

Privacy Policy

Effective Date: October 1, 2023

Spot is an online incident reporting, case management, and DEI compliance training platform for reporting and managing cases of harassment, discrimination, bullying, misconduct, and other issues in the workplace, as well as surfacing employee feedback and providing compliance training through a DEI lens. This Privacy Policy explains the collection, use, and sharing of information and data across the websites, emails, and mobile applications that facilitate our incident reporting, case management, and DEI compliance training services (collectively “**Spot**”).

You use Spot either as 1) a “**Spot User**,” an unaffiliated individual using Spot for free OR an employee, member, or other affiliate of an Organization that is paying for Spot or 2) as an “**Organization**” paying for Spot and thus enabling its employees, members, or other affiliates to access their Spot instance. Organizations appoint “**Spot Administrators**” to manage their Spot account via the Spot dashboard.

Issues and concerns can be reported anonymously by Spot Users. Spot facilitates two-way communication between Organizations and their employees, members, or other affiliates so that concerns can be raised and resolved. Employees, members, or other affiliates access Spot through their Organization’s branded web portal. An Organization’s Spot Administrators manage cases and administer compliance trainings using the Spot dashboard. Individuals who are unaffiliated with an Organization that pays for Spot can use Spot for free on the web to document incidents and, if they choose, have Spot anonymously submit a report on their behalf to any recipient.

By using Spot as a Spot User or Organization, you agree to the collection, use, and sharing of information and data described in this Privacy Policy.

Our Philosophy of Privacy Protection

We do not track Spot Users or Organizations for the purposes of advertising or selling your data. We do track minimal aggregated, anonymized statistics to determine how Spot is being used. Our business model is not based on owning data, selling data, or selling access to data. Instead, we sell software as a service with the purpose of helping Spot Users and Organizations create, communicate about, and resolve confidential records and reports of workplace issues and feedback, and complete DEI compliance trainings.

The policy below explains in detail how we operate in accordance with this philosophy.

Distributed by Palace

Spot is created and developed by Palace Inc., a Delaware corporation (referred to as “**Palace**,” “**we**,” or “**us**”). This Privacy Policy applies to information that we receive via our websites, emails, and mobile applications.

Please note that we implement the principles set out in Regulation (EU) 2016/679 – General Data Protection Regulation, including the United Kingdom General Data Protection Regulation (herein as “**GDPR**”). If you have any question regarding this Privacy Policy and your rights as a data subject, please let us know by emailing hello@talktospot.com.

Data Collected by Spot & How We Use It

We collect and process your personal data based on the consent you give when using Spot. You have the possibility to withdraw your consent at any time by writing to us at hello@talktospot.com.

I. SPOT USERS

Personal data that you may provide us

If you use Spot as an employee, member, or other affiliate of an Organization, the data controller is the Organization and Palace is the data processor of this Organization. When unaffiliated individuals use Spot for free, Palace is a data controller.

When you use Spot to document issues or feedback, you may elect to provide Spot with certain personal information. The categories of data processed are the following.

Compulsory information

- Email address (the only mandatory personal data to be provided; required for us to give you access to your report; not shown to your Organization when you submit a report, whether your Organization pays for Spot or you’re using the free version of Spot; only used by the system to forward communication)

Optional information

- Your name
- Demographic information (such as your gender and occupation)
- Other information about your Organization, such as your department or location
- Name(s) of people involved in the incident
- Other details about an event, such as the time, location, or recurring nature
- Feedback to Palace about the experience of using Spot
- If using the free version of Spot as an unaffiliated individual: Email address(es) to which you would like us to submit a report

- If affiliated with an Organization that uses the Spot's DEI compliance training: Anonymous questions on training content and responses to survey questions in the training (identity is not disclosed as part of your survey responses, and responses are delivered to your Organization in batches of five to ensure privacy)

Depending on how you decide to use Spot, the personal data we collect from you may vary. For example, you may want to summarize your workplace experience without adding identifying details. This helps protect anonymity while still alerting your Organization of inappropriate behavior or unfair treatment. You can always choose "Skip," "Not applicable," or "I don't know" in response to questions.

