

Updated: September 2, 2021

What this policy covers

Your privacy is important to us, and so is being transparent about how we collect, use, store, and share information about you. This policy is intended to help you understand:

- What information we collect about you and for what purpose
- How we share information we collect
- How we store and secure information we collect
- How to access and control your information
- Website Visitors, EEA, UK, and Switzerland: Legal basis for processing
- How we transfer information we collect internationally
- EEA, UK, and Switzerland Users Only
- California State Resident Rights
- Other important privacy information
- How to Contact Us

This privacy policy covers the information we collect about you when you interact with us in the course of business including through our website, www.imply.io, and other websites that link to this policy, use our products or services, or otherwise interact with us (for example, by attending our training or events, through partners, or by receiving email newsletters and related information), unless a different policy is displayed. Imply, we and us refers to Imply Data, Inc. We offer analytics products for on-prem use and use in public and private cloud environments. We refer to all of these products, together with our services and website as "Services" in this policy. This policy also explains your choices about how we use information about you. Your choices include how you can object to certain uses of information about you and how you can access and update certain information about you. **If you do not agree with this policy, do not access or use our Services or interact with any other aspect of our business.**

INFORMATION WE COLLECT AND FOR WHAT PURPOSE

We collect information about you when you input it into the Services or otherwise provide it directly to us. We collect information automatically when you use and access our Services, such as information about your use of the Services; technical information or data obtained from systems and networks accessing the Services, device and connection information; and information collected through cookies and other tracking technologies. When you use our monitoring products, we may also collect certain metadata and system level information, including without limitation, your IP Address, user id, and/or email to track and monitor Service usage. For example, we use IP addresses to monitor the regions from which users use our products. We also collect information from other sources, such as user of our Services, other services you may link to your account; our partners; and third parties such as advertisers and market research companies.

How we use the information we collect depends in part on which Services you use, how you use them, and any preferences you have communicated to us. The specific purposes for which we use the information we collect about you, include the following: to provide the Services and personalize your experience; for research and development; to communicate with you about the Services; to market promote and drive engagement with the Services; to provide customer support; for safety and security; to protect our legitimate business interests and legal rights; and with your consent.

From time to time, we may obtain information about you from third party sources, such as public databases and websites, resellers and distributors, joint marketing or business partners, security and fraud detection firms and social media platforms. Examples of the information we may receive from third party sources include: account information; page-view information; contact information from business partners with whom we operate co-branded events, services and marketing campaigns or joint offerings; and search results and links, including paid listings (such as sponsored links).

COOKIES AND OTHER TRACKING TECHNOLOGY USED TO COLLECT INFORMATION

We and our third party partners may automatically collect certain types of usage information when you visit or use our Services. For instance, when you visit our website, we may send one or more cookies — a small text file containing a string of alphanumeric characters — to your computer that uniquely identifies your browser and lets us help you log in faster and enhance your navigation through the site.

A cookie may also convey information to us about how you use the website (e.g., the pages you view, the links you click, how frequently you access the website, and other actions you take on the website), and allow us to track your usage of the website over time. We may collect log file information about your browser or mobile device each time you access the website.

Log file information may include anonymous information such as your web request, IP address, browser type, information about your mobile device, referring / exit pages and URLs, number of clicks and how you interact with links on the website, domain names, landing pages, pages viewed, and other such information.

We may employ clear gifs (also known as web beacons) which are used to anonymously track the online usage patterns of our users. In addition, we may also use clear gifs in HTML-based emails sent to our users to track which emails are opened and which links are clicked by recipients. The information allows for more accurate reporting and improvement of the website. We may also collect analytics data, or use third-party analytics tools, to help us measure traffic and usage trends for the website. These tools collect information sent by your browser or mobile device, including the pages you visit, your use of third party applications, and other information that assists us in analyzing and improving the Services.

When you access our Services by or through a mobile device, we may receive or collect and store a unique identification numbers associated with your device, as well as information about your mobile carrier, device type, model and manufacturer, mobile device operating system brand and model, phone number, and, depending on your mobile device settings, your geographical location data, including GPS coordinates (e.g. latitude and/or longitude) or similar information regarding the location of your mobile device.

We may use the data collected through cookies, log file, device identifiers, location data and clear gifs information to: (a) provide and monitor the effectiveness of our Services; (b) monitor aggregate metrics such as total number of visitors, traffic, usage, and demographic patterns on Services; (c) diagnose or fix technology problems; and (d) otherwise to plan for, research and enhance our Services.

