Preava Application Privacy Notice

Effective on: October 22nd, 2020
Last updated on: January 29th, 2024

Introduction

At Preava, Inc. ("Preava", "we", "us", "our"), privacy is part of our mission. We take the protection of personal data ("Personal Data") very seriously. Please read this privacy notice (the "Notice") to learn what we're doing with your Personal Data, how we protect it, and what privacy rights you have under data protection and privacy laws, such as:

- the European Union General Data Protection Regulation ("GDPR"); and
- U.S. state privacy laws, including, but not limited to: the California Consumer Privacy Act ("CCPA"); the Colorado Privacy Act; the Connecticut Data Privacy Act; and the Virginia Consumer Data Protection Act. Collectively, these laws and their associated regulations, if any, are referred to as "U.S. State Privacy Laws."

What Is Covered by this Privacy Notice?

This Notice addresses individuals (or "data subjects") whose Personal Data we may receive from our direct customers ("Customers") in our web-based software application (the "Application").

Our Customers license our Application to help prevent data breaches. Since the Application scans Customer's emails for suspected security issues, the Application has access to any Personal Data that each such email message contains. The Application therefore processes the Personal Data of a variety of types of data subjects, including our Customers themselves (if they're individuals), employees and contractors of our direct Customers (if they're organizations), our Customers' customers or email contacts, and any other individuals whose Personal Data our Customers include in an email message scanned by our Application.

Our Customers use our Application to store and process Personal Data of themselves, their own customers, clients, employees, and others. When Preava processes Personal Data on behalf of our Customers in our Application, we act only as a data processor or as a "service provider" under the CCPA. We do not decide what Personal Data our Customers submit to or scan with our Application. In general, we will only access such Personal Data as necessary in order to provide and maintain the Application, at a Customer's request in connection with technical support or account administration matters, or if we are required to do so by law.

For information about how our Customers use your Personal Data, please contact the relevant Preava Customer directly or refer to the Customer's privacy notice.

Also, if our Customers agree that we may do so, we may process the Personal Data our Customers store and process in our Application by irreversibly anonymizing it and using that anonymized

data to improve our Application, including by training the machine learning and artificial intelligence functionalities in the Application. When Preava processes Personal Data for our own purposes and means in our Application, we act as a data controller or as a "business" under the CCPA.

What Is Not Covered by this Privacy Notice?

General and Website Personal Data

This Notice does not apply to the Personal Data of data subjects (which includes both individuals and households) whose Personal Data we:

- receive directly through our website(s);
- receive from our business partners; or
- process to promote our products and services.

Please see our General Privacy Notice for more information on how we handle this type of information.

Human Resources Personal Data

This Notice does not apply to the Personal Data of employees, job applicants, contractors, business owners, directors, officers, or other personnel of Preava.

Information Which Does Not Constitute Personal Data

If we do not maintain information in a manner that identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular individual or household, such information is not considered "Personal Data" and this Notice will not apply to our processing of that information.

What Can You Find in this Notice?

This Notice tells you, among other things:

- What Personal Data we collect about you and how we obtain it;
- The legal bases for processing your Personal Data;
- For what purposes we use that Personal Data;
- How long we keep your Personal Data;
- To whom we disclose your Personal Data;
- Your rights about the Personal Data we collect about you and how you can exercise those rights;
- How we protect your Personal Data; and
- How to contact us.

Our Role with Respect to Your Personal Data

There is Personal Data that we process for our own purposes and Personal Data that we process on behalf of our Customers. This means that we do not always have the same degree of decision-making with respect to why and how each piece of Personal Data will be processed.

- Regarding the Personal Data of individuals that Preava processes for our Customers in our Application, we generally act as an agent, also known as a data processor or "service provider" under the CCPA. This means that our Customers determine the type(s) of

Personal Data they provide for us to process on their behalf. We typically have no direct relationship with the individuals whose Personal Data we receive from our Customers, unless the Personal Data is that of our Customers themselves (if they're individuals).

- If our Customers agree that we may do so, Preava may also process the Personal Data of individuals in our Application by irreversibly anonymizing it and using that anonymized data to train the machine learning and artificial intelligence functionalities in the Application. When Preava acts in this role, we decide the purposes and means of processing, and consequently act as a data controller or as a "business" under the CCPA.
- Regarding the Personal Data of users of our website(s) generally or business contacts and prospects of Preava, we decide the purposes and means of processing, and consequently act as a data controller or "business." For more information regarding how we treat this type of data, please see our General Privacy Notice.

