

Wrike Privacy Policy

This is the Privacy Policy for Wrike and its Affiliates. For a PDF of this Privacy Policy, click [here](#).

1. Definitions

- **“Affiliates”** means the legal entities owned directly or indirectly by Wrike, Inc. or that are otherwise in Wrike, Inc.’s corporate family.
- **“CCPA”** means the California Consumer Protection Act. If you are a California resident, you should read this Privacy Policy together with its [Additional Privacy Details for California Residents](#) section, which provides additional information about our California information practices, including a description of CCPA rights available to some Californians.
- **“Controller”** means the entity that has certain legal rights to determine the purposes for which Personal Data will be Processed and the means by which that Processing will happen.
- **“Customer”** means the entity that has contracted with Wrike to receive a free, trial, or paid Platform Plan or other Service Offerings. For example: When a business purchases a Platform Plan and sets up accounts under that Platform Plan for employees, the business is the Customer, and each individual using the Platform under the Plan is a User. If a one-person business signs up for its own free Platform Plan, that person is both the Customer and the User. If that person invites others to set up accounts under that Plan, those other people will be Users as well.
- **“GDPR”** means the EU General Data Protection Regulation.
- **“Personal Data”** means any information about an identified or identifiable individual, such as their name or contact information.
- **“Platform”** means the work management and collaboration platform on wrike.com and the Wrike [desktop and mobile apps](#).
- **“Platform Plan”** means a Customer’s subscription to the Platform.
- **“Process,” “Processed,” and “Processing”** refer to any operation or set of operations that can be performed on Personal Data or on sets of Personal Data. This includes, for example, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure and destruction.

- **“Processor”** means an entity that Processes Personal Data on behalf of a Controller.
- **“Service Data”** is Personal Data or other information that Users: input directly into the Platform; create within the Platform; send to the Platform through our [Chrome browser extension](#) or through other [apps and integrations](#); or provide to Wrike through authorized methods as part of other Service Offerings.
- **“Service Offerings”** means the Platform and Wrike’s related support and professional services.
- **“User”** means an individual who uses a Service Offering. Within the Platform, there are three types of Users: [Regular Users](#), [External Users](#), and [Collaborators](#). Those User types are defined at that hyperlink.
- **“Workspace”** means the Platform instance to which a Customer gains access when entering into a Platform Plan. The Workspace may contain one or more projects administered by the Customer.
- **“Wrike”** means Wrike, Inc., whose contact information is at the end of this Privacy Policy.

2. Scope of this Privacy Policy, and a Note Regarding Service Data

Where indicated, this Privacy Policy applies to Service Data. We do not control the content of Service Data, and, because of security features in the Platform, in most cases we are unable to read such content. Under the GDPR and similar laws, Wrike is considered the Customer’s Processor of any Personal Data in the Service Data.

Wrike Processes Personal Data in the Service Data pursuant to the instructions of the relevant Customer or as required by applicable law, as described in the Wrike Terms of Service at <https://www.wrike.com/security/terms> or the alternative agreement (if applicable) signed by Wrike and that Customer for the Service Offerings. For any Workspace on the Platform, the relevant Customer is the one that Wrike authorizes to control the administrator account. Specifically, that Customer is the Controller for all information submitted by any User to that Workspace, including [Regular Users](#), [External Users](#), and [Collaborators](#). The foregoing is true even when those Users happen to be employees of another Customer, as each Customer is a Controller of only its own Workspaces. Regular Users of a Workspace

can find contact information for the relevant Customer's administrator(s) by logging in to the Workspace and selecting "Profile", then "Profile Settings", and then "Account Information". Other individuals may contact Wrike to ask Wrike to forward a request or inquiry to a particular Workspace's administrator or designated contact point.

Wrike may disclose any Service Data, including certain deleted Service Data, or data previously received from deactivated Users, to the relevant Customer, and Wrike provides the Customer with certain tools for modifying, deleting or taking other steps with Service Data. Accordingly, Users and other individuals should contact the relevant Customer with any requests relating to Personal Data about them that may appear in that Customer's Service Data. If Wrike receives a request from a User to exercise rights in Service Data, we will refer the User's request to the relevant Customer and cooperate with that Customer's handling of the request, subject to any special contractual arrangement with that Customer. For requests from Customer account administrators relating to their own Personal Data, Wrike may handle the request directly.