HOW WE SHARE THE INFORMATION WE COLLECT

We share information we collect about you in the ways discussed below, including in connection with possible business transfers, but we are not in the business of selling information about you to advertisers or other third parties. Examples of how we share the information we collect include the following:

Managed account administration: If you register or access the Services using an email address with a domain that is owned by your employer or organization, and such organization wishes to establish an account or site, certain information about you including your name, contact info, content and past use of your account may become accessible to that organization's administrator and other Service users sharing the same domain. If you are an administrator for a particular site or group of users within the Services, we may share your contact information with current or past Service users, for the purpose of facilitating Service-related requests

THIRD PARTY SHARING

We share information with third parties that help us operate, provide, improve, integrate, customize, support and market our Services.

Service Providers: We work with third-party vendors and service providers to provide website and application development, hosting, maintenance, backup, storage, virtual infrastructure, payment processing, analysis and other services for us, which may require them to access or use information about you. If a service provider needs to access information about you to perform services on our behalf, they do so under close instruction from us, including policies and procedures designed to protect your information.

Impley Partners: We work with third parties who provide consulting, sales, and technical services to deliver and implement customer solutions around the Services. We may share your information with these third parties in connection with their services, such as to assist with billing and collections, to provide localized support, and to provide customizations. We may also share information with these third parties where you have agreed to that sharing.

Links to Third Party Sites: The Services may include links that direct you to other websites or services whose privacy practices may differ from ours. If you submit information to any of those third party sites,

your information is governed by their privacy policies, not this one. We encourage you to carefully read the privacy policy of any website you visit.

Social Media Widgets: The Services may include links that direct you to other websites or services whose privacy practices may differ from ours. Your use of and any information you submit to any of those third-party sites is governed by their privacy policies, not this one.

Third-Party Widgets Some of our Services contain widgets and social media features, such as the Twitter "tweet" button. These widgets and features collect your IP address, which page you are visiting on the Services, and may set a cookie to enable the feature to function properly. Widgets and social media features are either hosted by a third party or hosted directly on our Services. Your interactions with these features are governed by the privacy policy of the company providing it.

With your consent: We share information about you with third parties when you give us consent to do so. For example, we often display personal testimonials of satisfied customers on our public website. With your consent, we may post your name alongside the testimonial.

Compliance with Enforcement Requests and Applicable Laws; Enforcement of Our Rights: In exceptional circumstances, we may share information about you with a third party if we believe that sharing is reasonably necessary to (a) comply with any applicable law, regulation, legal process or governmental request, including to meet national security requirements, (b) enforce our agreements, policies and terms of service, (c) protect the security or integrity of our products and services, (d) protect Imply, our customers or the public from harm or illegal activities, or (e) respond to an emergency which we believe in good faith requires us to disclose information to assist in preventing the death or serious bodily injury of any person. Law enforcement requests can be directed to legal@imply.io.

Business Transfers: We may share or transfer information we collect under this privacy policy with our affiliates and in connection with any merger, sale of company assets, financing, acquisition, or dissolution transaction or a proceeding involving sale, transfer, divestiture, or disclosure of all or a portion of our business or assets. You will be notified via email and/or a prominent notice on the Services if a transaction takes place, as well as any choices you may have regarding your information.

HOW WE STORE INFORMATION WE COLLECT

Information storage and security: We use global data hosting service providers to host the information we collect, and we use reasonable and appropriate technical measures to secure your data. While we implement safeguards designed to protect your information, no security system is impenetrable and due to the inherent nature of the Internet, we cannot guarantee that data, during transmission through the Internet or while stored on our systems or otherwise in our care, is absolutely safe from the intrusion of others. If you use our on-prem products or our hybrid analytics Services, responsibility for securing storage and access to the information you put into the Services rests with you and not Imply. We strongly recommend that users of our on-prem products or hybrid analytics Services configure SSL to prevent interception of data transmitted over networks and to restrict access to the databases and other storage points used.

How long we keep information: How long we keep information we collect about you depends on the type of information, as described in further detail below. After such time, we will either delete or anonymize your information or, if this is not possible (for example, because the information has been stored in backup archives), then we will securely store your information and isolate it from any further use until deletion is possible.

Account information: We retain your account information for as long as your account is active and a reasonable period thereafter in case you decide to re-activate the Services. We also retain some of your information as necessary to comply with our legal obligations, to resolve disputes, to enforce our agreements, to support business operations, and to continue to develop and improve our Services. Where we retain information for Service improvement and development, we take steps to eliminate information that directly identifies you, and we only use the information to uncover collective insights about the use of our Services, not to specifically analyze personal characteristics about you.

Information you share on the Services: If your account is deactivated or disabled, some of your information and the content you have provided will remain in order to allow your team members or other users to make full use of the Services. For example, we continue to display messages you sent to the users that received them and continue to display content you provided.