You may elect to submit a more detailed report that includes information such as your name or the names of people involved in the incident you're reporting. You should not include sensitive data (for example, names or specific locations) in a Spot report if you want to submit it to your Organization and preserve anonymity. Spot asks you early in the process if you would like to stay anonymous and gives tips for doing so. Please understand that you are solely responsible for deciding the amount of personal data to include in a Spot report.

Using Spot's incident reporting for private purposes

You may elect to provide information and generate a private report solely for your own purposes. If you create a report only for yourself, you'll receive it either as an email attachment from Spot or via your report management page, depending on whether you are accessing Spot as an unaffiliated individual or as an employee, member, or other affiliate of an Organization that pays for Spot

If you receive your report via email attachment, you'll proceed to a step that deletes all the data from your chat with Spot. We strongly advise checking the email attachment you receive before you agree to delete all data from your chat with Spot. We are not able to retrieve chat data once it's deleted.

If you access your private report via the report management page, your private report is stored indefinitely until you delete it using the "Delete" button on that page. If you submit the private report to your Organization using the "Submit report" button on that page, you can no longer delete that report.

Information retained when you submit a report to your Organization

Spot can submit your report to your Organization. How you submit your report will vary depending on whether you're using Spot as an unaffiliated individual or as an employee, member, or other affiliate of an Organization pays for Spot.

Unaffiliated individual using Spot for free

As an unaffiliated individual, you can ask Spot to submit your report to your employer or to another party. To do so, you must provide us with the recipient's email address. We use such email addresses solely for the purpose of submitting the report on your behalf.

The recipient receives an email from Spot with a link to download the report, and you receive a link to a status webpage that shows if the recipient has initiated a download. We retain the report for 30 days after the recipient downloads it for the first time, then we delete that report. If the recipient hasn't downloaded the report 90 days after the download link was sent, we delete that report from our servers. If you sent a report via Spot and the recipient has not yet downloaded it, you can delete that report from our servers on the status webpage. If the recipient is an Organization that pays for Spot, they can add the report to their Spot dashboard; in this case, the report is retained on our servers for as long as the Organization continues to use Spot.

When we email a download link to a recipient, Spot retains indefinitely the recipient's email address and a timestamp for when the download link was sent. If the recipient downloads the report, Spot also retains indefinitely a timestamp for that event. We do not retain any other data about your report. Should the recipient ever deny that they received a download link or initiated a download of your report, Spot can offer proof that the email was sent and indicate whether a download for the report was initiated. We will not have the report itself after the expiration of the 30-day period following the first download. We also will not have the report itself if you manually delete it on the status webpage before the recipient downloads it.

If you wish to obtain information regarding the delivery of a report download link or download initiation, email Spot at hello@talktospot.com. If possible, please provide: 1) the report ID on the version of the report you kept for your records, 2) the email address where you asked Spot to send the report, and 3) the date and time you chatted with Spot. We review all requests for information and will investigate whether or not the individual requesting information is entitled to receive it.

Employee, member, or other affiliate of an Organization that pays for Spot

Reports submitted to Organizations that pay for Spot may be retained by the Organization for as long as they continue to use Spot or longer, if they opt to download reports from the Spot dashboard and retain them outside of Spot. These reports cannot be manually deleted by the employee, member, or other affiliate who submitted them. For more information regarding the retention of your information, contact your Organization.

II. ORGANIZATIONS

Data collected from Organizations

As an Organization, you agree to permit Palace to collect, access, process, and use a variety of information ("**Organization Data**") when you use Spot. We rely on Spot Administrators providing

accurate data about their Organizations so that we can deliver notices and important messages and otherwise operate Spot. Data that we collect from Organizations includes:

- Information you provide when subscribing to Spot
- Financial information, including credit card, debit card, or bank account information, which you provide when paying for Spot
- Information you provide in connection with any customer support, product evaluation, and dispute resolution
- Communications through which Spot monitors the progress of reports, communications between the Organization and staff working on Spot, and other communications generated by use of our service
- All data that Spot Administrators are able to access in the dashboard, including submitted reports, follow-up interviews, messages sent to reporters, activity logs for each report, optional internal notes for each report, email addresses of trainees, completion rates of training, and aggregated responses to training survey questions

Please note that the processing of your data is necessary for the performance of the contract you signed to use Spot at your Organization.

