Wrike Privacy Policy

Last updated June 1st, 2026.

Table of Contents

1. Scope of Privacy Policy and note regarding Customer Data

This Privacy Policy applies primarily to our handling of personal data that is not Customer 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.

Except where indicated, this Privacy Policy does not apply to Customer Data or personal data Wrike processes in connection with its performance of the Service Offerings. We do not control the content of Customer Data, and, because of security features in the Platform, in most cases we are unable to read such content. Under the EU General Data Protection Regulation ("**GDPR**") and similar laws, Wrike is considered the Customer's processor of any personal data in the Customer Data.

Wrike processes personal data in connection with its performance of the Service Offerings 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/terms/ or the alternative terms of service or agreement (if applicable) between Wrike and that Customer for the Service Offerings, together with its related Data Processing Addendum ("**DPA**"). For any Workspace on the Platform, the relevant Customer is the one that Wrike authorizes to control the Customer account. Specifically, that Customer is the controller for all information submitted by any User to that Workspace, including Full Users and Limited Users. This is true even when those Users happen to be employees of another company or 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 Customer Data, to the relevant Customer, and Wrike provides the Customer with certain tools for modifying, deleting or taking other steps with Customer Data. Accordingly, Users and other individuals should contact the relevant Customer with any request relating to personal data about them that may appear in that Customer's Customer Data. If Wrike receives a request from a User to exercise rights in Customer 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.

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 Customer Data.

This Privacy Policy does not cover any data we process in the context of our own recruiting and human resources management activities, which are governed by separate privacy policies.

2. Types of personal data we collect

In addition to personal data subject to the Wrike DPA that Customers provide to Wrike as Customer Data or otherwise in connection with the Service Offerings, we also collect personal data, including 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 from 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 and third-party sites like LinkedIn. When we obtain data from these third-party sources, we take steps to ensure the data was collected lawfully and that we have the right to process it for our commercial purposes.

We may also collect and process personal data contained in business communications with Wrike, including email content and other correspondence, where relevant to our relationship with current or prospective customers, partners, and other business contacts. Sales representatives' emails and related correspondence, including complete email chains and third-party responses to Wrike communications, may be processed using AI-enabled tools for the purposes described in this Privacy Policy. Individuals who correspond with Wrike's sales team will be provided notice of this processing at the point of contact. These tools are used to enhance our responsiveness to prospective customers and to ensure the accuracy of our sales records. When we collect personal data via AI-enabled tools or automated systems, we ensure such collection is limited to what is necessary for the specified purpose. In addition, when individuals participate in a videoconference using a Wrike conference tool or another conference tool made available by Wrike, we may collect and process audio recordings, video recordings, transcripts, and related meeting metadata (such as date, time, participants, and meeting title), but only where the relevant participant has provided active consent to the recording in accordance with Section 5 of the Privacy Policy. Where AI-enabled tools are used in connection with recorded videoconference or related business communication, we may also generate and process derived data such as transcripts, summaries, notes, action items, key topics, follow-up recommendations, and similar outputs.

3. How We Use personal data

Wrike uses personal data as follows:

- To provide and improve our Service Offerings, including internal analysis of usage patterns;
- To verify the identity of prospective customers and prevent fraudulent account creation;
- 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 record, store, transcribe, summarize, review and use videoconferences conducted through conference tools made available by Wrike, where the relevant participant has actively consented to the recording, and to use AI-enabled tools and related service providers in connection with those videoconferences and emails to assist with transcription, summarization, note-taking, action item generation, internal training, quality assurance, knowledge management, service improvement, documentation, and business operations;
- To monitor, investigate, and protect against fraud, misuse, security incidents, or other unlawful or unauthorized activity;
- 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 any personal information and use and disclose 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.

AI-generated outputs may contain errors or omissions and may be reviewed by Wrike personnel. Wrike implements appropriate technical and organizational measures to ensure that AI-assisted processing of Customer and prospective customers data is conducted in a manner that protects the rights and freedoms of the data subjects. Wrike does not use call or video recordings, transcripts, email content, or related communications described in this section to make solely automated decisions that produce legal effects or similarly significant effects on individuals without providing a mechanism for human review and the ability for the individual to contest the outcome. If automated decision-making or profiling would be utilized, we would provide you with specific notice and the right to human intervention, to express your point of view, and to contest the decision. Wrike does not permit third-party providers engaged to provide transcription, storage, analytics, or AI-assisted services to use such data to train their own general-purpose AI models, except where expressly authorized by Wrike and permitted by applicable law and contract. Current Customers and Users are responsible for ensuring that they do not activate call or video recording and/or AI processing features where their applicable services agreement, internal policies, or legal obligations do not permit them to do so. By activating such recording and/or AI processing features, the User represents, both for him or herself and on behalf of their employer/Customer, that they are authorized to do so and that any required notices, consents, or approvals have been obtained.

