



Privacy Notice

Effective Date: March 4, 2024

Date Last Updated: October 9, 2023

This Privacy Notice (“Notice”) only applies when Drata Inc. (“Drata,” “us,” “we,” or “our”) is the Controller of personal data (example: Drata website visitors’ personal data and business-to-business contact data). Drata is a Processor, not a Controller, of personal data that we process on behalf of our Customers when they use Drata products and Services. For clarity, this means that this Notice does not apply to Drata products and Services. If you have questions related to how a Drata Customer utilizes your personal data, please contact them directly. We are not responsible for the privacy or data security practices of our Customers. This Notice also does not apply to personal data about current and former Drata employees, job candidates, or contractors and agents acting in similar roles.

Table of Contents:

1. Introduction
2. Personal Data We Collect and Disclose
3. How We Process Personal Data
4. Sources of Personal Data
5. Cookies and Tracking Technologies
6. Security and Retention
7. Children’s Privacy
8. External Links
9. Supplemental Terms for California Residents
10. Supplemental Information for the EEA, Switzerland, and the U.K.
11. Supplemental Information for Other Regions
12. Contact Information
13. English Version Controls

1. Introduction

Capitalized terms that we use but are not defined in the Notice (such as Site, Services, etc.) have the meaning provided in our Terms of Service - Subscription Agreement (“Agreement”). If you are located in the European Economic Area (“EEA”), Switzerland, or the United Kingdom (“U.K.”), please refer to Section 10 of this Notice for more information about which specific entity or entities act as a controller of your personal data.

When Does This Notice Apply? This Notice only applies to personal data that Drata handles as a Controller (meaning where Drata controls how and why your personal data is processed). This includes when you:

- Visit or interact with the drata.com website, our branded social media pages, and other Sites which we operate (collectively, our “Digital Properties”);
- Register for or participate in our webinars, events, programs, marketing, and promotional activities;
- Interact with us in person, such as when you visit our offices; and
- Inquire about or engage in commercial transactions with us.

Changes: We may update this Notice from time to time. Please check back periodically for updates. If you do not agree with any changes we make, you should stop interacting with us. When required under applicable law, we will notify you of any changes to this Notice by posting an update on our Privacy Notice webpage or in another appropriate manner.

2. Personal Data We Collect and Disclose

The below table describes what personal data we collect about you and to whom we disclose personal data. California individuals: This table includes the parties we disclose personal data to for a business or commercial purpose, as defined by California law.

Categories of Personal Data Collected	Disclosures of Personal Data
Identifiers , such as your name, email address, postal address, phone number, and device identifiers (e.g.,	<ul style="list-style-type: none">• Drata Inc.• Service providers, such as security and platform vendors

Categories of Personal Data Collected	Disclosures of Personal Data
<p>advertising identifiers and IP address).</p>	<ul style="list-style-type: none"> • With third parties that are necessary to complete a transaction, such as credit card processors • Business partners who we partner with to jointly market or sell our products and Services, such as channel partners • With third parties at your direction, such as event sponsors • Professional advisors, such as lawyers, accountants, and auditors • Entities involved in a corporate transaction, including if we sell, acquire, or merge all or some of our assets • Companies that operate Cookies and Tracking Technologies, described in Section 5, such as marketing and advertising partners • To which you have consented to the disclosure
<p>Commercial information, including preferences, such as purchasing history or tendencies and transactional information, such as banking information.</p>	<ul style="list-style-type: none"> • Drata Inc. • Service providers, such as security and platform vendors • With third parties that are necessary to complete a transaction, such as credit card processors • Professional advisors, such as lawyers, accountants, and auditors • Entities involved in a corporate transaction, including if we sell, acquire, or merge all or some of our assets • To which you have consented to the disclosure
<p>Internet or other electronic network activity information and device information, such as your browsing history, search history, device information, and other information (whether passive browsing or</p>	<ul style="list-style-type: none"> • Drata Inc. • Service providers, such as security and platform vendors • Companies that operate Cookies and Tracking Technologies, described in Section 5, such as marketing and advertising partners

