Omnigo Software - Privacy Policy

Effective Date: March 2024

By using, browsing, and/or accessing our website, you agree to the terms of this Privacy Policy. Your visit to the website and any dispute over privacy is subject to our Terms of Use and the laws of the state of Texas. Use of this website is strictly voluntary. If you disagree with this Privacy Policy, you are advised not to access our website.

This Privacy Policy describes the types of personal information we obtain, how we may use that personal information, with whom we may share it, and how you may exercise your rights under United States and European laws (collectively referred to as "Data Protection Laws" herein) regarding our processing of that information. The Privacy Policy also describes the measures we take to safeguard the personal information we obtain and how you can contact us about our privacy practices.

Sources of Personal Information

- When you browse the Omnigo website.
- When you fill out any forms (e.g, sales forms for products or a support ticket request) on the Omnigo website.
- When you create an online customer account.
- When you interact with an online chat function on the Omnigo website; and
- Cookies and other technologies.

Cookie Policy

- Background: Omnigo uses cookies, web beacons (including pixels and tags), and similar technologies on our website which may read or write information on your device to collect certain information about you by automated means. A "cookie" is a text file that websites send to a visitor's computer or other Internet-connected device to uniquely identify the visitor's browser or to store information or settings in the browser. A "web beacon," also known as an Internet tag, pixel tag, or transparent GIF, links web pages to web servers and their cookies and may be used to transmit information collected through cookies back to a web server.

- Purpose: We use these automated technologies to collect information about your equipment, browsing actions, and usage patterns. The personal information we obtain in this manner includes IP address and other identifiers associated with your devices, including Apple Advertising Identifier or Android Advertising ID, device characteristics (such as operating system), language preferences, referring/exit pages, navigation paths, access times, browser preferences and characteristics, installed plugins, local time zones, local storage preferences, clickstream data, and other information about your online activities.

- Your browser may tell you how to be notified when you receive certain types of cookies or how to restrict or disable certain types of cookies. Please note, however, that without cookies, you may be unable to use all our website's features. For mobile devices, you can manage how your device and browser share specific device data by adjusting the privacy and security settings on your mobile device.

- The length of time a cookie will stay on your browsing device depends on whether it is a "persistent" or "session" cookies. Session cookies are automatically deleted when you close your browser. Persistent cookies remain on your computer or other Internet-connected device after you end your browsing session unless you choose to delete them.

- Specific Cookies We Use: Cookies used by Omnigo include:
    (1) Essential cookies.
    (2) Functional cookies.

(3) Analytics/Performance cookies; and

(4) Targeting/Advertising cookies.

(1) Essential Cookies: These cookies are operational and necessary for us to provide our products and services on our website and typically may not be disabled. You may set your browser to block or alert you about these cookies, but parts of our website may not function properly. Essential cookies authenticate you to our website, identify you after you log in, and increase the security of our products.

(2) Functional Cookies: These cookies enable our website to provide enhanced functionality and personalization. We or third-party providers whose services we add to our website may set functional cookies. Functional cookies remember your language preference and geolocation data when you visit our website and provide enhanced, personal features.

(3) Analytics/Performance Cookies: These cookies collect information on how users navigate and use our website, such as the pages they view, how long they stay on a page, whether the page is displayed correctly or whether errors occur. Analytics cookies improve our website's performance.

a. Google Analytics. We use cookies from third-party analytics providers, including Google Analytics, for aggregated, anonymized website traffic analysis. To track your session usage, Google drops a cookie (_ga) with a randomly generated ClientID in your browser. This ID is anonymized and contains no identifiable information like email, phone number, name, etc. We also send Google your IP Address. We use GA to track aggregated website behavior, such as what pages you looked at, for how long, and so on. This information is essential for improving the user experience and determining site effectiveness.

(4) Targeting/Advertising Cookies: These cookies deliver advertisements relevant to your interests and may be set by either of us (first-party cookies) or our third-party partners, including social media cookies. Advertising cookies limit the number of times you see an advertisement and help measure the effectiveness of an advertising campaign. Third-party cookies recognize your browser when you visit our website and may use information from your visit to place advertisements for our products on other websites you visit. We do not control the types of information collected and stored by these third-party cookies. You should check the third-party's website for more information on how they use cookies.