The Privacy Policy also applies to our handling of Personal Data that is not Service Data, such as Personal Data about:

- Visitors to our websites and events;
- Prospective Customers and their personnel;
- Reseller and referral partners;
- People who sign up for our newsletters or other marketing; and
- Current Customers and Users, in relation to their procurement of Service Offerings and management of the relationship with Wrike.

However, this Privacy Policy does not cover any data we Process in the context of our own recruiting and human resources management activities.

3. Types of Personal Data We Collect

Because we designed the Platform to be content- and data-agnostic, our Customers are empowered to provide us with any kind of Personal Data in the Service Data.

In addition to Service Data, we collect contact details, professional details such as title and name of company, information about the browsers and devices that individuals use to interact with us, information about an individual's interactions with Wrike or our partners, payment information, and inferences drawn other Personal Data.

We obtain much of this data directly from the relevant individuals, including in some cases with the technology described in the "Cookies and Automated Data Collection" section further below. We also obtain Personal Data directly from our current or prospective Customers and from other third-party sources such as resellers, referral partners, distributors, list vendors and marketing companies, as well as from publicly available sources such as prospective Customers' websites and third-party sites like LinkedIn.

4. How We Use Personal Data

Wrike uses Personal Data as follows:

- To provide and improve our Service Offerings, including internal analysis of aggregate usage patterns;
- To respond to questions, concerns, or customer service inquiries, and to otherwise fulfill individuals' requests;
- To send information about our current and future Service Offerings, including marketing communications by phone, email, online display advertising, and other channels;
- To offer and provide our Service Offerings to you through our approved resellers;
- To analyze market conditions and use of our Service Offerings;
- To customize the content and advertising individuals see on our websites, across the Internet, and elsewhere;
- To enforce the legal terms that govern our business and online properties;
- To comply with law and legal process and protect rights, safety and property; and

- For other purposes requested or permitted by our Customers, Users or other relevant individuals, such as website visitors.

We may combine data collected from you with other sources to help us improve the accuracy of our marketing and communications as well as to help expand or tailor our interactions with you. This includes combining Personal Data we obtain through online channels with information we obtain through offline channels, as well as other information (such as referral programs), for the purposes described above. We may anonymize or aggregate personal information and use it for the purposes described above and for other purposes to the extent permitted by applicable law. We also may use Personal Data for additional purposes that we specify at the time of collection. We will obtain your consent for these additional uses to the extent required by applicable law.

5. Disclosures of Personal Data

We share Personal Data as follows:

- For the uses of information described above, including to make appropriate disclosures in response to lawful requests by public authorities, such as to meet national security or law enforcement requirements; and
- In connection with an actual or potential business sale, merger, consolidation, change in control, transfer of substantial assets or reorganization.

For those purposes, we may share information with:

- Our Affiliates;
- Other entities that help us with any of the above, such as our [sub-processors](#), our CRM system provider, data storage and backup providers, marketing service providers, customer relationship management providers, accounting providers, technical service providers, our payment processor, and the marketing and analytics companies described in Section 7 below;
- Other entities involved in the legal-related matters described above; or
- Other entities involved in the significant corporate transactions described above, such as an acquirer of Wrike.

6. Legal Bases for Processing Personal Data

The laws in some jurisdictions require companies to tell you about the legal grounds they rely on to use or disclose your Personal Data. To the extent those laws apply, our legal grounds for Processing Personal Data are as follows:

- *To honor our contractual commitments to an individual:* Some of our Processing of Personal Data is to meet our contractual obligations to the individuals to whom the Personal Data relate, or to take steps at their request in anticipation of entering into a contract with them. For example, when an individual purchases admission to a Wrike event, we may Process their payment information on this basis.
- *Consent:* Where required by law, and in some other cases, we handle Personal Data on the basis of consent. For example, some of our direct marketing activities happen on the basis of opt-in consent, such as sending marketing emails to individuals who have requested them.
- *Legitimate interests:* In many cases, we handle Personal Data on the ground that it furthers our legitimate interests in commercial activities, such as the following, in ways that are not overridden by the interests or fundamental rights and freedoms of the affected individuals: Customer support; Marketing, including, in some cases, direct marketing such as via email; Protecting our Customers, Users, personnel and property; Analyzing and improving our business and Service Offerings; and Managing legal issues. We may also Process Personal Data for the same legitimate interests of our Customers and business partners.
- *Legal compliance:* We need to use and disclose Personal Data in certain ways to comply with our legal obligations.