Managed accounts: If the Services are made available to you through an organization (e.g., your employer), we retain your information as long as required by the administrator of your account.

Marketing information: If you have elected to receive marketing emails from us, we retain information about your marketing preferences for a reasonable period of time from the date you last expressed interest in our Services, such as when you last opened an email from us or ceased using your Imply

account. We retain information derived from cookies and other tracking technologies for a reasonable period of time from the date such information was created.

HOW TO ACCESS AND CONTROL YOUR INFORMATION

You have certain choices available to you when it comes to your information. Below is a summary of those choices, how to exercise them and any limitations.

Your Choices: You have the right to request a copy of your information, to object to our use of your information (including for marketing purposes), to request the deletion or restriction of your information, or to request your information in a structured, electronic format. Below, we describe the tools and processes for making these requests. You can exercise some of the choices by logging into the Services and using settings available within the Services or your account. Where the Services are administered for you by an administrator (see "Notice to End Users" below), you may need to contact your administrator to assist with your requests first. For all other requests, you may contact us as provided in the Contact Us section below to request assistance.

Your request and choices may be limited in certain cases: for example, if fulfilling your request would reveal information about another person, or if you ask to delete information which we or your administrator are permitted by law or have compelling legitimate interests to keep. Where you have asked us to share data with third parties, for example, by installing third-party apps, you will need to contact those third-party service providers directly to have your information deleted or otherwise restricted. If you have unresolved concerns, you may have the right to complain to a data protection authority in the country where you live, where you work or where you feel your rights were infringed.

Access and update your information: Our Services give you the ability to access and update certain information about you from within the Service. For example, you can access your profile information from your account. You can update your profile information within your profile settings and modify content that contains information about you using the editing tools associated with that content.

Deactivate your account: If you no longer wish to use our Services, you or your administrator can deactivate your Services account by contacting us.

Retention and Deletion: Imply will retain your personal information for as long it is needed to provide you with Service(s); as needed for the purposes outlined in this privacy policy or at the time of collection; as necessary to comply with our legal obligations (e.g., to honor opt-outs), resolve disputes, and enforce our agreements; or to the extent permitted by law. At the end of the retention period, Imply will delete your personal information in a manner designed to ensure that it cannot be reconstructed or read.

Request that we stop using your information: In some cases, you may ask us to stop accessing, storing, using and otherwise processing your information where you believe we don't have the appropriate rights to do so. For example, if you believe a Services account was created for you without your permission or you are no longer an active user, you can request that we delete your account as provided in this policy. Where you gave us consent to use your information for a limited purpose, you can contact us to withdraw that consent, but this will not affect any processing that has already taken place at the time. You can also opt-out of our use of your information for marketing purposes by contacting us, as provided below. When you make such requests, we may need time to investigate and facilitate your request. If there is delay or dispute as to whether we have the right to continue using your information, we will restrict any further use of your information until the request is honored or the dispute is resolved, provided your administrator does not object (where applicable). If you object to information about you being shared with a third-party app, please disable the app or contact your administrator to do so.

Opt out of communications: You may opt out of receiving promotional communications from us by using the unsubscribe link within each email, updating your email preferences within your Service account settings menu, or by contacting us as provided below to have your contact information removed from our promotional email list or registration database. Even after you opt out from receiving promotional messages from us, you will continue to receive transactional messages from us regarding our Services. You can opt out of some notification messages in your account settings.

You may be able to opt out of receiving personalized advertisements from other companies who are members of the Network Advertising Initiative or who subscribe to the Digital Advertising Alliance's Self-Regulatory Principles for Online Behavioral Advertising. For more information about this practice and to understand your options, please visit: <http://www.aboutads.info>, <http://optout.networkadvertising.org/> and <http://www.youronlinechoices.eu>. To “opt out” of the collection of any information through cookies or other tracking technology you will need to manage the settings on your browser or mobile device. Please refer to your browser’s or mobile

device's technical information for instructions on how to delete and disable cookies, and other tracking/recording tools. (To learn more about cookies, clear gifs/web beacons and related technologies, you may wish to visit <http://www.allaboutcookies.org> and/or <http://www.youronlinechoices.com>).

Data portability: Data portability is the ability to obtain some of your information in a format you can move from one service provider to another (for instance, when you transfer your mobile phone number to another carrier). Depending on the context, this applies to some of your information, but not to all of your information. Should you request it, we will provide you with an electronic file of your basic account information and the information you create on the spaces under your sole control.