Lawfulness of Processing

When acting as a data processor, Preava processes Personal Data within the scope of this Notice based on the instructions of our Customers. To learn about the lawful grounds on which they process your Personal Data, please contact the Preava Customer who used our Application to process your Personal Data directly or refer to their privacy notice.

When acting as a data controller, we must have a valid reason to use your Personal Data (i.e., a "lawful basis for processing"). We may process your Personal Data on the basis of:

- your consent;
- to perform a contract with you or to take steps at your request before entering into a contract;
- our legitimate interests, such as our interest in improving and training the Application;
- the need to comply with the law; or
- any other ground, as required or permitted by law.

When we rely on legitimate interests as a lawful basis of processing, you have the right to ask us more about how we decided to choose this legal basis. To do so, please use the contact details provided here.

Where we process your Personal Data based on your consent, you may withdraw it at any time. However, this will not affect the lawfulness of our processing before you withdraw your consent. It will also not affect the validity of our processing of Personal Data performed on other lawful grounds.

What Personal Data We Process and How We Obtain It

The table below describes the categories of Personal Data we have collected about you in the last twelve months.

Personal Data We Collect, Process, or Store	How We Obtain It
Identifiers	We obtain identifiers contained in emails that our Customers scan with our Application.

Names, online identifiers, Internet Protocol (IP) addresses, email addresses.	
Sensitive or special categories of Personal Data We may process sensitive or special categories of Personal Data, including information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, data concerning health, or data concerning a natural person's sex life or sexual orientation if such data is included, directly or indirectly, in an email processed in our Application.	While we do not intentionally collect sensitive or special categories of Personal Data, we process all information contained in emails that our Customers scan with our Application.
Protected characteristics We may process personal information with protected characteristics such as age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, or genetic information (including familial genetic information) if such data is included, directly or indirectly, in an email processed in our Application.	While we do not intentionally collect personal information with protected characteristics, we process all information contained in emails that our Customers scan with our Application.
Commercial information We may process commercial information such as records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies if such data is included, directly or indirectly, in an email processed in our Application.	While we do not intentionally collect commercial information, we process all information contained in emails that our Customers scan with our Application.
Biometric information We may process biometric information such as genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or	While we do not intentionally collect biometric information, we process all information contained in emails that our Customers scan with our Application.

identifying information, such as fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data, if such data is included, directly or indirectly, in an email processed in our Application.	
Internet or other similar network activity We may process browsing history, search history, and information on a consumer's interaction with a website, application, or advertisement if such data is included, directly or indirectly, in an email processed in our Application.	We process internet and network activity information contained in emails that our Customers scan with our Application.
Geolocation data Physical location or movements, including IP addresses.	We process geolocation data, including IP addresses, contained in emails that our Customers scan with our Application. Our Application also collects these categories of Personal Data automatically whenever an authorized user of the Application interacts with the Application.
Professional or employment-related information We may process current or past job history or performance evaluations and job title if such data is included, directly or indirectly, in an email processed in our Application.	While we do not intentionally collect professional or employment-related information, we process all information contained in emails that our Customers scan with our Application.
Non-public education information We may process education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	While we do not intentionally collect non-public education information, we process all information contained in emails that our Customers scan with our Application.
Inferences drawn from other Personal Data Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	While we do not intentionally collect inferences drawn from other Personal Data, we process all information contained in emails that our Customers scan with our Application.

We will not intentionally collect additional categories of Personal Data without informing you. However, we have access to all information contained in emails that our Customers scan with our Application. We cannot control what Personal Data our Customers process in our Application. This means that additional categories of Personal Data may be processed by us solely for the purpose of carrying out the Application's functionality. Whether or not additional categories of Personal Data are included in a given scanned email is under the sole control of our Customers and the authors of any scanned emails.

Cookies

A "cookie" is a small file stored on your device that contains information about your device. We may use cookies to provide application functionality, authentication (session management), usage analytics (web analytics), to remember your settings, and to generally improve our Application.