How we use Organization Data

We use data collected from Organizations to:

- Establish the Organization's account and communicate with Spot Administrators and Spot Users regarding the Organization's account
- Operate, improve, and personalize Spot, including any collection and processing of payment
- Provide you information regarding Spot and other services or products, or provide promotional offers (consistent with your communications preferences)
- Provide reports and other information in the Organization's Spot dashboard
- Define the domain names for email addresses through which Spot Users can verify that they are employees, members, or other affiliates of an Organization that pays for Spot
- Contact Spot Administrators and Spot Users to detect, prevent, and mitigate fraudulent or illegal activities, investigate or inform about any security issues, enforce our Terms of Use or other applicable policies or agreements, and comply with our legal obligations

Data that we retain

We retain Organization Data, including personal data collected from their Spot Users, as long as it is necessary and relevant for the operation of the service for which you are paying. When your Organization stops using Spot and your relationship with Palace is terminated, we retain your Organization's data for 90 days from the expiration of your Organization's subscription to Spot. This data is retained for backup purposes, facilitating a transition to another case management system, or simply allowing Spot Administrators to retrieve all report data from the Organization's Spot

dashboard. You can request that we delete all data immediately upon expiration of your Organization's subscription to Spot.

We do not retain the content of chats (used to create reports), conducted with the Spot chatbot by employees, members, or other affiliates of an Organization that pays for Spot. We also do not retain the content of Spot forms (used to create reports), filled out by employees, members, or other affiliates of an Organization that pays for Spot. We do retain private reports, unless a private report is deleted by the Spot User who created it, so that Spot Users can access them in the future. We also retain submitted reports so that Organizations can manage and investigate them and comply with data retention obligations.

We have strict internal policies that prohibit Palace personnel from monitoring communications with the Spot chatbot, reading reports submitted to the Organization, or reading reports' internal notes and activity logs. Communications with the Spot chatbot cannot be accessed because chats are conducted locally on the Spot User's device and that data is not stored. We have technical restrictions in place for accessing information that is saved by Spot Users, submitted to Organizations by Spot Users, and added to the dashboard or sent to Spot Users by Spot Administrators. An extremely limited list of persons with authorization, which includes password and two-factor authentication protection, can access this information, and the list of those with authorization is audited regularly. Such authorization is used only to investigate technical issues or when required to provide customer support to the Organization.

Under certain circumstances, we may retain data from Organizations whose subscriptions to Spot have been terminated. We do this to ensure that the service is not interrupted and no data is lost due to interrupted service plans, lengthy renewal discussions, or other unanticipated events. We may also do this to prevent fraud, collect any fees owed, resolve disputes, troubleshoot problems, assist with ongoing investigation, enforce our Terms of Use, comply with applicable legal data retention obligations, and take other actions permitted by law.

Protection of Organization Data

As an Organization, you agree that Palace acts as the data processor and you act as the data controller regarding the processing of personal data of your employees, members, and other affiliates, and respect the following data protection clause. (When unaffiliated individuals use Spot, Palace is a data controller.)

Palace, that acts as a data processor, processes Spot Users' personal data and Organization Data following the written instructions received from the Organization, acting as a data controller. Palace and the Organization shall comply with their respective obligations under any applicable data protection laws and regulations and in particular under GDPR of 27th April 2016 which article 28.3 prescribe to detail the following points:

- The purposes of the processing operation are to help the Organization and its employees, members, and other affiliates: create reports of workplace issues and feedback; at the specific

request of employees, members, and other affiliates, submit their reports to the Organization; manage, investigate, communicate about, and resolve reports; and complete DEI trainings, including anonymous questions on training topics and anonymous surveys on employee experience of training topics.

Categories of data

The categories of data processed are the following, being specified that the provision of certain information is compulsory and the provision of other information is optional.

