process your deletion requests.

Cookies. Most browsers let you remove or reject cookies. To do this, follow the instructions in your browser settings. See our Cookie Notice for more information about how to control cookies.

Do Not Track. Some Internet browsers may be configured to send “Do Not Track” signals to the online services that you visit. We currently do not respond to “Do Not Track” signals. To find out more about “Do Not Track,” please visit <http://www.allaboutdnt.com>.

Other sites and services

The Service may contain links to or integrations of websites and other online services operated by third parties. In addition, our content may be integrated into web pages or other online services that are not associated with us. These links and integrations are not an endorsement of, or representation that we are affiliated with, any third party. We do not control websites or other online services operated by third parties, and we are not responsible for their actions. We encourage you to read the privacy policies of the other websites and other online services you use.

Security and Retention

We use technical and organizational safeguards designed to protect the personal data we collect and process about you. However, security risk is inherent in all internet and information technologies, and we cannot guarantee the security of your personal data.

We retain personal data for as long as necessary to fulfill the purposes for which we collected it, including for the purposes of satisfying any legal, accounting, or reporting requirements, to establish or defend legal claims, or for the compliance and protection purposes described above. Factors determining the appropriate retention period for personal data include the amount,

nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of personal data, the purposes for which we process the personal data, whether we can achieve those purposes through other means, and the applicable legal requirements.

When we no longer require the personal data, we have collected about you, we will either delete or anonymize it (so that it is no longer personally identifiable with you) or, if this is not possible (for example, because your personal data has been stored in backup archives), then we will isolate your personal data from any further processing, employing security safeguards designed to protect it until deletion is possible.

International data transfers

We are headquartered in the United States and may use service providers that operate in the United States and other countries other than the country in which you are resident. These countries may have data protection laws that differ from those of your country (and, in some cases may not be as protective as those in your state, province, or country).

Individuals in the European Economic Area, United Kingdom, and Switzerland should read the information provided below about the transfer of personal data outside of those locations.

Children

The Service is not intended for use by anyone under 16 years of age. If you are a parent or guardian of a child under 16 from whom you believe we have collected personal data in a manner prohibited by law, please [contact us](#). If we learn that we have collected personal data through the Service from a child under 16 without the consent of the child's parent or guardian as required by law, we will comply with applicable legal requirements to delete the information.

Changes to this Privacy Notice

We reserve the right to modify this Privacy Notice at any time. If we make material changes to this Privacy Notice, we will notify you by updating the date of this Privacy Notice and posting it on the Service or other appropriate means. Any modifications to this Privacy Notice will be effective upon our posting the modified version (or as otherwise indicated at the time of posting). In all cases, your use of the Service after the effective date of any modified Privacy Notice indicates your acknowledgment that the modified Privacy Notice applies to your interactions with the Service and our business.

How to contact us

If you have questions or concerns about this Privacy Notice or our practices, please contact us at privacy@front.com.

California privacy notice

This notice describes our collection, use and disclosure of personal information of California residents in our capacity as a "business" under the California Consumer Privacy Act ("CCPA")

and their rights with respect to their personal information. For purposes of this notice, “personal information” has the meaning given in the CCPA but does not include information exempted from the scope of the CCPA.

Information practices. The following describes our practices currently and during the past 12 months:

- Collection and disclosure.** The chart below describes the personal information we collect by reference to the statutory categories of personal information specified in the CCPA’s definition of “personal information”, and the categories of third parties to whom we disclose it. The terms in the chart refer to the categories of information described above under Personal data we collect and the categories of third parties described above under How we share your personal data. We collect all categories of personal information from the sources described in Personal data we collect and use them for the business/commercial purposes described in How we use your personal data. Information you voluntarily provide to us, such as in free-form webforms, may contain other categories of personal information not described below. We may also disclose personal information to professional advisors, law enforcement and government authorities, and business transferees as described in the [How we share your personal data](#) section of this Privacy Notice.