4. Disclosures of personal data

We disclose personal data as follows:

- For the uses of information described above,
- For making 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 set out above, we may disclose information to:

- Our affiliates;
- Other third party 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, event services, chatbot technology providers, event sponsors,

webinar providers, customer relationship management providers, accounting providers, technical service providers, our payment processor, and the marketing and analytics companies and other providers described in Section 6 below or as listed on our Cookie Preferences tool linked in the footer of our website as well as providers of conference, recording, transcription, storage, analytics, and AI-Large Language Model (LLM) infrastructure that help us process videoconferences, transcripts, and email communications for the purposes described in this Privacy Policy. We may engage a third-party provider to host or operate any aspect of our business, potentially including any mechanism through which we send or receive communications, such as our email systems and websites. Certain third-party providers engaged in this manner may collect information from you directly when you interact with us;

- Other entities involved in the legal-related matters described above;
- Other entities involved in the significant corporate transactions described above, such as an acquirer of Wrike; or
- Regulatory authorities, courts, or government agencies where we believe disclosure is necessary as a matter of applicable law or regulation.

5. 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 a contract with them. For example, when an individual purchases admission to a Wrike event or purchases a Wrike account for their single-person business, we may process their payment information on this basis.
- *Consent:* Where required by law, and in some other cases, we handle personal data based on consent. For example, some of our direct marketing activities happen because of opt-in consent, such as sending marketing emails to individuals who have requested them. We also rely on consent to record videoconferences and to process the resulting recordings and transcripts. Where required by applicable law, including in jurisdictions that require all-party or two-party consent, the consent prompt will be presented before recording begins. If an individual wishes to withdraw consent to the recording of videoconferences, they may do so by asking the host of the

videoconference to stop recording during the session. Withdrawal of consent will apply to future recording activities after the withdrawal is processed and, unless otherwise required by applicable law, will not affect the lawfulness of recording or processing carried out prior to withdrawal. Wrike will assess any request relating to deletion of previously created recordings or transcripts in accordance with applicable law and its contractual obligations

- *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. Specifically, for prospective customers, we rely on legitimate interests to provide relevant information about our Service Offerings, provided that such interest is balanced against the individual's privacy expectations. Subject to applicable law, these legitimate interests may also include internal training, quality assurance, service improvement, sales enablement, business analytics, and the use of AI-enabled tools to assist with those activities in relation to email communications and other business communications that are not subject to a consent requirement. If our processing (especially involving AI) would likely result in a high risk to the rights and freedoms of natural persons, we would (i) conduct a Data Protection Impact Assessments (DPIAs) where our processing (especially involving AI) is likely to result in a high risk to the rights and freedoms of natural persons and (ii) update the Privacy Policy.
- *Legal compliance:* We need to use and disclose personal data in certain ways to comply with our legal obligations.

6. 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, 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. 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 the following categories:

- *Essential:* These are necessary for our website to function and cannot be switched off in the Cookie Preferences menu. You can set your browser to block or alert you about these cookies, but some parts of the site will not work if you block these.
- *Functional:* These mainly let the website provide enhanced functionality and personalization. If Functional cookies are off, some of these features may not work properly.
- *Analytics:* These cookies mainly let us count and understand visits and traffic sources so we can measure and improve the performance of our website. They may collect information including clicks, cursor movements, and other interactions with pages on our website. They help us to know which pages, emails and online content are the most and least popular and see how visitors move around and interact with the website. For example, they allow us to measure how effective our ads are in bringing visitors to our website.
- *Ad Targeting:* We and our advertising partners use these cookies mainly to build a profile of your interests and show you relevant ads on other websites and deliver other online or offline marketing to you. If these cookies are blocked, you may experience advertising that is less targeted.

To manage cookies on a Wrike website, click on the Cookie Preferences link in the footer of the website, adjust your preferences, and click Submit Preferences. If you replace, change or upgrade your browser, or delete your cookies, or use a browser that automatically deletes cookies, you may need to use this opt-out tool again.

To learn more about interest-based advertising, including certain additional opt-out options for 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. If you replace, change or upgrade your browser, or delete

your cookies, or use a browser that automatically deletes cookies, you may need to use these opt-out tools again.