Categories of Personal Data Collected	Disclosures of Personal Data
<p>active engagement) regarding your interactions with us and use of our products, Services, emails, and other Digital Properties.</p>	<ul style="list-style-type: none"> • Entities involved in a corporate transaction, including if we sell, acquire, or merge all or some of our assets
<p>Geolocation information, such as approximate location based on your IP address, mobile device location, or information you provide to us (such as city and state you provide through a webform). You may be able to control collection of this data through the settings of your device.</p>	<ul style="list-style-type: none"> • Drata Inc. • Service providers, such as security and platform vendors. • Entities involved in a corporate transaction, including if we sell, acquire, or merge all or some of our assets. • Companies that operate Cookies and Tracking Technologies, described in Section 5, such as marketing and advertising partners
<p>Audio, electronic, visual, and other sensory information, such as CCTV recordings of our premises (e.g., if you visit our offices); recordings of your interactions with our sales or support teams (e.g., for quality assurance or training purposes, in accordance with applicable laws); or customer support chat or messaging logs.</p>	<ul style="list-style-type: none"> • Drata Inc. • Service providers, such as security and platform vendors. • Entities involved in a corporate transaction, including if we sell, acquire, or merge all or some of our assets
<p>Inferences as defined by California law, such as marketing you are likely to react positively to.</p>	<ul style="list-style-type: none"> • Drata Inc. • Service providers, such as platform vendors • Entities involved in a corporate transaction, including if we sell, acquire, or merge all or some of our assets

Categories of Personal Data Collected	Disclosures of Personal Data
<p>Sensitive Personal Data, such as proof of vaccination or race and ethnicity (optional) (where permissible under applicable law).</p>	<ul style="list-style-type: none"> • Drata Inc. • Service providers, such as platform vendors • Entities involved in a corporate transaction, including if we sell, acquire, or merge all or some of our assets • To which you have consented to the disclosure

In addition to the above disclosures, we may share your personal data to respond to lawful requests by law enforcement or other government authorities, including to meet national security requirements, in accordance with our Drata Law Enforcement Data Request Guideline in the Drata Trust Center. We may also de-identify, anonymize, or aggregate personal data to use or share with third parties for any purpose, where legally permitted.

3. How We Process Personal Data

We may process your personal data for the below purposes:

Purpose of Processing	Lawful Basis
<p>To provide our products, Services, and Digital Properties to you, including processing and fulfilling transactions; enabling you to access the Digital Properties and our Services; operating, maintaining, and improving our Digital Properties and Services; communicating with you, such as by completing your support requests or providing security updates; and diagnosing, repairing, and tracking service and quality issues.</p>	<p>Legitimate interests; Contract; Legal obligations</p>
<p>For our own business purposes, including maintaining internal business records and conducting internal reporting; collecting payments and performing accounting and similar business functions; auditing and managing projects related to our Services; performing IT security management and IT-related tasks, such as administration of our technologies and network; evaluating and improving our business, Services, and Digital Properties; and performing research and development of new</p>	<p>Legitimate interests; Legal obligations</p>

Purpose of Processing	Lawful Basis
<p>products and services; and processing your survey and questionnaire responses.</p>	
<p>For legal, safety, or security reasons, including to comply with legal requirements; establish, exercise, or defend against legal claims; protect the safety, security, and integrity of our property and the rights of those who interact with us or others; investigate any content or conduct policy violations; and detect, prevent, and respond to security incidents or other malicious, deceptive, fraudulent, or illegal activity.</p> <p>These safety purposes may also involve collecting and processing special categories of personal data (i.e., health data), for office visits and events where necessary for public health or as required by applicable law.</p>	<p>Legitimate interests; Legal obligations; Public interest</p>
<p>For marketing our products and Services or those of third parties, such as our business partners, including to solicit or publish testimonials or feedback about our products and Services; send you marketing and promotional communications or product recommendations (via email, phone, or other online and offline channels) about our Services or those of third parties; facilitate your participation in a contest or event; assess ad impressions or engage in contextual ad customization.</p> <p>You may opt out of marketing communications by clicking the “unsubscribe” link at the bottom of our marketing communications or contacting us via email to privacy@drata.com. Note that some of our marketing materials and information may use tracking technologies and analytics tools to help us understand your preferences. For further information, please see Section 5 below and our Cookie Notice.</p>	<p>Consent (where required by law); Legitimate interests</p>
<p>To fulfill a referral request when you use our referral service to tell a friend about our Services, including by using the name, email address, title, and company name that you provide us to contact the person to whom you are referring.</p>	<p>Consent (where required by law); Legitimate interests</p>

Purpose of Processing	Lawful Basis
You must only provide others' personal data if you have their consent to do so.	
Diversity, equity, and inclusion , such as promoting diversity, equity, and inclusion initiatives and representation within our business (where authorized by applicable law).	Consent (where required by law); Legitimate interests
Corporate transactions , such as sales, mergers, acquisitions, reorganizations, bankruptcy, and other corporate events.	Legitimate interests; Legal obligations
When you have voluntarily agreed to have your personal data processed.	Consent

Drata will honor data subject rights to the extent required by law. You may have the right to access, correct, update, and, in some cases, request deletion of your personal data (subject to exceptions). You may submit a request to privacy@drata.com.