Compulsory information

- Obfuscated email address of any Spot User submitting a report (the only mandatory personal data to be provided; not shown to the Organization and only used by the system to forward communication)
- Email addresses and names of Spot Administrators

Optional information that may be collected from Spot Users depending on customizations requested by the Organization

- Their name
- Demographic information (such as gender and occupation)
- Other information about the Spot User, such as department or location
- Other details about an event, such as the time, location, or recurring nature
- Name(s) of people involved in the incident
- Feedback about the experience of using Spot
- Anonymous questions on training content and responses to survey questions in the training (identity is not disclosed as part of your survey responses, and responses are delivered to Organizations in batches of five to ensure privacy)

Data classes

- Spot User
- Organization
- Spot Administrator (on behalf of an Organization)
- People named in an incident report

Obligations of the data processor

- Palace shall ensure that any agent or subcontractor employed by Palace to process Organization Data has implemented controls to prevent unauthorized or unlawful processing or accidental loss or destruction of the data;
- Palace shall engage subcontractors only under terms that confer the same requirements for security and duty of confidence as Palace. Palace shall notify Organization of new subcontractors;
- Palace shall ensure that each of its employees, agents, or subcontractors are made aware of its obligations with regard to the security and protection of Organization Data and maintain the same levels of security and protection as Palace.
- Palace shall not divulge Organization Data whether directly or indirectly to any person, firm, or company without the express consent of the Organization except to those of its employees, agents and subcontractors who are engaged in the processing of the data and are subject to the binding obligations referred to above.
- Palace must inform Organization as soon as it is aware of any data breach or data violation as considered by article 33.2 of the GDPR;
- Palace must help and assist Organization in ensuring compliance with obligations pursuant to article 32 to 36 of the GDPR (security, PIA, prior consultation of the DPA in case the PIA results indicate that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk);
- Palace agree to provide Organization on request with whatever information the Organization requires to ensure that Article 28 of the GDPR obligations are met;
- Palace will assist Organization in providing subject access requests and allowing data subjects to exercise their rights under the GDPR; should Palace receive a subject access request, Palace will notify Organization without undue delay and not later than 24 hours of receiving the subject access request;
- Palace will assist Organization in meeting its GDPR obligations in relation to the security of the processing, the notification of data breaches and carrying out data protection impact assessments;
- If Palace becomes aware of a data breach, Palace will notify Organization of the breach without undue delay and not later than 24 hours after becoming aware of the data breach;
- Palace and its subcontractors must comply with the GDPR;
- If Palace considers one of Organization's instructions constitute a violation of the data protection law, Palace must inform Organization immediately;
- As the case may be, if Palace needs to transfer the processed data outside of the European Union to comply with a legal obligation and except if such transfer is made under Organization's instruction, Palace must inform Organization of such transfer in advance of the transfer and demonstrate to Organization its legal obligation to make this transfer;
- Palace must make available to Organization all information necessary to demonstrate its compliance with its obligations specified in article 28.3 of the GDPR to enable Organization, or any mandated by the controller auditor, to conduct audits, including inspections, and Palace must help the conduct of such audits;
- In case of termination of your contractual relationship with Palace, for any reason whatsoever, Palace must securely return/delete all the processed data immediately if requested by Organization; in the case of secure deletion, Palace will provide a certificate of secure deletion if requested by Organization.

Communication Preferences

We do not sell or rent your information to third parties for their marketing purposes without your explicit consent. We use Spot Users' email addresses to send PDF versions of Spot documents or a link to a report status page where the full report is accessible and can be downloaded as a PDF; to send a link to your report management page if your Organization pays for Spot; to verify Spot Users as employees, members, or affiliates of an Organization that pays for Spot through email domain verification; to notify Spot Users of action taken on your reports; and/or to respond to Spot Users if you contact us. We use Spot Administrators' email addresses to send notifications of report updates.

You may choose to subscribe to a newsletter on our website. In this case, we may contact you via email with news updates and special offers. We may also contact you with information about products and services from our business partners. You may opt out of such commercial communications at any time by following the opt-out instructions provided in these messages.

