Privacy Policy

Last Updated: 31 December 2019

When you use and interact with our websites or services, communicate with or otherwise contact us, or visit our offices, or attend our events, we may collect, use, share and process information relating to you ("Personal Data"). This Privacy Policy governs our privacy policies and procedures and your related rights with respect to the website: www.datrium.com (“Website”), our products and services (collectively, “Services”), and use of your information in connection with our customer interactions, vendor, and partner relationships. If you are entering into this agreement on behalf of a company or other legal entity, you represent that you have the authority to bind such entity, its affiliates, and all users who access our Services through your account, to these terms and conditions, in which case the terms "you" or "your" shall refer to such entity, its affiliates and users associated with it. If you disagree with the practices described in this Privacy Policy, then you should (a) take necessary steps to remove cookies from your computer after leaving our Website, and (b) not access or use the Services, Website or any other aspect of our business.

This policy does not cover third-party websites, products, or services (“Third-Party Services”) even if they link to our Services—you should consider those privacy policies carefully. In addition, a separate agreement governs delivery, access, and use of the Services (the “Customer Agreement”), including the processing of any messages, files or other content submitted through Service accounts (collectively, “Customer Data”). The organization (e.g., your employer or another entity or person) that entered into the Customer Agreement (“Customer”) controls their instance of the Services and any associated Customer Data.

1. Information We Collect And Receive

We may collect and receive Customer Data and other information and data (“Other Information”) in a variety of ways:

Customer Data. Customers or individuals granted access to the Services by a Customer ("Authorized Users") routinely submit Customer Data when using the Services.

Other Information. We also collect, generate, and/or receive Other Information, as set forth below:

i. *User Account Information*. To create or update an account, you or our Customer (e.g., your employer) supply us with an email address, phone number, password, domain, and/or similar account details. In addition, Customers that purchase a paid version of the Services provide us(or our payment processors) with billing details such as credit card information, banking information, and/or a billing address.

ii. *Usage Information*.

- *Services Metadata*. When an Authorized User interacts with the Services, metadata is generated that provides additional context about the way Authorized Users work. For example, we log the features, content, and links you interact with, the types of files shared, service names, cluster names, and user interface elements and what Third-Party Services are used (if any).
- *Log data*. As with most websites and technology services delivered over the Internet, our servers automatically collect information when you access or use our Website or Services and record it in log files. This log data may include the Internet Protocol (IP) address, the address of the web page visited before using the Website or Services, browser type and settings, the date and time the Services were used, information about browser configuration and plugins, language preferences, and cookie data.
- *Device information*. We collect information about devices accessing the Services, including type of device, what operating system is used, device settings, application IDs, unique device identifiers, and crash data. Whether we collect some or all of this Other Information often depends on the type of device used and its settings.
- *Location information*. We receive information from you, our Customer and other third parties that help us approximate your location. We may, for example, use a business address submitted by your employer, or an IP address received from your browser or device to determine approximate location. We may also collect location information from devices in accordance with the consent process provided by your device.

iii. Cookie Information. We use cookies and similar technologies in our Website and Services that help us collect Other Information. The Website and Services may also include cookies and similar tracking technologies of third parties, which may collect Other Information about you via the Website and Services and across other websites and online services. For more details about how we use these technologies, please see our Cookie Policy.

iv. Third-Party Services. Typically, Third-Party Services are software that integrates with our Services, and a Customer can permit its Authorized Users to enable and disable these integrations. Once enabled, the provider of a Third-Party Service may share certain information with us. Authorized Users should check the privacy settings and notices in these Third-Party Services to understand what data may be disclosed to us. When a Third-Party Service is enabled, we are authorized to connect and access Other Information made available to us in accordance with our agreement with the Third-Party Service Provider. We do not, however, receive or store passwords for any of these Third-Party Services when connecting them to the Services.

v. Third-Party Data. We may receive data about organizations, industries, Website visitors, marketing campaigns, and other matters related to our business from our partners or others that we use to make our own information better or more useful. This data may be combined with Other Information we collect and might include aggregate level data, such as which IP addresses correspond to zip codes or countries. Or it might be more specific: for example, how well an online marketing or email campaign performed.

vi. Additional Information Provided to Us. We receive Other Information when submitted to our Website or if you participate in a focus group, activity or event, apply for a job, request support, interact with our social media accounts, or otherwise communicate with us.

Generally, no one is under a statutory or contractual obligation to provide any Customer Data or Other Information (collectively, “Information”). However, certain Information is collected automatically and, if some Information, such as account setup details, is not provided, we may be unable to provide the Services.