7. Cookies and Automated Data Collection

In our websites, apps and emails, we and third parties may collect certain information by automated means such as cookies, Web beacons, JavaScript, chatbots, mobile device functionality, browser-based or plugin-based local storage such as HTML5 storage or Flash-based storage, and other similar techniques and technologies.

This information includes unique browser identifiers, unique device identifiers such as the Apple Advertising Identifier or Android Advertising ID, IP address, browser and operating system information, geolocation, other device information, Internet connection information, as well as details about individuals' interactions with our apps, websites and emails, including interactions with and information provided to our chatbots. Such details include, for example, the URL of the third-party website from which you came, the pages that you visit on our websites, and the links you click on in our websites.

As part of this, we and third parties may use automated means to read or write information on your device, such as in various types of cookies and other local storage. Cookies and local storage are files that can contain data, such as unique identifiers or other information,

that we or a third party may transfer to or read from an individual's device for the purposes described in this Privacy Policy.

The cookies and other technologies described here fall into four basic categories:

- *Essential:* These are strictly necessary to provide you with our online presence, such as access to secure areas that require registration. Users cannot refuse them without impacting functionality.
- *Functional:* These allow Users to browse or benefit from some of its features, such as setting language preferences. Similar to the essential technology described above, if these are disabled, it could impact your experience to use some functionality.
- *Analytics:* These allow us or our third-party analytics providers to collect statistics on the use of our Service Offerings and website.
- *Advertising:* These cookies and other technologies, administered primarily by our third-party advertising partners, track individuals' online activities over time and use this information to show them ads that are tailored to their individual interests or characteristics and/or based on prior visits to certain sites or apps, or other information we or they know, infer or have collected from them. For example, we and these providers may use different types of cookies, other automated technology, and data to (i) recognize individuals and their devices; (ii) inform, optimize and serve ads; and (iii) to report on our ad impressions, other uses of ad services, and interactions with these ad impressions and ad services, including how they are related to visits to specific sites or apps.

To learn more about interest-based advertising, including how to opt out from the targeting of interest-based ads by some of our current ad service partners, visit aboutads.info/choices, youradchoices.ca or youronlinechoices.eu from each of your browsers on each of your devices. You can opt out of Google Analytics and customize the Google Display Network ads by visiting the [Google Ads Settings page](#) and installing the [Google Analytics Opt-out Browser Add-on](#) from each browser on each device. If you replace, change or upgrade your browser, or delete your cookies, you may need to use these opt-out tools again. Please visit your mobile device manufacturer's website, or the website for its operating system, for instructions on any additional privacy controls in your mobile operating system, such as privacy settings for device identifiers and geolocation.

You may be able to set your web browser to refuse certain types of cookies, or to alert you when certain types of cookies are being sent. Some browsers offer similar settings for HTML5 local storage, and Flash storage can be managed as described [here](#).

8. Personal Data Rights and Choices (Including Direct Marketing Opt-Out)

All Users can:

- Review and update certain User information by logging in to the relevant portions of the Platform.
- Deactivate their accounts by contacting us at <https://help.wrike.com/hc/requests/new>, subject to any contractual provisions between Wrike and the Customer responsible for the account. Except when the Customer has requested closure of all its User accounts, information in a deactivated User account may be available to the Customer for some time.
- Deactivate data collection by our browser extension by uninstalling it.

Controls related to cookies and other automated data collection are described in the “Cookies and Automated Data Collection” section above. Anybody can unsubscribe from marketing emails by clicking the unsubscribe link they contain.