We use session and persistent cookies. Session cookies are deleted when you close your browser. Persistent cookies may remain even after you close your browser, but always have an expiration date. Most of the cookies placed on your device through our Application are first-party cookies, since they are placed directly by us. Other parties, such as Google, may also set their own (third-party) cookies through our Application. Please refer to the policies of these third parties to learn more about the way in which they collect and process information about you.

If you would prefer not to accept cookies, you can change the setup of your browser to reject all or some cookies. Note, if you reject certain cookies, you may not be able to use all of our Application's features. For more information, please visit https://www.aboutcookies.org/.

You may also set your browser to send a Do Not Track (DNT) signal. For more information, please visit https://allaboutdnt.com/. Please note that our Application does not have the capability to respond to "Do Not Track" signals received from web browsers.

For more information about our use of cookies, please see our Cookie Notice.

For What Purposes Do We Use Your Personal Data?

If you are a Customer or a Customer employee, we may process your Personal Data on the instructions of our Customers for the following business purposes:

- to enable the use of our Application;
- to provide you with information or products that you request from us;
- to respond to your requests or questions;
- to fulfill legal obligations and enforce our rights;
- to improve and train our Application; and
- to send you email marketing communications about our business which we think may interest you.

If you are an individual whose Personal Data was contained in an email that a Preava Customer processed in our Application, we will only process your Personal Data for the following purposes:

- to provide the features of our Application; and

- if our Customers agree that we may do so, to anonymize it and use that anonymized data to improve and train our Application.

How Long We Keep Your Personal Data

When acting as a data processor, we retain Personal Data for as long as instructed by the respective Customer. We delete the Personal Data submitted to us by our Customers within six months of the end of our service agreement with the Customer, unless applicable laws require otherwise.

When acting as a data controller, when the purposes of processing are satisfied, we will delete the related Personal Data within six (6) months or upon receipt of a verified request.

Your Personal Data may need to be retained in our backup systems and will only be deleted or overwritten at a later time, normally six months after the purpose for processing your Personal Data has been fulfilled. This may be the case even when you or a regulator has validly asked us to delete your Personal Data or when we no longer have a legal basis for processing such Personal Data.

Disclosing Personal Data to Third Parties

We do not "sell" or "share" your Personal Data (as those terms are defined in the CCPA) to third parties within the context of this Notice.

We do, however, make your Personal Data available to our carefully selected third-party service providers and business partners for our own operational business purposes. Preava remains liable for the protection of your Personal Data that we transfer or have transferred to third parties, except to the extent that we are not responsible for the event that leads to any unauthorized or improper processing. In the preceding twelve (12) months, we have disclosed the following categories of Personal Data to third parties for business purposes:

Category	Categories of Third Parties Receiving Personal Data
Identifiers	• Communication service providers • Consent management providers • Financial management providers • Identity and access management tool providers • Infrastructure services providers • Marketing service providers • Office tools providers • Payment processing providers • Project management tool providers • Web analytics providers
Sensitive or special categories of Personal Data	• Infrastructure services providers
Protected characteristics	• Infrastructure services providers

Commercial information	• Communication service providers • Consent management providers • Financial management providers • Identity and access management tool providers • Infrastructure services providers • Marketing service providers • Office tools providers • Payment processing providers • Project management tool providers • Web analytics providers
Biometric information	• Identity and access management tool providers • Infrastructure services providers
Internet or other similar network activity	• Consent management providers • Identity and access management tool providers • Infrastructure services providers • Marketing service providers • Payment processing providers • Web analytics providers
Geolocation data	• Communication service providers • Consent management providers • Identity and access management tool providers • Infrastructure services providers • Marketing service providers • Payment processing providers • Web analytics providers
Professional or employment-related information	• Communication service providers • Identity and access management tool providers • Infrastructure services providers • Marketing service providers • Office tools providers
Non-public education information	• Communication service providers • Identity and access management tool providers • Infrastructure services providers • Marketing service providers • Office tools providers
Inferences drawn from other Personal Data	• Marketing service providers • Web analytics providers

Some of these third parties may be located outside of the European Union or the European Economic Area ("EEA"), the United Kingdom ("UK"), or Switzerland. In some cases, the European Commission may have determined that in some countries, their data protection laws provide a level of protection equivalent to European Union law. You can see here the list of countries that the European Commission has recognized as providing an adequate level of

protection to Personal Data. We will only transfer your Personal Data to third parties in countries not recognized as providing an adequate level of protection to Personal Data when there are appropriate safeguards in place. These safeguards may include 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, or the Standard Contractual Clauses ("SCCs") as approved by the European Commission under Article 46.2 of the GDPR.