2. How We Use Information

Customer Data will be used by us in accordance with Customer’s instructions, including any applicable terms in the Customer Agreement and Customer’s use of Services

functionality, and as required by applicable law. We are a processor of Customer Data, and Customer is the controller. Customer may, for example, use the Services to grant and remove access, assign roles and configure settings, access, modify, export, share and remove Customer Data.

We use Other Information in furtherance of our legitimate interests in operating our Services, Website, and business. We use Other Information:

i. To provide, update, maintain, and protect our Services, Websites, and business. This includes use of Other Information to support delivery of the Services under a Customer Agreement, prevent or address service errors, security or technical issues, analyze and monitor usage, trends, and other activities or at an Authorized User's request.

ii. As required by applicable law, legal process or regulation. In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

iii. To communicate with you by responding to your requests, comments, and questions. If you contact us, we may use your Other Information to respond.

iv. To develop and provide support, training and productivity tools, and additional features. We aim to make the Services as useful as possible. For example, we may improve search functionality by using Other Information to make Services suggestions based on historical use and predictive models, identify organizational trends and insights, to customize a Service experience or create new productivity features and products.

v. To send emails and other communications. We may send you service, technical, and other administrative emails, messages, and other types of communications. We may also contact you to inform you about changes in our Services, our Services offerings, and important Services-related notices, such as security and fraud notices. These communications are considered part of the Services, and you may not opt out of them. In addition, we sometimes send emails about new product features, promotional communications, or other news about us. These are marketing messages so you can control whether you receive them.

vi. For billing, account management, and other administrative matters. We may need to contact you for invoicing, account management, and similar reasons, and we use account data to administer accounts and keep track of billing and payments.

vii. To investigate and help prevent security issues and abuse.

If Information is aggregated or de-identified so it is no longer reasonably associated with an identified or identifiable natural person, we may use it for any business purpose. To the extent Information is associated with an identified or identifiable natural person and is protected as personal data under applicable data protection law, it is referred to in this Privacy Policy as "Personal Data."

3. Data Retention

We will retain Customer Data in accordance with a Customer's instructions, including any applicable terms in the Customer Agreement and Customer's use of Services, and as required by applicable law. Depending on the Service, Customer may be able to customize its retention settings and apply those customized settings in the use of the Services. We may retain Other Information pertaining to you for as long as necessary for the purposes described in this Privacy Policy. This may include keeping your Other Information after you have deactivated your account for the period of time needed for us to pursue our legitimate business interests, conduct audits, comply with (and demonstrate compliance with) legal obligations, resolve disputes and enforce our agreements.

4. How We Share And Disclose Information

This section describes how we may share and disclose Information. Customers determine their own policies and practices for the sharing and disclosure of Information, and we do not control how they or any other third parties choose to share or disclose Information.

i. Customer's Instructions. We will solely share and disclose Customer Data in accordance with a Customer's instructions, including any applicable terms in the Customer Agreement and Customer's use of Service functionality, and in compliance with applicable law and legal process.

ii. Collaborating with Others. The Services may provide different ways for Authorized Users to collaborate, such as through support and user channels available through a Third-Party Service provider.

iii. Customer Access. Administrators, Authorized Users, and other Customer representatives and personnel may be able to access, modify, or restrict access to Other Information.

iv. Third-Party Service Providers and Partners. We may engage third-party companies or individuals as service providers or business partners to process Other Information and support our business. These third parties may, for example, provide virtual computing and storage services. Additional information about the subprocessors we use to support the hosting and delivery of our Services is set forth at the url https://www.datrium.com/legal/Datrium-Sub-Processors-List.pdf.

v. Third-Party Services. Customer may enable or permit Authorized Users to enable Third-Party Services. When enabled, we may share Other Information with Third-Party Services. Third-Party Services are not owned or controlled by us, and third parties that have been granted access to Other Information may have their own policies and practices for its collection and use. Please check the privacy settings and notices in these Third-Party Services or contact the provider for any questions.

vi. With Business Affiliates or During a Change to our Business. If we engage in a merger, acquisition, bankruptcy, dissolution, reorganization, sale of some or all of our assets or stock, financing, public offering of securities, acquisition of all or a portion of our business, a similar transaction or proceeding, or steps in contemplation of such activities (e.g. due diligence), some or all Other Information may be shared or transferred, subject to standard confidentiality arrangements.

vii. Aggregated or De-identified Data. We may disclose or use aggregated or de-identified Other Information for any purpose. For example, we may share aggregated or de-identified Other Information with prospects or partners for business or research purposes, such as telling a prospective customer the average amount of time spent within our Services and typical customer usage.

viii. To Comply with Laws. If we receive a request for information, we may disclose Other Information if we reasonably believe disclosure is in accordance with or required by any applicable law, regulation, or legal process. Unless we are prohibited from doing so or there is a clear indication of illegal conduct or risk of harm, we will notify Customer of the request before disclosing any of Customer's Customer Data so that the Customer may seek legal remedies.

ix. To enforce our rights, prevent fraud, and for safety. To protect and defend the rights, property, or safety of us or third parties, including enforcing contracts or policies, or in connection with investigating and preventing fraud or security issues.

ix. With Consent. We may share Other Information with third parties when we have consent to do so.