Statutory category/ personal information we collect	Categories of third parties to whom we disclose the personal information for a business purpose
<p>Identifiers</p> <ul style="list-style-type: none"> • Contact data • Account data • Communications data • Device data • Referral data 	<ul style="list-style-type: none"> • Affiliates • Service providers • Payment processors • Authentication services • Other users and the public
<p>California Customer Records (as defined in California Civil Code §1798.80)</p> <ul style="list-style-type: none"> • Contact data • Account data • Transaction data • Communications data • Referral data 	<ul style="list-style-type: none"> • Affiliates • Service providers • Payment processors • Other users and the public
<p>Commercial Information</p> <ul style="list-style-type: none"> • Device data 	<ul style="list-style-type: none"> • Affiliates • Service providers • Payment processors

<ul style="list-style-type: none"> • Usage data • Transaction data 	<ul style="list-style-type: none"> • Authentication services
<p>Internet or Network Information</p> <ul style="list-style-type: none"> • Device data • Usage data 	<ul style="list-style-type: none"> • Affiliates • Service providers
<p>Geolocation data</p> <ul style="list-style-type: none"> • Usage data • Precise geolocation data 	<ul style="list-style-type: none"> • Affiliates • Service providers
<p>Audio, Electronic, Visual, Thermal, Olfactory, or Similar Information</p> <ul style="list-style-type: none"> • Security data • Communications data • Device data • Usage data 	<ul style="list-style-type: none"> • Affiliates • Service providers
<p>Professional or Employment Information</p> <ul style="list-style-type: none"> • Contact data • Account data 	<ul style="list-style-type: none"> • Affiliates • Service providers
<p>Education Information</p> <ul style="list-style-type: none"> • Contact data • Account data 	<ul style="list-style-type: none"> • Affiliates • Service providers
<p>Sensitive personal information</p> <ul style="list-style-type: none"> • Account data (Service account or third party service passwords) • Transaction data (payment card information) • Precise geolocation data 	<ul style="list-style-type: none"> • Affiliates • Service providers • Payment processors • Authentication services
<p>Inferences</p> <p>May be derived from all the above</p>	<ul style="list-style-type: none"> • Affiliates • Service providers

- **Sales and sharing of personal information.** Our use of the targeted advertising services described above may constitute the “sharing” or “sale” of personal information (including the identifiers, California customer records, commercial information and inferences described in the chart above) under the CCPA from which you have the right to opt-out. Click the Your Privacy Choices link in the footer of this webpage for instructions on exercising this opt-out right. Your request to opt-out will apply only to the browser and the device from which you submit the request. Although our Services are not intended for children under 16 years of age, we are required to inform you that we do not have actual knowledge that we have sold the personal information of California residents under the age of 16.
- **Sensitive personal information.** We do not use or disclose sensitive personal information for purposes subject to the right to limit the use and disclosure of sensitive personal information under the CCPA.
- **Retention.** We retain personal information as described in the security and retention section above.

Your privacy rights. As a California resident, you have the following rights under the CCPA:

- **Right to know.** You can request information about the categories of personal information that we have collected; the categories of sources from which we collected personal information; the business or commercial purpose for collecting, sharing and/or selling personal information; the categories of any personal information that we sold or disclosed for a business purpose; and the categories of any third parties with whom personal information was sold, shared or disclosed for a business purpose.
- **Right to access.** You can request a copy of certain personal information that we have collected about you.
- **Right to deletion.** You can request that we delete personal information that we collected from you.
- **Right to correction.** You can request that we correct inaccurate personal information that we have collected about you.
- **Nondiscrimination.** You are entitled to exercise the rights described above free from discrimination as prohibited by the CCPA.

Exercising your rights. You may submit requests to exercise your right to know, access, deletion and correction by contacting us. The rights described above are not absolute, and in certain cases, we may decline your request as permitted by law. We cannot process your request if you do not provide us with sufficient detail to allow us to understand and respond to it.

Identity verification. We need to verify your identity to process your requests to exercise your rights to know, access, deletion, and correction, and we reserve the right to confirm your California residency. To verify your identity, we may require you to log into a Service account if you have one, provide identifiers we can match against information we may have collected from you previously, confirm your request using the email address or telephone number that we have on record, provide government identification, or provide a declaration under penalty of perjury, where permitted by law.

Authorized agents. Your authorized agent may make a request on your behalf upon our verification of the agent's identity and our receipt of a copy of a valid power of attorney given to your agent pursuant to applicable state law. If you have not provided your agent with such a power of attorney, we may ask you and/or your agent to take additional commercially reasonable steps permitted by law to verify that your request is authorized, such as by verifying your identity directly with us, providing proof that you have given the authorized agent signed permission to submit the request, and directly confirming with us that you gave the authorized agent such permission.