Other Disclosures of Your Personal Data

We may disclose your Personal Data to the extent required by law, or if we have a good-faith belief that we need to disclose it in order to comply with official investigations or legal proceedings (whether initiated by governmental/law enforcement officials, or private parties). If we have to disclose your Personal Data to governmental/law enforcement officials, we may not be able to ensure that those officials will maintain the privacy and security of your Personal Data.

We may also disclose your Personal Data if we sell or transfer all or some of our company's business interests, assets, or both, or in connection with a corporate restructuring. Finally, we may disclose your Personal Data to our subsidiaries or affiliates, but only if necessary for business purposes, as described in the section above.

We reserve the right to use, transfer, sell, share, and disclose aggregated, anonymous data for any legal purpose. Such data does not include any Personal Data. The purposes may include analyzing usage trends or seeking compatible advertisers, sponsors, and customers.

What Privacy Rights Do You Have?

You have specific rights regarding your Personal Data that we collect and process. Please note that you can only exercise these rights with respect to Personal Data that we process about you when we act as a data controller or as a "business" under the CCPA. To exercise your rights with respect to information processed by us on behalf of one of our Customers, please read the privacy notice of that Customer.

In this section, we first describe those rights and then we explain how you can exercise those rights.

Right to Know What Happens to Your Personal Data

This is called the right to be informed. It means that you have the right to obtain from us all information regarding our data processing activities that concern you, such as how we collect and use your Personal Data, how long we will keep it, and whom it will be disclosed to, among other things.

We are informing you of how we process your Personal Data with this Notice.

Right to Know What Personal Data Preava Has About You

This is called the right of access. This right allows you to ask for full details of the Personal Data we hold about you, including confirmation of whether or not we process Personal Data concerning you, and, where that is the case, a copy of or access to the Personal Data and certain related information.

Once we receive and confirm that the request came from you or your authorized agent, we will disclose to you:

- The categories of your Personal Data that we process;
- The categories of sources for your Personal Data;
- Our purposes for processing your Personal Data;
- Where possible, the retention period for your Personal Data, or, if not possible, the criteria used to determine the retention period;
- The categories of third parties to whom we disclose your Personal Data;
- If we carry out automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for you;
- The specific pieces of Personal Data we process about you in an easily sharable format;
- If we sold or disclosed your Personal Data for a business purpose, the categories of Personal Data and categories of recipients of that Personal Data;
- If we rely on legitimate interests as a lawful basis to process your Personal Data, the specific legitimate interests; and
- The appropriate safeguards used to transfer Personal Data from the EEA to a third country, if applicable.

Under some circumstances, we may deny your access request. In that event, we will respond to you with the reason for the denial.

Some U.S. State Privacy Laws do not allow us to disclose Social Security numbers, driver's license numbers or other government-issued identification numbers, financial account numbers, any health insurance or medical identification numbers, account passwords, or security questions and answers. We can inform you that we have this information generally, but we may not provide the specific numbers, passwords, etc. to you for security and legal reasons.

Right to Change Your Personal Data

This is called the right to rectification. It gives you the right to ask us to correct without undue delay anything that you think is wrong with the Personal Data we have on file about you, and to complete any incomplete Personal Data.

Right to Delete Your Personal Data

This is called the right to erasure, right to deletion, or the right to be forgotten. This right means you can ask for your Personal Data to be deleted.

Sometimes we can delete your information, but other times it is not possible for either technical or legal reasons. If that is the case, we will consider if we can limit how we use it. We will also inform you of our reason for denying your deletion request.

Right to Ask Us to Change How We Process Your Personal Data

This is called the right to restrict processing. It is the right to ask us to only use or store your Personal Data for certain purposes. You have this right in certain instances, such as where you believe the data is inaccurate or the processing activity is unlawful.

Right to Opt-Out of Certain Processing

Please note that Preava does not "sell" or "share" your Personal Data (as those terms are defined in the CCPA) to third parties within the context of this Notice. However, you may have the right to opt-out of certain other types of processing, such as processing for the purposes of targeted advertising or profiling for use in making automated decisions that significantly impact you.