Drata uses a limited number of third-party service providers to assist us in processing data for certain purposes. These third-party providers help support certain site features, perform database monitoring and other technical operations, assist with the transmission of data, and provide data storage services. These third parties may process or store personal data while providing their services. Drata maintains contracts with these third parties restricting their access, use and disclosure of personal data in compliance with our obligations under the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, including the onward transfer provisions, and Drata remains liable if they fail to meet those obligations and we are responsible for the event giving rise to damage.

4. Sources of Personal Data

- **Information you provide to us directly**, including when you register and communicate with us directly through our Digital Properties, visit our offices, or participate in our events, marketing, and outreach activities.
- **Information collected from your employer**, coworkers, or friends, including information about representatives or other employees of our current, past, and prospective customers, suppliers, investors, and business partners. We may also receive your information from a friend as part of a referral for our Services.
- **Information automatically collected**, including technical information about your interactions with our Digital Properties (such as IP address, browsing preferences, and purchase history). More information is available in Section 5 below and in our Cookie Notice.
- **Information from public sources**, including information from public records and information you share in public forums, such as social media.
- **Information from other third parties**, including information from third-party service and content providers, entities with whom we partner to sell or promote products and services, and social media networks (including widgets related to such networks, such as the “Facebook Like” button).

We may combine information that we receive from the various sources described in this Notice, including third-party sources and public sources, and use or disclose it for the purposes identified above.

5. Cookies and Tracking Technologies

We use cookies and other tracking technologies and offer you the option to manage these settings as described in our Cookie Notice. Some tracking technologies enable us to track your device activity over time and across devices and websites. While some browsers have incorporated Do Not Track or DNT preferences, we do not honor such signals from web browsers at this time.

6. Security and Retention

We maintain appropriate security procedures and technical and organizational measures to protect your personal data against accidental or unlawful destruction, loss, disclosure, alteration, or use.

Your personal data will be generally retained as long as necessary to fulfill the purposes for which we collected the personal data. Once you and/or your company have terminated the contractual relationship with us or otherwise ended your relationship with us, we may retain your personal data in our systems and records to ensure adequate fulfillment of surviving provisions in terminated contracts or for other legitimate business

purposes, such as to evidence our business practices and contractual obligations, to provide you with information about our products and services, or to comply with applicable legal, tax, or accounting requirements. When we have no ongoing legitimate business need nor lawful legal ground to process your personal data, we will delete, anonymize, or aggregate it or, if this is not possible (for example, because your personal data has been stored in backup archives), then we will securely store your personal data and isolate it from any further processing until deletion is possible. If you want to know more about retention periods applicable to your particular circumstance, please contact us using the details provided in Section 12 below.

7. Children’s Privacy

Our Sites and Services are not directed to children under the age of 16, and we do not knowingly collect online personal data directly from children. If you are a parent or guardian of a minor child and believe that the child has disclosed online personal data to us, please contact us using the details provided in Section 12 below.

8. External Links

When interacting with us, you may encounter links to external sites or other online services, including those embedded in third-party advertisements. We do not control and are not responsible for privacy and data collection policies for such third-party sites and services. You should consult such third parties and their respective privacy notices for more information or if you have any questions about their practices.

9. Supplemental Terms for California Residents

Pursuant to the California Consumer Privacy Act (“CCPA”), this Section 9 applies to certain personal data collected about California individuals where Drata controls how and why the personal data is processed (which the CCPA calls a “business”) and supplements the rest of our Notice above. This Section 9 does not apply to current or former employees, applicants, contractors, or agents.

a. Additional Data Processing Disclosures:

The below table provides the categories of personal data we have sold, shared, or disclosed to third parties, as defined by the California Privacy Rights Act. For reference, the table in Section 2 provides the categories of personal data collected and our disclosures of personal data.