- Do Not Track Signals: Certain web browsers allow you to instruct your browser to send Do Not Track ("DNT") signals to websites you visit, informing those sites that you do not want your online activities to be tracked. Our website is not designed to respond to "do not track" signals received from web browsers. However, with most web browsers, you can take steps to limit tracking by erasing cookies from your device and by setting your browser to block all cookies or warn you before a cookie is stored.

Personal Information We Collect

- Contact information (such as name email address, telephone number, postal or other physical address) for you or for others (e.g., principals in your business or billing contacts).
- Information used to create your online account (such as username and password).
- Billing and financial information (such as name, billing address, payment card details, bank account information, and purchase history); and
- IP address and geolocation data (such as data derived from your IP address, country, and zip code).

How We Use Personal Information Collected

- Provide and administer Omnigo products and services (including websites and apps you have registered).
- Process and fulfill orders related to Omnigo products and services and keep you informed about the status of your order.
- Help you complete a transaction or order and provide customer support.
- Bill you for products and services purchased.
- Operate, evaluate, and improve our business (such as by administering, developing, enhancing, and improving Omnigo products and services, managing our communications and customer relationships, and performing accounting, auditing, billing, reconciliation, and collection activities).
- Perform data analytics (such as research, trend analysis, financial analysis, and customer segmentation).
- Communicate with you about your account and orders (including sending emails about your registration, account status, order confirmations, renewal or expiration notices, and other important information).
- Conduct advertising, marketing, and sales activities (including sending you promotional materials, generating leads, pursuing marketing prospects, performing market research, determining and managing the effectiveness of our advertising and marketing campaigns, and managing the Omnigo brand).
- Communicate with you about and administer your participation in events, programs, promotions, and surveys; and
- Comply with and enforce relevant industry standards, contractual obligations, and Omnigo policies.

Our Purpose and Legal Basis for Collection

- Performance of a contract with you or a relevant party.
- Our legitimate business interests.

- Compliance with a legal obligation, a court order, or to exercise or defend legal claims; or
- Your consent to the processing, which you can revoke at any time; and
- We may combine personal information collected from you with other sources to help us improve the accuracy of our marketing and communications as well as to help expand or tailor our interactions with you. This includes combining personal information we obtain through our website with other channels. We may anonymize or aggregate personal information and use it for the purposes identified in this section and other purposes to the extent permitted by applicable law.

When We Share Personal Information with Third Parties

- If sharing your personal information is necessary to provide a product, service, or information you have requested.
- To inform you about the latest product announcements, software updates, special offers, or other information we think you would like to hear from our business partners.
- With service providers, we have engaged to perform services on our behalf (such as payment processing, order fulfillment, customer support, customer relations management, and data analytics). These service providers are contractually required to safeguard the information provided to them and are restricted from using or disclosing such information except as necessary to perform services on our behalf or to comply with legal requirements.
- If we are required to share your personal information under applicable law, regulation, or legal process (such as a court order or subpoena) or with law enforcement authorities or other government officials to comply with a legitimate legal request (e.g., an investigation of suspected or actual fraud, illegal activity or in response to a security issue).
- If we believe disclosure is necessary to prevent physical harm or financial loss to Omnigo or the public as required or permitted by law or to establish, exercise, or defend our legal rights; and
- In the event of a potential or actual sale or transfer of all or a portion of our business or assets (including in the event of a merger, acquisition, joint venture, reorganization, divestiture, dissolution, or liquidation) or other business transaction.
- Omnigo does not sell personal information as the term sell is commonly understood. Under certain Data Protection Laws, a “sale” is defined to include disclosures of personal information to a third party for monetary or valuable consideration. When you use the Omnigo website, our third-party authorized partners, such as data analytics providers and social networks, may collect cookies and similar technology and use this data (such as your Internet or other similar network activity) for their own purposes, such as improving their own services. This activity may qualify as a “sale” under applicable Data Protection Laws. You can allow or prevent such uses by clicking on the Cookie Preferences link at the bottom of the page.