5. Right to Access, View, or Remove Your Information

You have a right to access the Personal Data we hold about you. Whenever you use our Website or Services, we strive to make sure that your Personal Data is correct. If that information is incorrect, we give you the tools and methods to update it or delete it, unless that information is necessary for legal or business purposes. When updating your Personal Data, we may ask you to verify your identity before making changes. We may reject requests that are unreasonably repetitive, require disproportionate technical effort (for example, developing new systems or fundamentally changing our existing practice), risk the privacy of others, or would be extremely impractical (e.g. requests concerning information on our backup systems). Because we protect information from accidental or malicious destruction, after data is removed from our servers, it can take some time for that data to be purged.

If you no longer wish to receive marketing communications from us, please follow the unsubscribe instructions provided in our email communications. You may also opt out of receiving commercial email from us by sending your request to us by email at privacy@datrium.com. Please be aware that, even after you opt out of receiving commercial or marketing communications, you will continue to receive administrative messages from us regarding the Services.

To request removal of your Personal Data, contact us at privacy@datrium.com. If you are an Authorized User of our Service and need to correct, amend, or delete inaccurate data about you, please contact our Customer (e.g. your employer). We will comply with the requests of our Customers should they direct us to take action about the modification/removal of collected data.

6. Privacy of Minors

The Website is not directed to persons under 16. If a parent or guardian becomes aware that his or her child has provided us with Personal Data without their consent, he or she should contact us at privacy@datrium.com. We do not knowingly collect

Personal Data from children under 16. If we become aware that a child under 16 has provided us with Personal Data, we will delete such data from our files.

7. Specific Privacy Rights of United States Residents

California Resident Rights

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

Categories of Information We Collect and Share for a Business Purpose

We may collect Personal Information from you in a variety of different situations, including, but not limited to, on our Website, your mobile device, through email, your use of our Services, in physical locations, through the mail, and/or over the telephone. Datrium collects the following categories of Personal Information from its Consumers. In addition, during the past twelve months, we have shared these categories of personal information for a business purpose:

- Identifiers, such as your name, alias, Internet Protocol address, email address, and other similar identifiers.
- Personal Information categories listed in commercial and consumer records, including payment information. Some personal information included in this category may overlap with other categories.
- Internet or other electronic network activity information, such as session logs.
- Geolocation data, such as the physical location of your recorded activity.
- Electronic, visual, or similar information, such as photos or user information submitted by you during account registration or collected during attendance of conferences or webinars.
- Inferences drawn from any of the above information to create a profile reflecting your preferences, characteristics, behavior, abilities, and interests.

According to California law, personal information does not include:

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

How We Share and Disclose Information

See the main privacy policy for business purposes to learn how we share and disclose your information, including personal information. Datrium does not sell Consumer Personal Information, nor has sold Consumer Personal Information in the preceding twelve months.

How We Obtain this Information

Datrium obtains the categories of Personal Information listed above from the following categories of sources:

- Directly from you. For example, from forms you complete or products and services you purchase.
- Indirectly from you. For example, from observing your actions on our Website or from information your computer or mobile device transmits when interacting with our Website or mobile applications, among other things.

Your Consumer Rights and Choices

The CCPA provides Consumers 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 Datrium 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 (see Exercising Access, Data Portability, and Deletion Rights), 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 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.

Deletion Request Rights

You have the right to request that we delete any of your Personal Information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request (see Exercising Access, Data Portability, and Deletion Rights), we will delete (and direct our service providers to delete) your Personal Information from our records, unless an exception applies. In accordance with

the CCPA, we may deny your deletion request under certain circumstances and will inform you of the basis for the denial, which may include, but is not limited to, if retaining the information is necessary for us or our service provider(s) to:

- Complete the transaction for which we collected the Personal Information, provide the Service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
- Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
- Comply with a legal obligation.
- Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

Exercising Access, Data Portability, and Deletion Rights

To exercise the Access, Data Portability, and Deletion Rights described above, please submit a verifiable consumer request to us:

Email us at **privacy@datrium.com**

Only you, or your agent, 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 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 have authority as an authorized representative.
- Describe your request with sufficient detail that allows us to understand, evaluate, and respond to it properly.

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.

Response Timing and Format

We endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to an additional 45 days), we will inform you of the reason and extension period in writing.