<p style="text-align: center;">Categories of Personal Data We Collect</p>	<p style="text-align: center;">California Privacy Rights Act Details: Categories of Third Parties to Whom Personal Data is “Sold or Shared”</p>
<p>Identifiers, such as your name, email address, postal address, phone number, and device identifiers (e.g., advertising identifiers and IP address).</p>	<ul style="list-style-type: none"> • Companies that operate Cookies and Tracking Technologies, described in Section 5, such as marketing and advertising partners. • Business partners who we partner with to jointly market or sell our products and Services, such as channel partners.
<p>Commercial information, including preferences, such as purchasing history or tendencies and transactional information, such as banking information.</p>	<ul style="list-style-type: none"> • <i>Not applicable</i>
<p>Internet or other electronic network activity information and device information, such as your browsing history, search history, device information, and other information (whether passive browsing or active engagement) regarding your interactions with us and use of our products, Services, emails, and other Digital Properties.</p>	<ul style="list-style-type: none"> • Companies that operate Cookies and Tracking Technologies, described in Section 5, such as marketing and advertising partners.
<p>Geolocation information, such as approximate location based on your IP address, mobile device location, or information you provide to us (such as city and state you provide through a webform). You may be able to control collection of this data through the settings of your device.</p>	<ul style="list-style-type: none"> • Companies that operate Cookies and Tracking Technologies, described in Section 5, such as marketing and advertising partners.

Categories of Personal Data We Collect	California Privacy Rights Act Details: Categories of Third Parties to Whom Personal Data is “Sold or Shared”
<p>Audio, electronic, visual, and other sensory information, such as CCTV recordings of our premises (e.g., if you visit our offices); recordings of your interactions with our sales or advocacy teams (e.g., for quality assurance or training purposes, in accordance with applicable laws); or customer support chat or messaging logs.</p>	<ul style="list-style-type: none"> • <i>Not applicable</i>
<p>Inferences as defined by California law, such as marketing you are likely to positively react to.</p>	<ul style="list-style-type: none"> • <i>Not applicable</i>
<p>Sensitive Personal Data, such as proof of vaccination or race and ethnicity (optional) (where permissible under applicable law).</p>	<ul style="list-style-type: none"> • <i>Not applicable</i>

Although we have not “sold” or “shared” personal data for money in the past 12 months, we engage in routine practices with our Digital Properties involving third parties that could be considered a “sale” or “sharing” as defined under California law. We do not knowingly sell or share any personal data of minors under the age of 16. We do not collect or process “sensitive personal information,” as defined by California law, to infer characteristics about you. Drata only uses sensitive personal information consistent with the exceptions to the right to limit sensitive personal information.

Financial Incentives: We may offer a benefit or offering in exchange for you providing personal data, such as a discount or coupon to individuals who respond to a survey. As part of these surveys we may collect personal data, such as your name, contact information, preferences, experiences, beliefs, opinions, and other responses to the survey questions. Participation in surveys is governed by the applicable terms and conditions for the survey, which will describe any financial incentives associated with that survey and how to participate. The value of your data is the value of the offer presented to you. We have calculated such value by using the expense related to the

benefit. You may withdraw from any financial incentive at any time by emailing us at privacy@drata.com. If we offer another type of financial incentive, we will share with you the material terms of each offer when we ask you to participate.

b. Your Data Protection Rights:

Subject to legal limitations, certain California residents may have the below rights.

- **Right to Know.** You have the right to request information about the categories of personal data we have collected about you, the categories of sources from which we collected the personal data, the purposes for collecting the personal data, the categories of third parties to whom we have disclosed your personal data, and the purpose for which we disclosed your personal data. You may also request information about the specific pieces of personal data we have collected about you (“Specific Pieces Report”).
- **Right to Delete.** You have the right to request that we delete personal data that we have collected from you.
- **Right to Correct.** You have the right to request that we correct inaccurate personal data that we maintain about you.
- **Right to Opt Out of Sale or Sharing.** We do not sell personal data to third parties in exchange for money. However, as we explain in Section 5, we share information with advertising partners and allow advertising partners to collect information from our Digital Properties. This exchange may be considered a “sale” or “sharing” under California law, and you have the right to opt out of this “sale” or “sharing” of personal data.