Residents of the European Economic Area, the UK, and many other jurisdictions have certain legal rights to do the following with Personal Data we control:

- Obtain confirmation of whether we hold Personal Data about them, and to receive information about its Processing;
- Obtain a copy of the Personal Data, and in some cases, receive it in a structured, commonly used and machine-readable format, or have it transmitted to a third party in such form;
- Update, correct or delete the information;
- Object to our Processing of the information for direct marketing purposes;
- Object to other Processing of the information; and/or
- Withdraw consent previously provided for the Processing of the information.

Residents of the European Economic Area, the UK, and Switzerland also have certain rights under the Data Privacy Framework, as described in the “International Data Transfers” section below.

To exercise any of those rights with respect to the Personal Data Wrike controls, individuals should contact us as described at the end of this Privacy Policy.

To exercise any rights relating to Service Data, Users should contact the relevant administrator for the Workspace associated with the Service Data, not Wrike. Regular Users of a Workspace can find contact information for the relevant Customer’s administrator(s) by logging in to the Workspace and selecting “Profile”, then “Profile Settings”, and then “Account Information”. Other individuals may contact Wrike to ask Wrike to forward a request or inquiry to a particular Workspace’s administrator or contact point. If you are a Customer account administrator or Customer account owner and require assistance with this process, such as if you want to make a request with respect to your own User data, you may contact us as described below.

Many of the rights described above are subject to significant limitations and exceptions under applicable law. For example, objections to the Processing of Personal Data and withdrawals of consent typically will not have retroactive effect.

Every individual also has a right to lodge a complaint with the relevant supervisory authority.

9. Security

To provide security for Service Data within the Platform, we maintain physical, organizational, and technical safeguards, which are subject to periodic changes. The specific Platform security options available to Customers depend on their [Platform Plan](#). Customers’ use of available safeguards will impact the level of protection available for the Service Data. Communications with Wrike through other methods such as email or phone are not subject to those protections. Third-party software and services integrated

into our Service Offerings, such as Google Drive, Box, Dropbox, and [other integrations](#) are handled by such third parties subject to their own privacy and security procedures, which we do not control.

Wrike's use and transfer to any other app of information received from Google APIs will adhere to [the Google API Services User Data Policy](#), including the Limited Use requirements stated therein.

We use different safeguards to help secure the other Personal Data we handle.

No security method is perfect, and we cannot guarantee that any data will remain secure.

10. Data Retention

We hold Personal Data for as long as necessary to fulfill the purposes set forth in this Privacy Policy. Information may persist in copies made for backup and business continuity purposes for additional time.

11. International Data Transfers

We are headquartered in the United States, and recipients of the data disclosures described in this Privacy Policy are located in the United States and elsewhere in the world, including where privacy laws may not provide as much protection as those of your country of residence. However, eligible Customers can arrange to have their Workspaces stored in [our data center located in the European Union](#).

Customers also may transfer Service Data to Wrike on the basis of legal mechanisms approved by the European Commission and other relevant authorities for cross-border data transfers. These include Standard Contractual Clauses, which may be used in conjunction with additional safeguards that Wrike offers, such as [Wrike Lock](#) (which allows Customers to access to their Wrike data while managing their own encryption keys) and other encryption and security features provided under our multiple information security certifications: ISO/IEC 27001:2013, SOC2 Type II, ISO/IEC 27018:2019, and Cloud

Security Alliance STAR Level 2.

Wrike has certified that it adheres to 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 program (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Wrike, Inc. has certified to the U.S. Department of Commerce that it adhered 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. Wrike has certified to the U.S. Department of Commerce that it adheres to Swiss-U.S. Data Privacy Framework program Principles (Swiss-U.S. Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is a conflict between the terms in this privacy policy 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/>.

The following statements apply to all EEA, UK, and Swiss Personal Data that is received by Wrike in the United States pursuant to the DPF:

- Wrike is subject to the jurisdiction and enforcement authority of the United States Federal Trade Commission.
- EEA, Swiss, and UK individuals have the right to access their Personal Data that has been transferred into the United States and to correct or update that information. Individuals also have the right to erase information that has been processed in violation of the DPF Principles. To exercise any of these rights, which are subject to exceptions under the DPF Principles, individuals should refer to the contact information at the end of this policy.