Social Media and Other Third-Party Links

Our websites may, from time to time, contain links to and from (1) social media platforms and (2) third-party websites. When you use social media links, we may collect additional information from or about you, such as your screen names, profile pictures, contact information, contact lists, and the profile pictures of your contacts. Please be advised that social media platforms and third-party websites may also collect information from you. We do not have control over or responsibility for the collection, use, and sharing practices of social media platforms and third-party websites. We recommend you carefully review their privacy policies before you provide personal information on a social media platform or third-party website.

As applicable: We use third-party partners to supply and support our online chat or chatbot function, which we use to handle customer inquiries in real time. If you use our online chat function, we may record and collect the contents of your online chat session. Unless otherwise stated, the information will be retained for 5 years and will not be shared other than to the extent required by law. The third-party partner providing the chatbot may collect information from your session to track the use of the services.

Nothing we communicate in the online chat will be considered a legal agreement, representation, or warranty regarding our services, decisions, or response times. You may not use online chat to send any abusive, defamatory, dishonest, or obscene message, and doing so may result in the termination of your online chat session. You may request a transcript of the recording of your online chat session by contacting us at compliance@omnigo.com.

How We Secure Personal Information

While Omnigo strives to protect your information, it cannot ensure or warrant the security of any information you transmit to or from our website by e-mail or otherwise. You provide such information at your own risk. Omnigo cannot guarantee against any loss, misuse, unauthorized disclosure, alteration, or destruction of data or personal information.

You acknowledge that: (1) there are security and privacy limitations in computer systems and on the Internet that are beyond Omnigo's control; (2) the security, integrity, and privacy of any and all information and data exchanged between you and Omnigo through our website cannot be guaranteed; and (3) any such information and data may be viewed or tampered with by a third party while such information or data is being used, transmitted, processed, or stored.

Notice to California Residents

The California Privacy Rights Act ("CPRA") grants residents of California certain rights with respect to their personal information as described in this section.

- Right to Transparency: When we collect personal information, you have the right to receive notice of the categories of personal information we collect and the purposes for which those categories of personal information will be used.

- Right to Access/Right to Know: You have the right to request access to the personal information we collected about you and information regarding the source of that personal information, the purposes for which we collect it, and the third parties, including service providers with whom we share it.

- Right to Deletion: You have the right to request that we erase data we have collected from you. Please note that we may have a reason to deny your deletion request or delete data in a more limited way than you anticipated (e.g., because of a legal obligation to retain it or to provide a good or service that you request)

- Right to Request Correction: You have a right to request correction of inaccurate personal information.

- Right to Opt-Out of Sale and Share: You have the right to request that we stop "selling" your personal information as that that term is defined in the California Privacy Rights Act. A "sale" of personal information is defined broadly: "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, an individual's personal information by the business to another business or a third party for monetary or other valuable consideration." "Sharing" of personal information is defined as: "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, an individual's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged."

- Right to Non-Discrimination: You have the right to not be discriminated against for exercising any of your privacy rights. The right is violated if you are denied any of our goods or services, charged different prices for goods or services, provided different levels of quality for goods or services, or if we suggest that you will be charged different prices for goods or services or provided different levels of quality for goods or services. Please note that exercising these rights may limit our ability to process personal information (e.g., in the case of deletion or a do-not-sell request), and we may no longer be able to provide you with our products and services or otherwise engage with you in the same manner.

- Right under Shine the Light Law: Subject to certain limitations, you may ask us to provide a list of the types of personal information that we disclose to third parties for their direct marketing purposes, and the identities and physical address of such third parties.

- Categories of Personal Information We Collect: We collect the categories of information described in the table below.

CATEGORY OF PERSONAL INFORMATION (AS SPECIFIED IN THE CPRA)	PERSONAL INFORMATION COLLECTED
Identifiers	Data such as your name, postal address, unique personal identifier, online identifier, IP address, email address, account name, and other similar identifiers.
Categories of Personal Information Described in Cal. Civ. Code § 1798.80(e) (the California Customer Records Statute)	Data such as your name, signature, address, phone number, bank account number, credit card number, debit card number, or any other financial information.
Characteristics of Protected Classifications	Data such as demographic information.
Commercial Information	Data such as records of products or services purchased, obtained, or considered and other purchasing or consuming histories or tendencies.
Internet or Other Electronic Network Activity Information	This includes data such as your browsing and search history and information regarding your interaction with websites, applications, or advertisements.
Geolocation Data	Data such as the location of your device (e.g., based on a browser or device's IP address or Bluetooth technology, if your device settings allow for this).
Audio, Electronic, Visual, Thermal, Olfactory, or Similar Information	Data such as your image and video footage captured by call and video recordings.