If you use an eligible browser, you can send an opt-out signal to Google Analytics and customize the Google Display Network ads for that browser by visiting the Google Ads Settings page and installing the Google Analytics Opt-out Browser Add-on . If you replace, change or upgrade your browser, or delete your cookies, or use a browser that automatically deletes cookies, you may need to use these opt-out tools again.

If you visit our website or apps from your mobile device, 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.

7. 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/en-us/articles/25097464163607-Contact-Wrike-Customer-Support, 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 unsubscribed 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 their 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;
- The right to restrict the processing of personal data where the accuracy of the data is contested or the processing is unlawful;
- Object to our processing of the information for direct marketing purposes;
- Object to other processing of the information;
- The right to opt-out of "profiling" if such profiling was to be used to make decisions with legal or similarly significant effects;
- The right to be informed about the logic involved in any automated decision-making process;
- The right to non-discrimination for exercising any of your privacy rights; 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 Customer Data, Users should contact the relevant administrator for the Workspace associated with Customer 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.

8. Security

To provide security for Customer Data within the Platform, we maintain physical, organizational, and technical safeguards, designed to protect personal data, and we update these safeguards periodically. 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 Customer 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, as well as third-party sites hyperlinked from ours, are handled by such third parties subject to their own privacy and security procedures, which we do not control.

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.

9. Data retention

Wrike retains personal data only for the period necessary to fulfill the purposes for which it was collected, as described in this Privacy Policy. To determine the appropriate retention period, we apply a criteria-based retention schedule that considers the nature of the data, our legal obligations, and potential limitation periods for legal claims.

Our retention criteria are as follows:

- Customer account information: We retain personal data related to your active account for the duration of your contract with us. Following contract termination, we retain core account records (such as invoices, signed contracts, and payment history) for 10 years to comply with statutory tax and commercial record-keeping obligations.
- Prospect and marketing data: personal data collected for marketing purposes (e.g., lead generation forms, webinar registrations) is retained for as long as you remain an "active prospective customer." We consider you active as long as you continue to interact with our communications. If no interaction is recorded for a period of 36 months, your personal data will be deleted or anonymized, unless you have opted out, in which case we retain only a record of your opt-out preference to ensure we respect your choice.
- AI-processed business communications: recordings, transcripts, and AI-generated summaries of business meetings are retained for a standard period of up to 12 months for quality assurance and training purposes, unless a specific legal hold is applied or a longer period is contractually agreed upon with the relevant Customer.

- Security and audit logs: information collected for security monitoring, fraud prevention, and system integrity (such as IP addresses and access logs) is typically retained for a maximum of two years, after which it is overwritten or deleted, unless required for an ongoing investigation.
- Cookies and automated data: The retention periods for data collected via cookies vary by category (e.g., “Essential” vs. “Analytics”). Categories of cookies are detailed in our Cookie Preferences tool. By way of example, most analytics cookies are set to expire within 12 to 24 months.

Once the retention period has expired or the purpose for processing has been exhausted, we will either permanently delete the data, destroy it, or anonymize it such that it can no longer be associated with a specific individual. Personal data may remain in encrypted backup copies for a limited period beyond the primary retention period as part of our disaster recovery and business continuity protocols.

10. 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 Customer 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 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. 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, including on the basis of the recipient's membership in the DPF, Standard Contractual Clauses or other appropriate contract language, depending on the situation. 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. If we were to transfer personal data to a country that does not provide an adequate level of protection, we would perform a Transfer Impact Assessment (TIA) to ensure that the data remains protected by safeguards equivalent to those in the jurisdiction of origin.

Personal data processed through providers of conference, recording, transcription, storage, analytics, and AI-assisted services, including in connection with recorded videoconferences and email communications, may be transferred to and processed in the United States and other countries where Wrike or its providers and their sub processors operate, subject to applicable transfer mechanisms and safeguards.

11. Children

The Service Offerings are not directed at minors under 18. We do not knowingly collect personal information from minors under 18. If you become aware that a minor may have provided us with personal information, please alert the appropriate support team

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 Customer 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: Data Protection Officer
550 West B Street, Floor 4, PMB 2305
San Diego, CA 92101
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 California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CPRA"), and its regulations (collectively, 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 Customer Data or personal data that we receive and process on behalf of our customers in connection with performing our Service Offerings as explained above, which is handled as described in Section 1 of our Privacy Policy, even when the Customer Data or such related personal data is about a resident of California.