Exercising Your Rights

We will honor any statutory right you might have. In accordance with the applicable law, each Spot User has the right to access, rectification, and erasure of personal data, and a right to object to processing of personal data by writing to hello@talktopot.com. Spot will not use automated decision-making, including profiling, in the provision of its services. Unaffiliated individuals who use Spot for free can ask for their personal data to be transferred to them or to another controller or request restriction of the processing of their personal data.

In accordance with certain applicable law, you also have the right to lodge a complaint to us by writing to hello@talktopot.com or to a data protection authority.

As the data controller when unaffiliated individuals use Spot, Palace acknowledges the rights below. If you're an employee, member, or other affiliate of an Organization that pays for Spot, contact your Organization, which is the data controller.

- Right to be informed: You can expect clear and concise information from us about what we do with your personal data
- Right of access: You can ask us if your data is being processed and request information about the processing operations; if you wish to do so, you can also ask us for a copy of your data
- Right to rectification: You can ask us to rectify, change, or update your personal data at any time
- Right to erasure: You can ask us to erase your personal data in certain cases
- Right to data portability: Upon certain conditions, you can request a copy of your data or its transmission to another controller
- Right to objection: You can object, in certain cases, to the processing of your data

- Right to restriction of the processing: You can ask us to limit the processing operations to only retention of your data in certain cases
- Rights related to automated decision-making, including profiling: Spot will not use automated decision-making, including profiling, in the provision of our services

For cases where Palace acts as the data controller, we will try to resolve your requests as soon as possible and aim for a response time shorter than 5 business days. We may have to retain certain data to comply with legal obligations, to resolve disputes, and to enforce our agreements.

Information We Collect by Automated Means

When you visit Spot's marketing website (<https://talktospot.com>), some anonymous usage data is collected to track trends in website traffic. All data collected is aggregated, and no personal data is collected.

Data collected includes referral sources, top pages, visit duration, and device information (device type, operating system, country of origin, and browser).

We use analytics on our website to understand how many people visit our website. We do so without the use of cookies or storing any identifiable data about an individual user.

When a Spot Administrator accesses their Organization's Spot dashboard, we collect the Spot Administrator's Internet protocol ("IP") address for security purposes. This information allows us to detect suspicious activity on your Organization's account.

Cookies

When you use Spot, we log essential information using "cookies," which are small data files stored on your hard drive by a website. You will not see a cookie banner on our website because we only store essential cookies. Please note, you have the option to block and delete these essential cookies through your browser settings. Doing so will impact the service we provide to you. Here is a list of all cookies we store while you use Spot.

First-party cookies

In what follows, we first list the **cookie name** and then follow with the **reason for usage**:

textSize: If the user changes the text size via our accessibility options, the chosen text size gets stored in the cookie "textSize".

reduceMotion: If the user toggles the reduce motion option via our accessibility options, the chosen state gets stored in the cookie "reductMotion".

companyIdentifier: If the user opens the unique link for their Organization to create a report or has looked up their Organization's name on our [Find](#) page, we store the Organization's internal ID as a cookie. This allows the application to remember what Organization a report should get submitted to.

companyName: If the user opens the unique link of their Organization to create a report or has looked up their Organization's name on our [Find](#) page, we store the Organization's name as a cookie. This allows the application to display the user's Organization's name throughout the application.

verificationId: This cookie is set to a static ID from a user's Organization to store that the user has verified that they are part of the Organization they claim to be.

trackedIntroVisit: This is set to "true" if the user has visited the Spot reporting application. This is set to avoid the browser calling further API calls to anonymously track number of visits. This doesn't track the user as it's solely set to "true".

loadingCompanyInfo: This is temporarily set to "true" during application loading and set to "false" on successful load.

localeOverride: Some Organizations have Spot set up for multiple languages. When the user picks their preferred language, that language code identifier is stored in the "localeOverride" cookie so that future usages of Spot are presented in the language the user previously picked.