- Categories of Personal Information We Disclose: We may disclose any of the categories of information listed above and use them for the purposes listed below.

BUSINESS PURPOSES (AS SPECIFIED IN THE CCPA)	CATEGORIES OF PERSONAL INFORMATION

Performing services, including maintaining or servicing accounts, providing customer service, processing, or fulfilling orders and transactions and verifying customer information, processing payments, providing advertising or marketing services, providing analytics services or providing similar services.	• Identifiers • Categories of Personal Information Described in Cal. Civ. Code § 1798.80(e) • Characteristics of Protected Classifications • Commercial Information • Internet or Other Electronic Network Activity Information • Geolocation Data • Audio, Electronic, Visual, Thermal, Olfactory, or Similar Information
Short-term, transient use, including, but not limited to, the contextual customization of ads shown as part of the same interaction.	• Identifiers • Commercial Information • Internet or Other Electronic Network Activity Information • Geolocation Data
Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.	• Identifiers • Categories of Personal Information Described in Cal. Civ. Code § 1798.80(e) • Characteristics of Protected Classifications • Commercial Information • Internet or Other Electronic Network Activity Information • Audio, Electronic, Visual, Thermal, Olfactory, or Similar Information
Debugging to identify and repair errors that impair existing intended functionality.	• Identifiers • Commercial Information • Internet or Other Electronic Network Activity Information
Undertaking internal research for technological development and demonstration.	• Identifiers • Characteristics of Protected Classifications • Commercial Information

	• Internet or Other Electronic Network Activity Information
Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by us and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by us.	• Identifiers • Categories of Personal Information Described in Cal. Civ. Code § 1798.80(e) • Characteristics of Protected Classifications • Commercial Information • Internet or Other Electronic Network Activity Information • Geolocation Data • Audio, Electronic, Visual, Thermal, Olfactory, or Similar Information

- Categories of personal information we "sell": We may "sell" any of the categories of personal information listed above to third parties.

- How to Exercise Your Privacy Rights:

    - To exercise your CPRA privacy rights, please email us at compliance@omnigo.com with the subject line "*CPRA Request*."

    - To exercise your California, Shine the Light Law privacy rights, please email us at compliance@omnigo.com with the subject line "*California Shine the Light Request*."

Notice to Colorado, Connecticut, Utah, and Virginia Residents

The disclosures in this section apply solely to individual residents of the States of Colorado, Connecticut, Utah, and the Commonwealth of Virginia. Privacy laws in these states give residents certain rights with respect to their personal information when they take effect over the course of 2023. These rights include:

- Right to Access Information: You have the right to confirm if Omnigo is processing your personal information and to access your personal information.

- Right to Request Deletion: You have the right to request that we delete personal information provided by or obtained about you.

- Right to Correct: You have the right to correct inaccuracies in your personal information.

- Right to Portability: You have the right to obtain a copy of your personal information in a format that is (i) portable to a technically reasonable extent; (ii) readily usable to a practical extent; (iii) enables you to transmit the personal information to another entity reasonably easily if the processing is carried out by automated means.

- Right to Opt-Out of Targeted Advertising: You may ask us not to use or disclose your personal information for the purposes of targeting advertising to you.

- Right to Opt-Out of Information Sales: You may ask us not to sell your personal information to third parties.

- Right to Non-Discrimination: You have the right to not be discriminated against for exercising any of your privacy rights. The right is violated if you are denied any of our goods or services, charged different prices for goods or services, provided different levels of quality for goods or services, or if we suggest that you will be charged different prices for goods or services or provided different levels of quality for goods or services. Please note that exercising these rights may limit our ability to process personal information (e.g., in the case of deletion or a do-not-sell request), and we may no longer be able to provide you with our products and services or otherwise engage with you in the same manner.