If you have an account with us, we will deliver our written response to that account. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option.

Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

Other California Privacy Rights

Users of our Website who are California residents may request certain information regarding our disclosure of Personal Information to third parties for their direct marketing purposes. We, however, do not disclose your Personal Information to third parties for their direct marketing purposes.

How to Contact Us

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

Nevada Resident Rights

We do not sell your covered information, as defined by Section 1.6 of Chapter 603A of the Nevada Revised Statutes. If you reside in Nevada, you have the right to submit a request to our designated request email address, privacy@datrium.com, regarding the sale of covered information.

8. Updates to This Privacy Policy

This Privacy Policy may be updated from time to time; each version will apply to Information collected while it was in place. We will notify you of any modifications to our Privacy Policy by posting the new Privacy Policy and indicating the date of the latest revision. You are advised to consult this Privacy Policy regularly for any changes.

In the event that the modifications materially alter your rights or obligations hereunder, we will make reasonable efforts to notify you of the change. For example, we may send a message to your email address or generate a pop-up or similar notification when you access the Service for the first time after such material changes are made. Your continued use of the Service after the revised Privacy Policy has become effective indicates that you have read, understood, and agreed to the current version of this Privacy Policy.

9. How to Contact Us

If you have any questions or comments regarding this Privacy Policy, or if you would like to exercise your rights to your Personal Data, you may contact us by emailing us at privacy@datrium.com or by writing to us at:

Datrium, Inc.
385 Moffett Park Dr.,
Sunnyvale, CA 94089
Attention: Legal Department

10. International Data Transfers, Privacy Shield, And Contractual Terms

We may transfer your Personal Data to countries other than the one in which you live. We deploy the following safeguards if we transfer Personal Data originating from the European Union, United Kingdom ("UK"), or Switzerland to other countries not deemed adequate under applicable data protection law:

i. E.U.-U.S. Privacy Shield and Swiss-U.S. Privacy Shield. To comply with European Union and Swiss data protection laws, Datrium, Inc. ("Datrium") self-certified under the E.U.-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield frameworks. We ensure that the Privacy Shield Principles apply to all information about you that is subject to this Privacy Policy and is received from the European Union and the UK, and/or Switzerland. To learn more about the Privacy Shield Program, please see http://www.privacyshield.gov/welcome.

ii. European Union Model Clauses. Datrium may also enter into the European Union Model Clauses, also known as Standard Contractual Clauses, to meet the adequacy and security requirements for our Customers that operate in the European Union, and other international transfers of Customer Data.

Identifying The Data Controller And Processor

Data protection law in certain jurisdictions differentiates between the "controller" and "processor" of information. In general, Customer is the controller of Customer Data. In general, Datrium is the processor of Customer Data and the controller of Other Information.

Accountability for Onward Transfer

Under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, we are responsible for the processing of information about you we receive from the EU and the UK, and/or Switzerland and onward transfers to a third party acting as an agent on our behalf. We comply with the Privacy Shield Principles for such onward transfers and remain liable in accordance with the Privacy Shield Principles if third-party agents that we engage to process such information about you on our behalf do so in a manner inconsistent with the Privacy Shield Principles, unless we prove that we are not responsible for the event giving rise to the damage.

Your Rights

Individuals located in certain countries, including the European Union, UK, and Switzerland, have certain statutory rights in relation to their Information, including Personal Data. Subject to any exemptions provided by law, you may have the right to request access to Information, as well as to seek to update, receive a copy, delete, or correct this Information. You can do this using the settings and tools provided in the marketing communications, your Services account, or by contacting us at privacy@datrium.com.

For the avoidance of doubt, if you wish to exercise your choice to be excluded from the onward transfer of information to third parties, or if you feel like your Personal Data will be used for purposes other than what it was intended for, or if you wish to otherwise limit the use and disclosure of your Personal Data in accordance with the Privacy Shield Principles, please contact us at privacy@datrium.com.

Questions, Complaints and Dispute Resolution

If you are a data subject and have any questions or concerns, please direct communications to privacy@datrium.com. Inquiries from the Department of Commerce will have the same channel.

Alternatively, written communications can be sent to:

Datrium, Inc.
385 Moffett Park Dr.,
Sunnyvale, CA 94089
Attention: Legal Department

In the event that your concern is not resolved, you may contact JAMS, a U.S. based independent third-party dispute resolution body that will assist you free of charge. A binding arbitration option may also be available to you in order to resolve complaints not resolved by other means. You can file a claim on their website. For those in the EU, UK or Switzerland, you may invoke binding arbitration when other dispute resolution procedures have been exhausted as per Annex I of Privacy Shield. Datrium is subject to the investigatory and enforcement powers of the US Federal Trade Commission ("FTC").