California residents may request to exercise the Right to Know, the Right to Delete, and the Right to Correct by emailing us at privacy@drata.com. We will not discriminate against you, in any manner prohibited by applicable law, for exercising these rights.

How to Fully Exercise the Right to Opt Out of Sale or Sharing: In order to fully exercise the Right to Opt Out of Sale or Sharing with respect to any “sale” or “sharing” of information, you must undertake both of the following steps:

1. Submit a Right to Opt Out of Sale or Sharing request by emailing us at privacy@drata.com; and
2. Disable the use of advertising cookies and other tracking technologies by clicking the “Do Not Sell or Share My Personal Information” link in our website footer. You must complete this step on each of our Sites from each browser and on each device that you use. These steps are necessary so that we can place a first-party cookie signaling that you have opted out on each browser and each device you use.

If you block cookies, we will be unable to comply with your Right to Opt Out of Sale or Sharing request for device data that we automatically collect and disclose to third parties online using cookies, pixels, and other tracking technologies. If you clear the cookies in your browser, you will need to follow Step 2 above again. To the extent required by California law, we will honor “Do Not Sell or Share” opt-out preference signals sent in a format commonly-used and recognized by businesses at the browser level, such as an HTTP header field or JavaScript object.

Verification: To process California data protection requests, we will need to obtain information to locate you in our records or verify your identity, depending on the nature of the request. In most cases, we will request information about you, which may include your name, email address, or other information. If you submit a Right to Know - Specific Pieces Report we may also request a signed declaration, under penalty of perjury, that you are who you say you are. We may request alternative information under certain circumstances and/or use third parties to help verify your identity.

Authorized Agents: Authorized agents may exercise California data protection rights on behalf of California individuals, but we reserve the right to verify the individual’s identity directly as described above. Authorized agents must contact us by submitting a request by emailing us at privacy@drata.com and indicate that they are submitting the request as an agent. We may require the agent to demonstrate authority to act on your behalf by providing signed permission from you. We may also require you to verify your own identity directly with us or to directly confirm with us that you provided the authorized agent permission to submit the request.

Timing: We will process Right to Opt Out of Sale or Sharing requests within fifteen (15) business days from the date we received the request. We will respond to Requests to Delete and Requests to Know within forty-five (45) days unless we need more time, in which case we will notify you, and it may take up to ninety (90) days to respond to your request.

10. Supplemental Information for the EEA, Switzerland, and the U.K.

The following terms supplement the Notice with respect to our processing of EEA (i.e., European Union Member States, Iceland, Liechtenstein, and Norway), Swiss, and U.K. personal data. In the event of any conflict or inconsistency between the other parts of the Notice and the terms of this Section 10, this Section 10 shall govern and prevail with regard to the processing of EEA, Swiss, and U.K. Personal Data, to the extent applicable.

Data Controller: The Drata entity with which you have a primary relationship (such as the entity that concluded the Services contract with you; the entity that has provided you with marketing materials and promotional communications; or the primary entity in the region where you access our Site) is the controller within the scope of this Notice. This will be Drata Inc., unless we specifically inform you otherwise.

a. Legal Basis for Processing:

Please see Section 3 for the legal basis on which we rely for the collection, processing, and use of personal data.

b. Your Data Protection Rights:

Under applicable data protection laws, you may exercise certain rights regarding your personal data:

- **Right to Access.** You have the right to obtain confirmation from us whether we are processing your personal data and related information, as well as the right to obtain a copy of your personal data undergoing processing.
- **Right to Data Portability.** You may receive your personal data, that you have provided to us, in a structured, commonly-used, and machine-readable format, and you may have the right to transmit it to other data controllers without hindrance. This right only exists if the processing is based on your consent or a contract, and the processing is carried out by automated means.
- **Right to Rectification.** You have the right to request the rectification of inaccurate personal data and to have incomplete data completed.
- **Right to Objection.** You have the right to object to the processing of your personal data in certain cases.
- **Right to Restrict Processing.** You may request that we restrict the processing of your personal data in certain cases.
- **Right to Erasure.** You may request that we erase your personal data in certain cases.
- **Right to Lodge a Complaint.** You have the right to lodge a complaint with a supervisory authority. In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, we commit to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO) and the Gibraltar Regulatory Authority (GRA), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.
- **Right to Refuse or Withdraw Consent.** In case we ask for your consent to process your personal data, you are free to refuse to give it. If you have given

your consent, you may withdraw it at any time without any adverse consequences. The lawfulness of any processing of your personal data that occurred prior to the withdrawal of your consent will not be affected.