When Wrike receives Personal Data under the DPF and then transfers it to a third-party service provider acting as an agent on Wrike's behalf, Wrike has certain responsibility under the DPF if both (i) the agent Processes the information in a manner inconsistent with the DPF, and (ii) Wrike is responsible for the event giving rise to the damage.

Covered European residents should direct any questions, concerns, or complaints

regarding Wrike's compliance with the DPF to Wrike as described at the bottom of this Privacy Policy. Wrike will attempt to answer your questions and satisfy your concerns in a timely and complete manner as soon as possible. If, after discussing the matter with Wrike, your issue or complaint is not resolved, Wrike has agreed to participate in the DPF independent dispute resolution mechanisms listed below, free of charge to you. Please contact Wrike first.

- For human resources Personal Data that Wrike receives under the DPF (defined under DPF essentially as information about an employee collected in the context of the employment relationship): cooperation with the EEA data protection authorities (DPAs), the UK Information Commissioner's Office (ICO), and the Swiss Federal Data Protection and Information Commissioner (FDPIC).
- For other Personal Data Wrike receives under the DPF: Wrike has further committed to refer unresolved privacy complaints under the DPF Principles to an independent dispute resolution mechanism, Data Privacy Framework Services, operated by BBB National Programs. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit <https://bbbprograms.org/programs/all-programs/dpf-consumers/ProcessForConsumers> for more information and to file a complaint. This service is provided free of charge to you. Please do not submit human resources complaints to Data Privacy Framework Services.

If your DPF complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See <https://www.dataprivacyframework.gov/s/article/G-Arbitration-Procedures-dpf?tabset-35584=2>.

Wrike makes its own international transfers of personal data. To exercise any legal right to see copies of the data transfer mechanism documents that Wrike uses to transfer data to third parties, please contact us. Our Service Offerings allow our Customers and Users to make international data transfers to third parties, such as to other Users, or to providers of integrations, for which they are solely responsible.

12. Notification of Changes

Wrike may change this Privacy Policy to reflect changes in the law, our data handling practices, or the features of our business. The updated Privacy Policy will be posted

on Wrike.com.

13. Contact Information

If you have questions, requests, or complaints relating to a Customer's handling of your Service Data, please contact the relevant Customer. If you have questions regarding our practices or this Privacy Policy, or to send us requests or complaints relating to Personal Data, please contact us at:

Wrike, Inc.

Attention: Legal and Compliance

9171 Towne Centre Drive, Suite 200

San Diego, CA 92122

privacy@team.wrike.com

14. Additional Privacy Details for California Residents

The subsections below apply only to “personal information” about California residents (as that term is defined in the CCPA) and they supplement the information in the rest of our [Privacy Policy](#) above. **Data about individuals who are not residents of California is handled differently and is not subject to the same rights described below.** These subsections also do not apply to Service Data ([defined above](#)), which is handled as described in [Section 2](#) of our Privacy Policy, even when the Service Data is about a resident of California.

The specific pieces of personal information we collected in the last 12 months generally fall into the following categories under California law, to the extent that any of the following are personally identifiable: identifiers (such as name, address, email address and other contact information); commercial information (such as transaction data, and information about an

individual's interactions with Wrike or our partners); financial data (such as payment card information); audio and visual information (such as recordings of certain calls, meetings, and events); internet or other network or device activity, and other information described in the [Cookies and Automated Data Collection](#) section of our Privacy Policy; geolocation information; professional or employment related data (such as title); other information that identifies or can be reasonably associated with you, and inferences drawn from any of the above.

In the twelve months leading up to the effective date of this Privacy Policy, Wrike used the personal information as follows:

- To provide and improve our Service Offerings, including internal analysis of aggregate usage patterns;
- To respond to questions, concerns, or customer service inquiries, and to otherwise fulfill individuals' requests;
- To send information about our current and future Service Offerings, including marketing communications by phone, email, online display advertising, and other channels;
- To analyze market conditions and use of our Service Offerings;
- To customize the content and advertising individuals see on our websites, across the Internet, and elsewhere;
- To enforce the legal terms that govern our business and online properties;
- To comply with law and legal process and protect rights, safety and property; and
- For other purposes requested or permitted by our Customers, Users or other relevant individuals, such as website visitors.