Right to Ask Us to Stop Using Your Personal Data

This is called the right to object. This is your right to tell us to stop using your Personal Data. You have this right where we rely on a legitimate interest of ours (or of a third party). You may also object at any time to the processing of your Personal Data for direct marketing purposes.

We will stop processing the relevant Personal Data unless: (i) we have compelling legitimate grounds for the processing that override your interests, rights, or freedoms; or (ii) we need to continue processing your Personal Data to establish, exercise, or defend a legal claim.

If we have received your Personal Data in reliance on the Data Privacy Framework, you may also have the right to opt out of having your Personal Data shared with third parties and to revoke your consent to our sharing your Personal Data with third parties. You may also have the right to opt out if your Personal Data is used for any purpose that is materially different from the purpose(s) for which it was originally collected or which you originally authorized.

Right to Port or Move Your Personal Data

This is called the right to data portability. It is the right to ask for and receive a portable copy of your Personal Data that you have given us or that you have generated by using our services, so that you can:

- Move it;
- Copy it;
- Keep it for yourself; or
- Transfer it to another organization.

We will provide your Personal Data in a structured, commonly used, and machine-readable format. When you request this information electronically, we will provide you with a copy in electronic format.

Right to Withdraw Your Consent

Where we rely on your consent as the legal basis for processing your Personal Data, you may withdraw your consent at any time. If you withdraw your consent, our use of your Personal Data before you withdraw is still lawful.

If you have given consent for your details to be disclosed to a third party and wish to withdraw this consent, please also contact the relevant third party in order to change your preferences.

Right to Non-Discrimination

We will not discriminate against you for exercising any of your privacy rights. Unless the applicable data protection laws permit it, we will not:

- Deny you goods or services;

- Charge you different prices or rates for goods or services, including through granting discounts or other benefits or imposing penalties;
- Provide you a different level or quality of goods or services; or
- Suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

Right to Lodge a Complaint with a Supervisory Authority

If the GDPR applies to our processing of your Personal Data, you have the right to lodge a complaint with a supervisory authority if you are not satisfied with how we process your Personal Data.

Specifically, you can lodge a complaint in the Member State of the European Union of your habitual residence, place of work, or the alleged violation of the GDPR.

Right to Appeal a Denial of a Request to Exercise Your Privacy Rights

Under certain U.S. State Privacy Laws, if we deny a request to exercise your privacy rights, you may have the right to appeal that decision. You can submit an appeal by responding to our correspondence regarding your request, or by contacting us using the methods listed below for exercising your rights.

How Can You Exercise Your Privacy Rights?

To exercise any of the rights described above, please submit a request by either:

- Contacting us by email at privacy@preava.com; or
- Writing to us by postal mail at:

Preava, Inc.
Attn: Chief Privacy Officer
22 Essex Way #8203
Essex, VT 05451
USA

Verification of Your Identity

In order to correctly respond to your privacy rights requests, we need to confirm that YOU made the request. Consequently, we may require additional information to confirm that you are who you say you are.

We will verify your identity via the following methods: checking information provided by you against your account with us; or asking you about information that matches the information that we already have about you.

We will only use the Personal Data you provide us in a request to verify your identity or authority to make the request.

Verification of Authority

If you are submitting a request on behalf of somebody else, we will need to verify your authority to act on behalf of that individual. When contacting us, please provide us with proof that the

individual gave you signed permission to submit this request, a valid power of attorney on behalf of the individual, or proof of parental responsibility or legal guardianship. Alternatively, you may ask the individual to directly contact us by using the contact details above to verify their identity with Preava and confirm with us that they gave you permission to submit this request.

Response Timing and Format of Our Responses

We will confirm the receipt of your request within ten (10) days, and, in that communication, we will also describe our identity verification process (if needed) and when you should expect a response, unless we have already granted or denied the request.

Please allow us up to one month to reply to your requests from the day we receive your request. If we need more time (up to three months or ninety (90) days, whichever is less, in total), we will inform you of the reason why and the extension period in writing.

If we cannot satisfy a request, we will explain why in our response. For data portability requests, we will choose a format to provide your Personal Data that is readily usable and should allow you to transmit the information from one entity to another entity without difficulty.

We will not charge a fee for processing or responding to your requests. However, we may charge a fee if we determine that your request is excessive, repetitive, or manifestly unfounded. In those cases, we will tell you why we made that determination and provide you with a cost estimate before completing your request.