WEBSITE VISITORS, EEA, UK, AND SWITZERLAND: LEGAL BASIS FOR PROCESSING

If you are a website visitor or Services user based in the European Economic Area ("EEA"), UK, or Switzerland, Imply Data, Inc. is the data controller of your personal data unless the data is collected in circumstances where one of our affiliates is running a local event, for example, and they collect and control that information. In such circumstances, we will endeavor to make this clear to you in a context specific notification at the point we collect your personal data. Our legal basis for collecting and using the personal data will depend on the personal data concerned and the specific context in which we collect it. However, we will normally collect personal data only where we have your consent to do so, where we need the personal data to perform a contract with you, or where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms. In some cases, we may also have a legal obligation to collect personal data from you. If we ask you to provide personal data to comply with a legal requirement or to perform a contract with you, we will make this clear at the relevant time. For more information on our legal basis for processing personal data, please contact us using the contact details provided below.

HOW WE TRANSFER INFORMATION WE COLLECT INTERNATIONALLY

Your personal information may be transferred to, and processed in, countries other than the country in which you are resident. These countries may have data protection laws that are different to the laws of

your country, and in some cases, may not be as protective. Specifically, our website servers are located in the U.S. and we may process your information in jurisdictions where our affiliates/partners and third-party service providers are located.

Whenever we transfer your information, we take safeguards to protect it. These safeguards include implementing the European Commission's Standard Contractual Clauses for transfers of personal data between us and our affiliates to whom we transfer the information which require these companies to protect personal information they process from the EEA, UK, or Switzerland in accordance with European Union data protection law. Our Standard Contractual Clauses can be provided on request. We implement similar appropriate safeguards with our third-party service providers and further details can be provided upon request.

Privacy Shield Update

Imply Data, Inc. previously participated in the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and complied with the Privacy Shield Principles regarding the collection, use, and retention of personal data transferred from the European Union and the UK, or Switzerland (as applicable) to the U.S. As a result of the July 16, 2020 Court of Justice of the E.U. judgment and subsequent September 8, 2020 FDPIC opinion, the Privacy Shield Framework is no longer a valid means to comply with E.U. data protection requirements when transferring personal data from the E.U., U.K. or Switzerland to the U.S., and Imply has withdrawn its certification from the program.

EEA, UK, and Switzerland Residents Only

If you are a resident of the EEA, UK, or Switzerland you have the following data protection rights.

- The right to access, correct, update, or request deletion of your personal information;
- The right to object to the processing of your personal information by asking us to restrict processing of your personal information or request portability of your personal information; and

- The right to withdraw your content at any time if we collected and processed your personal information with your consent

Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent. You may contact us as privacy@imply.io to exercise these rights.

To submit a complaint to a data protection authority about our collection and use of your personal information. Contact details for data protection authorities are listed below:

- [EEA](#);
- [United Kingdom](#); and
- [Switzerland](#).

EEA, UK, and Switzerland Users Only: Your Privacy Rights in Respect of Customer Data

If personal data pertaining to you as an individual has been submitted to the Service by or on behalf of an Imply customer and you wish to exercise any data protection rights you may have in respect of that data under applicable law, including (as applicable) the right to access, port, correct, amend or delete such data, please inquire with the relevant Imply customer directly. Imply has a limited ability to access its customer's data. However, if you wish to make your request directly to Imply, please provide the name of the customer who submitted your data to our Service. We will refer your request to that customer and will support them as needed in responding to your request within a reasonable timeframe.

CALIFORNIA STATE RESIDENT RIGHTS

If you are a California resident, as defined in the California Code of Regulations, you have rights under the California Consumer Privacy Act of 2018 ("the CCPA"), effective as of January 1, 2020. A description of your rights about your personal information is provided below.

Right to know about the personal information we collect, share, and restrict its sale

The CCPA gives you the right to request that we disclose the specific pieces of personal information we have collected about you, share, and restrict the sale of your personal information. Imply does not sell your personal information as defined by the CCPA and its implementing regulations. However, we may disclose certain personal information for a business purpose.