CCPA "sale" of California personal information

The CCPA requires businesses that "sell" personal information, as the term "sell" is defined under the CCPA, to provide an opt-out from such sales. Some people have taken the position that when a website or app uses third-party cookies and similar technology for its own analytics or advertising purposes, the website/app is engaged in a "sale" under the CCPA if the third parties have some ability to use, disclose or retain the data to improve

their service or to take steps beyond the most narrowly drawn bounds of merely providing their service to the website/app. Some take this position even when the website/app pays the third party (not vice versa), and in most cases merely provides the third party with an opportunity to collect data directly, instead of providing personal information to the third party. If you take the position that any of the relationships described above involve a “sale” within the meaning of the CCPA, then you may consider Wrike to have “sold” what the CCPA calls “identifiers” (like IP addresses), “internet or other electronic network activity information” (like information regarding an individual’s browsing interactions on wrike.com), and “commercial information” (like the fact that a browser visited a page directed to people who are considering purchasing from us) to marketing and analytics companies. As we await clarity on this point and, if applicable, the arrival of a proven method for handling CCPA-like choice options for it, we continue to offer opportunities to limit and/or opt out of the collection and/or use of data via certain third-party cookies and similar technology for analytics and advertising purposes, as described in the [Cookies and Automated Data Collection](#) section of our Privacy Policy. In any case, no matter how “sale” is defined, Wrike has no actual knowledge of selling the personal information of individuals under 16 years of age.

Collection and Disclosure of California Personal Information During Past 12 Months

The chart below provides more detail on our disclosures of California personal information during the 12 months leading up to the effective date of this Privacy Policy:

Category of personal information collected	Categories of third parties to which it was disclosed for a business purpose
Identifiers, such as name, username, email address, phone number, address, IP address	Affiliates, data storage and backup providers, marketing service providers, customer relationship management providers, accounting providers, technical service providers, payment processors, and marketing and analytics companies; and entities involved in legal-related matters with Wrike.
Professional or employment-related information, such as title	Same as first row
Commercial information, such as information provided to us in your communications (some	Same as first row

of which is personal information), transaction data, and information about interactions with Wrike or our partners	
Financial information such as payment card number	Payment processors
Audio and visual information	Same as first row
Internet or other electronic network activity information, such as technical data about a device and information about a device's interactions with our website	Same as first row, with the exception of payment processors
Audio and visual information	Same as first row
Internet or other electronic network activity information, such as technical data about a device and information about a device's interactions with our website	Same as first row, with the exception of payment processors

California Privacy Rights

If you are a California resident, California law may permit you to request that we:

- Inform you of the categories of personal information we have collected about you in the last twelve months; the categories of sources of such information; the categories of personal information that we sold or disclosed about you for a business purpose; the business or commercial purpose for collecting or selling your personal information; and the categories of third parties to whom we have “sold” or otherwise disclosed personal information for a business purpose.
- Provide access to and/or a copy of certain information we hold about you.
- Delete certain information we have about you.
- Rectify any inaccurate information about you. By visiting your account settings, you can correct and change certain personal information associated with your account.

Certain information is exempt from such requests under applicable law. You also may have the right to receive information about the financial incentives that we offer to you (if any).

You also have certain rights under the CCPA not to be subject to certain negative consequences for exercising CCPA rights.

We will take steps to verify your identity before responding to your request, which may include requesting that you respond to an email that we send to you, or otherwise verifying your name, email address or other information that will help us to confirm your identity.

If you are an agent making a request on behalf of a consumer, you must verify that you are authorized to make that request, which may include requiring you to provide us with written proof that satisfies CCPA requirements, such as an appropriate letter signed by the consumer or a power of attorney. We also may require the consumer to verify their identity directly with us.

To request to exercise any of these rights, please visit <https://www.wrike.com/contactus/> and click “Privacy” on the drop-down.

LAST UPDATED FEBRUARY 9, 2024 .