Retention:

Your personal information is retained until after its retention no longer is necessary to fulfill the business purposes described in this policy, or as otherwise required under law. Because we may collect and use the same category of personal information for different purposes and in different contexts, there is no fixed retention period that always will apply to a particular category of personal information. Duration of retention may vary depending upon factors such as legal compliance requirements, recordkeeping or, for resolving inquiries or complaints, and the existence of an ongoing relationship with you. Personal information may persist in copies made for backup and business continuity purposes for longer than the original copies.

"Sale," "sharing," and related opt out

As described further below, some of our disclosures of personal information qualify as what the CCPA defines as a "sale" or "sharing" of personal information. During the 12 months leading up to the effective date of this Privacy Policy, we "sold" and "shared" (as those terms are defined under the CCPA), what the CCPA calls "identifiers" (like IP addresses and email 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) about Californians to third parties that assist us, such as marketing partners and analytics providers. This practice continues today. To our knowledge, we do not "sell" or "share" (as those terms are defined under the CCPA) the personal information of individuals under 16 years of age.

To request to opt out of "sales" or "sharing" (as defined in the CCPA), follow the instructions on our Your Privacy Choices form. You also can contact us at privacy@team.wrike.com to perform the portion of the "sale" or "sharing" opt-out process in which you provide us with contact information.

Your browser may also offer a way to activate the Global Privacy Control signal ("GPC"). Wrike.com treats qualifying browsers for which the user has activated the GPC signal as having opted out of what CCPA calls a "sale" or "sharing" of any California personal information that is collected on that site from that browser using cookies and similar technology. You can override that treatment for a GPC-enabled browser by using the cookie controls available via the Cookie Preferences link in our website footer to opt into particular categories of cookies from that browser. In that case, "sales" and "sharing" via cookies and similar technology in those categories may resume on that browser.

Opting out of "sales" and "sharing" limits only some types of disclosures of personal information, and there are exceptions to all of the rights described in this Section.

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, accounting providers, payment processors, service providers (including providers of analytics and AI-enabled tools), 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 of which is personal information), transaction data, and information about interactions with Wrike or our partners	Same as first row
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
Inferences drawn from personal information we collect including insights generated through automated tools	Same as first row

Notice at Collection:

At or before the time of collection of personal information from California residents, Wrike provides a notice at collection. This notice includes the categories of personal information to be collected (as detailed in the table above), the purposes for which the information is used (as described in Section 3), whether that information is "sold" or "shared" (as described in Section 14), and the criteria used to determine the period of time the information will be retained (as described in Sections 9 and 14). If you provide us with personal information through our website forms or via a lead generation tool, our Privacy Policy is provided via a link or text adjacent to the point of collection.

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," "shared," or disclosed about you for a business purpose; the business or commercial purpose for collecting, "selling" or "sharing" your personal information; and the categories of third parties to whom we have "sold," "shared," or 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 receive "discriminatory treatment" (within the meaning of the CCPA) or retaliation for exercising the privacy rights conferred by the CCPA.

Limit the Use of Sensitive Personal Information:

Wrike does not use or disclose Sensitive Personal Information for purposes other than those permitted by the CCPA/CPRA (e.g., to perform services or for security purposes). As such, we do not currently offer a "Limit the Use of My Sensitive Personal Information" option, as our usage is already restricted to these exempt business purposes. .

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, login to your existing Wrike account (if there is one), or otherwise verify 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 an appropriate power of attorney. Unless we receive an appropriate power of attorney, we also may require the consumer to verify their identity directly with us and confirm directly to us that they authorized you to submit the request on their behalf. For security and legal reasons, we do not accept personal information requests that require us

to visit a third-party website or install special software (such as one operated by an agent) to view or respond to the requests.

To request to exercise any of these rights, please write to us at privacy@team.wrike.com or visit https://www.wrike.com/contact-us/ and use the "If you're still looking for answers" form near the bottom of the page.

15. Definitions

- **"CCPA"** means the California Consumer Protection Act (as amended by the California Privacy Rights Act ("CPRA") (collectively "CCPA")). 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.
- "**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.
- "**Platform**" means the hosted, on-demand, cloud-based work management and collaboration platforms on wrike.com and klaxoon.com and the Wrike desktop and mobile apps and Klaxoon mobile app.
- "**Platform Plan**" means a Customer's subscription to the Platform.
- "**Customer 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 licensed to use a Service Offering. Within the Platform, there are Full Users and Limited Users. 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.