Notice to European users

The information provided in this notice applies only to individuals in the United Kingdom (“**UK**”), the European Economic Area (“**EEA**”) and Switzerland (we collectively refer this group of countries as “**Europe**”). This notice applies in the event of any conflict or inconsistency between this notice and the other provisions of this Privacy Notice.

The personal data that we collect from you is identified and described in greater detail in the section of the Privacy Notice entitled Personal data we collect.

Controller. FrontApp, Inc. is the controller of your personal data described in this Privacy Notice unless you have entered into a service contract with or received direct marketing communications from a different Front affiliate, in which case that entity is the controller. If you have questions about the controller of your personal data, please [contact us](#). You may contact the relevant controller by email at privacy@front.com or by mail at:

FrontApp, Inc., 300 Montgomery Street, Floor 5, San Francisco, California 94104, USA
FrontApp Ireland Limited, 21-23 City Quay, 4th Floor, Dublin 2, D02 FP21, Ireland
FrontApp SARL, 32 Rue René Boulanger, 75010 Paris, France

Legal bases for processing. European data protection law requires that we have a “legal basis” for each purpose for which we process your personal data. Depending on the purpose for collecting your information, we may rely on one of the following legal bases:

- The processing is necessary to perform a contract that we are about to enter into, or have entered into, with you (“**Contractual Necessity**”).
- The processing is necessary to pursue our legitimate interests or those of a third party and we are confident that your privacy rights will be appropriately protected (“**Legitimate Interests**”).
- We need to comply with laws or to fulfill certain legal obligations (“**Compliance with Law**”).
- We have your specific consent to carry out the processing for the purpose in question (“**Consent**”). Generally, we do not rely on Consent as a legal basis for using your personal data other than in the context of direct marketing communications where required by applicable law. In some circumstances we are required to obtain your consent to use non-essential cookies or similar tracking technologies or to send direct marketing emails. Obtaining your consent in accordance with our obligations under

applicable laws implementing the ePrivacy Directive does not necessarily mean that we will rely on consent to process your personal data for these purposes under GDPR.

The table below identifies the legal bases we rely on in respect of the relevant purposes for which we use your personal data. For more information on these purposes and the categories of personal data involved, see the section in the Privacy Notice entitled [How we use your personal data](#).

Processing purpose	Types of personal data processed	Legal basis
Service delivery	<ul style="list-style-type: none"> ● Contact data ● Account data ● Payment data ● Communication data ● Device data ● Usage data ● Precise geolocation data ● Referral data 	Contractual Necessity. If we have not entered a contract with you, we process your personal data based on our Legitimate Interests (in providing the Services you access or request)
Business operations	<ul style="list-style-type: none"> ● Contact data ● Account data ● Communication data ● Device data ● Usage data ● Precise geolocation data ● Referral data 	Contractual Necessity. If we have not entered a contract with you, we process your personal data based on our Legitimate Interests (in operating, providing, and improving our business)
Research and development	<ul style="list-style-type: none"> ● Contact data ● Account data ● Communication data ● Device data ● Usage data ● Precise geolocation data ● Referral data 	Our Legitimate Interests (in analyzing and improving our Services and our business).
Marketing	<ul style="list-style-type: none"> ● Contact data ● Account data ● Communication data ● Device data ● Usage data ● Precise geolocation data ● Referral data 	Our Legitimate Interests (in promoting our products and services through marketing communications). We are required to rely on your Consent to the transmission of direct marketing emails in line with our obligations under applicable

		laws implementing the ePrivacy Directive, as explained above.
Targeted advertising	<ul style="list-style-type: none"> • Contact data • Device data • Usage data 	Our Legitimate Interests (in promoting our products and services through targeted advertisements).
Sharing your personal data as described in this Privacy Notice	<ul style="list-style-type: none"> • Contact data • Account data • Communication data • Referral data 	We use the original legal basis relied upon if the relevant further use is compatible with the initial purpose for which the personal data was collected. Otherwise, we rely on your Consent .
Compliance and Protection	<ul style="list-style-type: none"> • Security data • Precise geolocation data • All other data relevant in the circumstances 	Compliance with Law (where processing is necessary to comply with our legal obligations). Otherwise, we rely on our Legitimate Interests (in protecting our, your or others’ rights, privacy, safety or property).
Any of the above purposes facilitated by cookies, similar technologies or precise geolocation data	<ul style="list-style-type: none"> • Device data • Usage data • Precise geolocation data 	<p>Our Legitimate Interests (in operating, providing, and improving our business and promoting our products and services).</p> <p>We are required to rely on your consent to the use of cookies or similar tracking technologies in line with our obligations under applicable laws implementing the ePrivacy Directive, as explained above.</p>

Use for new purposes. We may use your personal data for reasons not described in this Privacy Notice where permitted by law and the reason is compatible with the purpose for which we collected it. If we need to use your personal data for an unrelated purpose, we will notify you and explain the applicable legal basis.