- How to Exercise Your Privacy Rights: To submit a request to exercise your privacy rights, please email us at compliance@omnigo.com with the subject line "*Privacy Rights Request*" and let us know in which state you live.

Notice to European Residents

European Data Protection Laws, including the European Union General Data Protection Regulation ("GDPR"), grant certain rights regarding your personal information. For purposes of these laws, including if Omnigo is the "controller" of your personal information. A "controller" is defined as an organization that processes personal data for its own purpose. A "processor" is defined as an organization that processes personal data on behalf of other organizations. We process your personal information only as permitted by law and in accordance with the table below.

PROCESSING PURPOSES	LEGAL BASIS (AS SPECIFIED IN THE GDPR)
Site Operation and Services Delivery	Processing is necessary to fulfil the contract governing the provision of our services or to take steps that you request prior to signing up for the Services. If we have not entered a contract with you, we process your personal information based on our legitimate interest in providing the information and/or services you access and request.
Research and Development. Marketing and Advertising. Customer Experience	These activities represent legitimate interests. We do not use your personal information for these activities where our interests are overridden by any impact on you (unless we have your consent or are otherwise required or permitted to by law).
Compliance with Applicable Laws	Processing is necessary to comply with our legal obligations.

If you are a resident of Europe, you may request that we take any of the following actions with respect to your personal information:

- Right to Access: You have the right to request access to the personal information we collected about you and information regarding the source of that personal information, the purposes for which we collect it, and the third parties, including service providers with whom we share it.

- Right to Request Correction: You have a right to request correction of inaccurate personal information.

- Right to Restrict: You have a right to restrict the processing of your personal information.

- Right to Withdraw: You have the right to withdraw your consent to the processing and use of your personal information entirely or partially at any time with future application.

- Right to Portability: You have the right to obtain a copy of your personal information in a format that is (i) portable to a technically reasonable extent, (ii) readily usable to a practical extent, (iii) enables you to transmit the personal information to another entity reasonably quickly if the processing is carried out by automated means.

- Right to Complain: You have the right to complain to the responsible supervisory authority if you believe that the processing of your personal information violates European Data Protection Laws. Please review "How to Submit a Complaint" below.

- How to Exercise Your Privacy Rights: To exercise your privacy rights under European Data Protection Laws, please email us at compliance@omnigo.com with the subject line "*CPRA Request*." You may be subject to a reasonable fee to meet our costs in providing details of personal information we hold about you.

- Automated Decision-Making and Profiling: For purposes of this Privacy Policy, automated decisions are defined as decisions about individuals that are solely based on the automated processing of personal information and that produce legal effects for the individual involved. This means processing using, for example, software code or an algorithm that does not require human intervention. We do not use automated decision-making. Omnigo may use profiling to capture data analytics from aggregated, anonymized website traffic analysis.

- How to Submit a Complaint. You have the right to submit a complaint about how we process your personal information or our response to your requests regarding your personal information. To lodge a complaint, you may contact us at compliance@omnigo.com or submit a complaint to the European data protection regulator in your jurisdiction. In the European Economic Area, you can find your data protection regulator here. In the United Kingdom, you can find your data protection regulator here.

Retention of Personal Information

To the extent permitted by applicable law, Omnigo typically retains personal information for as long as it is needed: (1) for the purposes for which we obtained it, in accordance with the terms of this Privacy Policy, which means that we will keep your personal information for the duration of our relationship or as long as you keep your account open with us; or (2) to comply with applicable laws, resolve disputes and enforce our agreements.

The CPRA requires us to disclose the criteria used to determine how long we retain personal information. Our records contain several categories of personal information combined, and therefore, we consider, on a case-by-case basis, a number of factors to assess how long personal information is retained. These factors include the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of your personal information, the purposes for which we process your personal information, whether we may achieve those purposes through other means, and applicable laws.

We will delete or anonymize your personal information that is no longer required. If deletion is impossible (e.g., when your personal information is stored in our backup archives), we will secure and isolate your personal information from further processing until deletion is possible.