<REPORT_ID>.authToken :This cookie is used for authentication purposes when accessing a report.

token: This cookie is used for authentication purposes when accessing a training course by Spot.

introShown: This cookie is set to "true" as soon as the user has accessed the first screen of a Spot training course. This is needed so that the user isn't presented the same screen again.

onboarding: This cookie is set to "true" as soon as the user has completed the onboarding instructions of a Spot training course. This is needed so that the user isn't presented with the same onboarding instructions again.

connect.sid: This is a session identifier used throughout the admin dashboard. It is deleted on logout and also automatically after 30 minutes of inactivity.

deviceToken: This cookie is used if a user of the admin dashboard wants to skip two-factor authentication on a given device for 30 days.

Third-party cookies

We do not use or store any third-party cookies.

Disclosure of Spot Users' and Organizations' Information

We created Spot to provide a secure way to report harassment, discrimination, and other workplace issues, not to obtain data to sell or rent to third parties. The circumstances in which we disclose Spot Users' data or Organizations' data are limited to the following:

- You provide express consent;
- We need to share your information with service providers for the limited purpose of processing data on our behalf in order to operate Spot and improve Spot's features and functionality, including fulfilling reporting requests (subject to contractual data protection requirements);
- We believe it is necessary to investigate potential violations of or enforce our Terms of Use, or we believe it is necessary to investigate, prevent, or take action regarding illegal activities, suspected fraud, or potential threats against persons, property, or the systems on which we operate Spot;
- We determine that the access, preservation, or disclosure of information is required or permitted by law to protect the rights, property, or personal safety of Spot or Spot Users, or is required to comply with applicable laws, including compliance with warrants, court orders, subpoenas, legal process, or other lawful government requests (including in response to public authorities to meet national security or law enforcement requirements);
- We share aggregated usage statistics that cannot be used to identify users individually;
- We do so in connection with the sale or reorganization of all or part of our business, as permitted by applicable law

While we use contractual and other measures to ensure protection of information, the laws and regulations relating to privacy and information protection in other legal jurisdictions may not be the same as, or similar to, your local privacy laws. The governments, courts, law enforcement, or regulatory agencies in these other jurisdictions may be able to request disclosure of personal data through the laws of these countries. In an effort to respect your privacy, we will not otherwise disclose your personal data to law enforcement, other government officials, or other third parties without a subpoena, court order, or substantially similar legal procedure, except when we believe in good faith that the disclosure of information is necessary to prevent imminent physical harm or financial loss, or to report potentially illegal or fraudulent activity.

Other Important Information

Security safeguards

We're committed to protecting the security of your information and take reasonable precautions to protect it. We use industry-standard encryption to protect your data in transit and while it is stored on

our servers. This is commonly referred to as transport layer security (TLS) or secure socket layer (SSL) technology. However, Internet data transmissions are not guaranteed to be 100% secure, and we cannot ensure the security of information during its transmission between you and us. Accordingly, you acknowledge that when you transport such information, you do so at your own risk.

We protect your information in our systems using technical and administrative security measures designed to reduce the risks of loss, misuse, unauthorized access, disclosure, and alteration. Some of the safeguards we use are firewalls and data encryption, physical access controls to our data centers, and information access to authorization controls.

As the data processor, if Palace learns of a system breach, we will notify your Organization as soon as possible, and in any event within 24 hours, and provide information on protective steps, if available, using the information that you have provided to us. We may also post a notice on our website and/or notify your Organization via other communication platforms. Depending on where you live, you may have a legal right to receive such notices in writing.

We explicitly recommend that Spot Users do not access Spot from any work device or while on a work network or a non-secure network. We cannot prevent, nor be held responsible for, you being monitored by others, particularly if you communicate using computing devices or networks owned or controlled by third parties, such as your employer.

If you received suspicious reports via a Spot email address, please contact us at hello@talktopot.com.

Vulnerability disclosure policy

Spot is committed to protecting your safety and keeping your data secure. If you believe you've discovered a potential security vulnerability with Spot's online systems, we appreciate your help in disclosing the issue to us at security@talktopot.com.

Privacy of minors

Spot is not intended for minors. Minors, as defined in the country of the Spot User, are expressly prohibited from using Spot or providing any personal data. If you become aware that a minor has provided us with personal data without parental consent, please contact us at hello@talktopot.com. If we become aware that we have inadvertently obtained information in violation of applicable laws, we will delete such information if we can identify it.