Special categories of data. We do not collect sensitive data defined by the GDPR as “special categories of data” (i.e., personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic or biometric data

processed for the purpose of uniquely identifying a natural person; data concerning health or data concerning a natural person's sex life or sexual orientation) and ask that you do not provide us with any such information.

Your rights. European data protection laws give individuals in Europe the following rights regarding their personal data:

- **Right of access.** You can ask us to provide you with information about our processing of your personal data and give you access to your personal data.
- **Right to rectification.** If the personal data we hold about you is inaccurate or incomplete, you are entitled to request to have it rectified.
- **Right to erasure.** You can ask us to delete or remove your personal data where there is no lawful reason for us continuing to store or process it, where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law.
- **Right to restrict processing.** You can ask us to suspend the processing of your personal data if you want us to establish the information's accuracy; where our use of the information proves to be unlawful but you do not want us to erase it; where you need us to hold the information even if we no longer require it as you need it to establish, exercise or defend legal claims; or if you have objected to our use of your information but we need to verify whether we have overriding legitimate grounds to use it.
- **Right to object.** You can object to our processing of your personal data where we are relying on a legitimate interest (or those of a third party) to do so and you believe it impacts your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes.
- **Right to data portability.** You have the right, in certain circumstances, to ask us to provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format.
- **Right to withdraw consent at any time.** Where we are relying on consent to process your personal data you have the right to withdraw your consent at any time. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent.

Exercising those rights. Please note that some of these rights may be limited where we have an overriding interest or legal obligation to continue to process the personal data or where certain exemptions apply. If we decline your request, we will tell you why, subject to legal restrictions.

To exercise any of these rights, please [contact us](#). We may request specific information from you to help us confirm your identity and process your request.

Your right to lodge a complaint with your supervisory authority. If you are not satisfied with our response to a request you make, or how we process your personal data, you can make a complaint to the data protection regulator in your habitual place of residence.

For individuals in the EEA: The contact information for the data protection regulator in your place of residence can be found here: https://edpb.europa.eu/about-edpb/board/members_en

For individuals in the UK: The contact information for the UK data protection regulator is below:

The Information Commissioner's Office
Water Lane, Wycliffe House
Wilmslow - Cheshire SK9 5AF
Tel. +44 303 123 1113
Website: <https://ico.org.uk/make-a-complaint/>

For individuals in Switzerland: You may contact the Swiss data protection regulator here: <https://www.edoeb.admin.ch/edoeb/en/home/deredoeb/kontakt.html>

International data transfers. We are headquartered in the United States and may use service providers that operate in the United States and other countries. Therefore, we may transfer your personal data to recipients outside of the European Economic Area, UK, and Switzerland. Some of these recipients are located in countries which have been formally recognized as providing an adequate level of protection for personal data by the relevant governmental body in the European Union, UK or Switzerland, as applicable, in which case, we rely on the relevant "adequacy decisions". Where the transfer is not subject to an adequacy decision or regulations, we take appropriate safeguards to ensure your personal data remains protected in accordance with this Privacy Notice and applicable laws by entering into appropriate data transfer mechanism permitted under Article 46 of the GDPR / UK GDPR (as applicable). With respect to data transfers to the United States, FrontApp, Inc. relies on its certification to the United States Department of Commerce that we adhere to the Data Privacy Framework Principles ("Principles") of the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework, as further described in the Front Data [Privacy Framework Certification Notice](#), which supplements this Privacy Notice with respect to personal data we process as a controller. Other relevant mechanisms include the [European Commission's Standard Contractual Clauses](#) or the UK International Data Transfer Addendum (as applicable). A copy of our data transfer mechanism can be provided on request.

English version controls

The information provided in non-English translations of this Privacy Notice are provided for convenience only. In the event of any ambiguity or conflict between translations, the English version is authoritative and controls.