- **Right to Not Be Subject to Automated Decision-making.** The types of automated decision-making referred to in Article 22(1) and (4) EU/UK General Data Protection Regulation (“GDPR”) do not take place in connection with your personal data. Should this change, we will inform you about why and how any such decision was made, the significance of it, and the possible consequences of it. You will also have the right to human intervention, to express your point of view, and to contest the decision.

You may exercise these rights by contacting us using the details provided in Section 12 or by visiting [here](#) to submit your request. Please note that we may refuse to act on requests to exercise data protection rights in certain cases, such as where providing access might infringe someone else’s privacy rights or impact our legal obligations.

c. International Transfers of Personal Data:

Due to the global nature of our operations, some of the recipients mentioned in Section 2 of the Notice may be located in countries outside the EEA, Switzerland, or the U.K., which do not provide an adequate level of data protection as defined by data protection laws in the EEA, Switzerland, and the U.K. Transfers to third parties located in such third countries take place using a valid data transfer mechanism, such as the EU Standard Contractual Clauses and/or the U.K. Addendum to such clauses, approved codes of conduct and certifications mechanisms, on the basis of permissible statutory derogations, or any other valid data transfer mechanism issued or approved by the EEA, Swiss, or U.K. authorities. Certain third countries have been officially recognized by the EEA, Swiss, and U.K. authorities as providing an adequate level of protection and no further safeguards are necessary. Please reach out to us using the contact information in Section 12, if you wish to receive further information about how we transfer personal data or, where available, a copy of the relevant data transfer mechanism.

Drata complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Drata 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. Drata has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard

to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this 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 Federal Trade Commission has jurisdiction over Drata's compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

Data Protection Officer: The contact details for our data protection officer are as follows: Drata Inc., Attn: Privacy Team, 4660 La Jolla Village Drive, Suite 100, San Diego, CA 92122, United States, privacy@drata.com.

11. Supplemental Information for Other Regions

- **Australia:** Personal data collected, stored, used, and/or processed by Drata, as described in this Notice, is collected, stored, used, and/or processed in accordance with the Australian Privacy Act 1988 (Commonwealth) and the Australia Privacy Principles. If you are dissatisfied with our handling of a complaint or do not agree with the resolution proposed by us, you may make a complaint to the Office of the Australian Information Commissioner ("OAIC") by contacting the OAIC using the methods listed on [their website](#). Alternatively, you may request that we pass on the details of your complaint to the OAIC directly.
- **Canada:** Personal data, as defined in the Personal Information Protection and Electronic Documents Act ("PIPEDA") will be collected, stored, used, and/or processed by Drata in accordance with the Drata's obligations under PIPEDA.
- **Nevada:** We do not presently sell personal data as defined under Nevada law. If you are a Nevada resident, you may nevertheless email us using the information above to exercise your right to opt-out of sale under Nevada Revised Statutes §603A et seq.
- **New Zealand:** Personal data collected, stored, used, and/or processed by Drata, as described in this Notice, is collected, stored, used, and/or processed in accordance with New Zealand's Privacy Act 2020 and its 13 Information Privacy Principles ("NZ IPPs").
- **Singapore:** Personal data collected, stored, used and/or processed by Drata, as described in this Notice, is collected, stored, used, and/or processed in accordance with Drata's obligations under the Personal Data Protection Act 2012 ("PDPA").
- **United Kingdom:** Personal data collected, stored, used, and/or processed by Drata, as described in this Privacy Notice, is collected, stored, used, and/or

processed in accordance with Drata's obligations under the UK Data Protection Act 2018, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, as amended, superseded or replaced ("U.K. GDPR").

12. Contact Information

If you have questions or complaints regarding this Notice or about the Drata's privacy practices, please contact us by email at privacy@drata.com, or at:

Drata Inc.

Attn: Privacy Team

4660 La Jolla Village Drive, Suite 100

San Diego, CA 92122, United States

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, we commit to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. to JAMS, a DPF an alternative dispute resolution provider based in the United States.

13. English Version Controls

Non-English translations of this notice are provided for convenience only. In the event of any ambiguity or conflict between translations, the English version is authoritative and controls.