Privacy of Children

The Application is not directed at, or intended for use by, children under the age of 16. However, we cannot control what Personal Data our Customers process in our Application.

Data Integrity & Security

We are strongly committed to keeping your Personal Data safe. We have implemented and will maintain technical, administrative, and physical measures that are reasonably designed to help protect your Personal Data from unauthorized processing. Unauthorized processing includes unauthorized access, exfiltration, theft, disclosure, alteration, or destruction.

As a company founded to help our customers improve their own privacy and security, Preava takes great pride in protecting your Personal Data with industry-leading data protection standards and technical security measures, including strong encryption and redaction.

Data Privacy Framework

Preava complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Preava has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of Personal Data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Preava has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of Personal Data received from Switzerland in reliance on the Swiss-U.S. DPF. If there

is any conflict between the terms in this Notice and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

Dispute Resolution

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, Preava commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EU, UK, and Swiss individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF should first contact Preava by email at privacy@preava.com or by postal mail at:

Preava, Inc.
Attn: Chief Privacy Officer
22 Essex Way, #8203
Essex, VT 05451
USA

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, Preava commits to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF to the VeraSafe Data Privacy Framework Dispute Resolution Procedure, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit https://www.verasafe.com/privacy-services/dispute-resolution/submit-dispute/ for more information or to file a complaint. The services of the VeraSafe Data Privacy Framework Dispute Resolution Procedure are provided at no cost to you.

Binding Arbitration

If your dispute or complaint related to your Personal Data that we received in reliance on the Data Privacy Framework cannot be resolved by us, nor through the dispute resolution mechanism mentioned above, you may have the right to require that we enter into binding arbitration with you under the Data Privacy Framework "Recourse, Enforcement and Liability" Principle and Annex I of the Data Privacy Framework. Additional information is available in Annex I: https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf?tabset-35584=2.

U.S. Regulatory Oversight

The Federal Trade Commission has jurisdiction over Preava's compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

Data Transfer Mechanisms

Preava uses the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, or the Standard Contractual Clauses ("SCCs") as approved by the European Commission under Article 46.2 of the GDPR as its primary data transfer mechanisms for transferring Personal Data

from the EU, UK, and Switzerland. These data transfer mechanisms are formally integrated into our agreements with third parties from whom and on behalf of whom we receive EU, UK, and Swiss Personal Data.

In addition, Preava regularly reviews and confirms its compliance with the most up-to-date guidance and obligations on valid data transfer under applicable privacy regulations. If we find it necessary to update the data transfer mechanism used, we will update this Privacy Notice accordingly.

Changes to this Notice

If we make any material change to this Notice, we will post the revised Notice to this web page and notify our Customers. We will also update the "last updated" date.

Contact Us

If you have any questions about this Notice or our processing of your Personal Data, or want to submit a verifiable consumer request, please write to our Chief Privacy Officer by email at privacy@preava.com or by postal mail at:

Preava, Inc.
Attn: Chief Privacy Officer
22 Essex Way, #8203
Essex, VT 05451
USA

Please allow up to four weeks for us to reply.

European Union Representative

We have appointed VeraSafe as our representative in the EU for data protection matters. While you may also contact us, VeraSafe can be contacted on matters related to the processing of Personal Data. VeraSafe can be contacted using this contact form, by telephone at: +420 228 881 031, or by postal mail at:

VeraSafe Ireland Ltd.
Unit 3D North Point House
North Point Business Park
New Mallow Road
Cork T23AT2P
Ireland

UK Representative

We have appointed VeraSafe as our representative in the UK for data protection matters. While you may also contact us, VeraSafe can be contacted on matters related to the processing of Personal Data. VeraSafe can be contacted using this contact form, by telephone at: +44 (20) 4532 2003, or by postal mail at:

VeraSafe United Kingdom Ltd.
37 Albert Embankment
London SE1 7TL
United Kingdom

Data Protection Officer

We have appointed VeraSafe as our Data Protection Officer (DPO). While you may contact us directly, VeraSafe can also be contacted on matters related to the processing of Personal Data. VeraSafe's contact details are:

VeraSafe
100 M Street S.E., Suite 600
Washington, D.C. 20003
USA
Email: experts@verasafe.com
Web: https://www.verasafe.com/about-verasafe/contact-us/