Disclosures Of Your Personal Information

Categories of information we collect and disclose for a business purpose

We collect the following categories of personal information from you in connection with the Services, as defined in the CCPA. In addition, during the past twelve months, we have disclosed these categories of personal information for a business purpose:

Categories of Personal Information We Collect	Categories of Third Parties with Whom we Share Information
Identifiers (e.g., name, address, email address, etc.)	Affiliates, vendors, services providers, and third party business partners
Any categories of personal information described in subdivision (e) of Section 1798.80 (e.g., address, telephone number, financial information, etc.)	Vendors, service providers, and third party business partners
Legally Protected Classifications (e.g., gender, marital status, etc.)	Vendors and service providers
Commercial Information (e.g., transaction data, etc.)	Vendors, service providers, and third party business partners
Internet or Other Network or Device Activity (e.g., browsing history, app usage, etc.)	Vendors and service providers
Approximate Location Information (e.g., location inferred from your IP address, city, country, etc.)	Vendors and service providers

Professional or Employment-Related Data (e.g., the name of your employer)	Vendors, service providers, and third party business partners
Educational Information (e.g., degrees and certifications)	Vendors and service providers
Inferences drawn from any of the information identified above	N/A

According to California law, personal information does not include:

- Publicly available information from government records.
- De-identified or aggregated consumer information.

Other disclosures about your personal information

Our privacy policy covers additional disclosures about your personal information that the CCPA requires we provide to you. Our privacy policy includes more information about the sources from which we collect your personal information, the business or commercial purposes for which we collect your personal information, and the categories of third parties with whom we share your personal information. For a description of all of our data collection, use and disclosure practices, please read this privacy policy in its entirety.

Right of deletion

You have the right to request that we delete your personal information, subject to certain exceptions. After we receive and validate your request, we will delete your personal information, as well as direct our service providers to delete your personal information, unless an exception applies.

How to make a request

You have the right to make a free request two times in any 12-month period, but do note you will be asked to verify your identity which may include providing us with additional personal information. Upon verifying your identity, we will make the disclosure within 45 days of receiving your request, unless we request an extension. In the event that we reasonably need a 45-day extension, we will notify you of the extension within the initial 45-day period. You may request these disclosures by emailing us at privacy@imply.io. In some cases, your requests may not be fulfilled if they are not consistent with our obligation to comply with applicable legal or operational requirements, for example, if your personal information is necessary for the performance of a contract between you and Imply. Imply will not discriminate nor retaliate against a party who makes a request under the CCPA.

How to contact us

If you have questions about your rights or our disclosures under the CCPA, you may reach us at privacy@imply.io.

Changes to This Information

We reserve the right to modify this information at any time. Please review it occasionally. If we make changes to this information, the updated page will be posted on the privacy policy webpage in a timely manner.

OTHER IMPORTANT PRIVACY INFORMATION

Notice to End Users

Our products are intended for use by organizations. Where the Services are made available to you through an organization (e.g. your employer), that organization is the administrator of the Services and is responsible for the accounts and/or Service sites over which it has control. If this is the case, please direct your data privacy questions to your administrator, as your use of the Services is subject to that organization's policies. We are not responsible for the privacy or security practices of an administrator's organization, which may be different than this policy.

Administrators are able to:

- require you to reset your account password;
- restrict, suspend or terminate your access to the Services;
- access information in and about your account;
- access or retain information stored as part of your account;
- install or uninstall third-party apps or other integrations

In some cases, administrators can also:

- restrict, suspend or terminate your account access;
- change the email address associated with your account;
- change your information, including profile information;

- restrict your ability to edit, restrict, modify or delete information

Even if the Services are not currently administered to you by an organization, if you use an email address provided by an organization (such as your work email address) to access the Services, then the owner of the domain associated with your email address (e.g. your employer) may assert administrative control over your account and use of the Services at a later date. You will be notified if this happens.

If an administrator has not already asserted control over your account or access to the Services, you can update the email address associated with your account through your account settings in your profile. Once an administrator asserts control over your account or use of the Services, you will no longer be able to change the email address associated with your account without administrator approval.

Please contact your organization or refer to your administrator's organizational policies for more information.

OUR POLICY TOWARDS CHILDREN

The Services are not directed to individuals under 16. We do not knowingly collect personal information from children under 16. If we become aware that a child under 16 has provided us with personal information, we will take steps to delete such information. If you become aware that a child has provided us with personal information, please contact us at privacy@imply.io.

CHANGES TO OUR PRIVACY POLICY

We may change this privacy policy from time to time. We will post any privacy policy changes on this page and, if the changes are significant, we will provide a more prominent notice by adding a notice on the Services homepages, login screens, or by sending you an email notification. We will also keep prior versions of this privacy policy in an archive for your review. We encourage you to review our privacy policy whenever you use the Services to stay informed about our information practices and the ways you can help protect your privacy.

If you disagree with any changes to this privacy policy, you will need to stop using the Services and deactivate your account(s), as outlined above.

CONTACT US

For information controlled by Imply, if you have questions or concerns about how your information is handled, please direct your inquiry to:

Imply Data, Inc.

Attn. Privacy

1633 Old Bayshore Highway, Suite 232

Burlingame, CA 94010

privacy@imply.io