Scope of policy

This Privacy Policy describes your privacy rights when you elect to use Spot, and by using Spot or engaging with us, you accept the substance and application of these terms and policies, and consent to our collection, use, disclosure, and retention of your personal data as described in this Privacy

Policy. Should you ever disagree with this Privacy Policy, you may provide us with your feedback at hello@talktospot.com. The information about you that we collect through Spot is controlled by Palace Inc.

California Privacy Rights

If you are a California resident, California Civil Code Section 1798.83 permits you to request information regarding the disclosure of your personal information to third parties for their direct marketing purposes. To make such a request, please send an email to hello@talktospot.com.

Your rights and choices

The CCPA provides consumers (California residents) with specific rights regarding their personal information. This section describes your CCPA rights and explains how to exercise those rights.

Access to specific information and data portability rights

You have the right to request that Spot disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request, we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting or selling that personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you (also called a data portability request).
- If we sold or disclosed your personal information for a business purpose, two separate lists disclosing: sales, identifying the personal information categories that each category of recipient purchased; and disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.

In particular, Spot has collected and processed the following categories of personal information within the last twelve (12) months:

Category: Identifiers, including personal information listed in customer records statutes.

A real name; email address.

Category: Protected classification characteristics.

Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, or veteran or military status.

Category: Usage.

Information on the user's interaction with Spot.

Category: Geolocation data.

Physical location of users, generally and specifically.

Use of personal information

We may use or disclose the personal information we collect for one or more of the following business purposes:

- To fulfill or meet the reason you provided the information. For example, if you share your name and contact information to request a price quote or ask a question about our services, we will use that personal information to respond to your inquiry. If you provide your personal information to purchase a service, we will use that information to process your payment and facilitate delivery. We may also save your information to facilitate new service orders.
- To provide, support, personalize, and develop our websites, products, and services.
- To create, maintain, customize, and secure your account with us.
- To process your requests, purchases, transactions, and payments and prevent transactional fraud.
- To provide you with support and to respond to your inquiries, including to investigate and address your concerns and monitor and improve our responses.
- To personalize your website experience and to deliver content and product and service offerings relevant to your interests, and via email (with your consent, where required by law).
- To help maintain the safety, security, and integrity of our websites, products and services, databases and other technology assets, and business.
- For testing, research, analysis, and product development, including to develop and improve our websites and services.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- As described to you when collecting your personal information or as otherwise set forth in the CCPA.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Spot's assets, whether as a going concern or as part of

bankruptcy, liquidation, or similar proceeding, in which personal information held by Spot about our service users is among the assets transferred.

Spot will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Non-discrimination

We will not discriminate against you for exercising any of your CCPA rights. Unless permitted by the CCPA, we will not:

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

However, we may offer you certain financial incentives permitted by the CCPA that can result in different prices, rates, or quality levels. Any CCPA-permitted financial incentive we offer will reasonably relate to your personal information's value and contain written terms that describe the program's material aspects. Participation in a financial incentive program requires your prior opt-in consent, which you may revoke at any time.

Exercising access, data portability, and deletion rights

To exercise the access, data portability, and deletion rights described above, please submit a verifiable user request to us by emailing us at hello@talktospot.com

Only you, or a person registered with the California Secretary of State that you authorize to act on your behalf, may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you.

Making a verifiable consumer request does not require you to create an account with us. However, we do consider requests made through your password-protected account sufficiently verified when the request relates to personal information associated with that specific account.

We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Updates to our Privacy Policy

We may revise this Privacy Policy from time to time by posting an updated version on the Spot website. The revised Privacy Policy will be effective immediately for Spot Users. You may always determine if this Privacy Policy has changed by checking the effective date at the top of the page.

For Organizations that pay for Spot, if we make a change that we believe reduces your rights or increases your responsibilities, we will notify you by email prior to the change becoming effective. If we update this Privacy Policy, you are free to decide whether to accept the update or to stop using Spot. Your continued use of Spot after an update is effective will be deemed to represent your consent to the provisions in the updated Privacy Policy.

Contact Information

Please contact us with any questions regarding this Privacy Policy:

hello@talktopot.com