Verification Process

Before responding to a request for personal information under applicable Data Protection Laws, Omnigo must verify the request. Verification is essential to protect your personal information and to help confirm that we are responding to a valid request and providing the response to the correct individual. To verify the request, we initially ask for at least two (2) or three (3) identifiers, such as name, email address, and location. If we have a need to request additional identifiers to reasonably verify your identity, we will contact you and request additional verification. The personal information we ask to verify your identity may depend on your relationship with Omnigo.

When you exercise your privacy rights under the applicable Data Protection Laws, you can designate an authorized agent or representative to make a request on your behalf by providing the authorized agent with written permission to do so and verifying your identity with us as part of the request, or by providing the authorized agent with Power of Attorney pursuant to applicable law (e.g., the California Probate code). We will ask the individual submitting the request to denote that they are an authorized agent or representative. When submitted by an authorized agent or representative, we ask the authorized agent or representative to provide a name, email address, and a description of the relationship with the individual who is the subject of the request and to certify that the representative has permission to submit the request and may request proof of the individual's written permission.

Children's Personal Information

The Omnigo website, including the products and services advertised thereon, is designed for a general audience and is not directed at children under the age of 13. We do not knowingly collect, solicit, share, or sell personal information from children under the age of 13 without parental or guardian consent. If we become aware that we have collected personal information from a child under the age of 13, we will promptly delete the information from our servers. If you believe that a child under the age of 13 may have provided us with personal information, please contact us at compliance@omnigo.com.

International Transfers of Personal Information

Please be aware that the personal information we collect may be transferred to and maintained on servers or databases located outside your state, province, country, or other jurisdiction, where the privacy laws may not be as protective as those in your location. If you are located outside the United States, please be advised that we process and store personal information in the United States. We may transfer personal data pursuant to your consent or when necessary for the fulfillment of a contract.

Data Privacy Framework Program (DPF)

Omnigo 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. Omnigo 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") regarding 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. Omnigo 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 (collectively, the "DDPF Principles"), the DPF Principles shall govern. To learn more about the Data Privacy Framework (DPF) program and to view our certification, please visit https://www.dataprivacyframework.gov/.

This Data Privacy Framework Policy (the "Policy") sets forth the privacy principles that Omnigo follows when processing Personal Data received from customers or prospective customers located in the European Economic Area ("EEA"), Switzerland, and the United Kingdom while providing services from the United States ("U.S."). This Policy does not apply to information collected through other Omnigo websites or to information collected during Omnigo-sponsored sales and marketing activities. This Policy also does not apply to Personal Data collected through Omnigo's recruiting process. For purposes of this Policy, Personal Data means data about an identified or identifiable individual that is received by Omnigo in the United States from the EEA, Switzerland, or the United Kingdom, and recorded in any form, and is within the scope of Regulation (EU) 2016/679 ("General Data Protection Regulation" or "GDPR"), the Swiss Federal Data Protection Act, or the UK Data Protection Act 2018, respectively.

Omnigo is the creator of certain software products. In connection with these software products, Omnigo provides product demonstrations, product development, product enhancements, cloud services, solution engineering services, professional technical services, data migration services, and product technical support services (collectively "Services") for the benefit of its customers and prospective customers in the EEA, Switzerland. The United Kingdom, through employees who may be located in the U.S., may process personal data to provide services to customers and prospective customers located in the EEA, Switzerland, or the United Kingdom.

Customers using Omnigo's cloud solutions are responsible for managing the data they store within Omnigo's cloud solutions. Customers determine the categories of Personal Data and other information that are stored by Omnigo. Similarly, Omnigo's customers and prospective customers who share data with Omnigo in connection with any of its Services determine which categories of Personal Data will be shared and for what purposes. Consequently, Omnigo does not generally know the categories of Personal Data to be processed or the purpose(s) of the processing unless and until Omnigo receives this information from its customers or prospective customers.

When Omnigo processes Personal Data, Omnigo does so only for the purpose of providing Services.

The Customer's and Prospective Customer's Responsibilities with Respect to Personal Data

Omnigo customers and prospective customers may choose to include Personal Data among the data stored within the Omnigo cloud or otherwise shared with Omnigo in connection with its provision of Services.

Omnigo processes only the Personal Data that its customers or prospective customers have chosen to share with Omnigo. Omnigo has no direct or contractual relationship with the subject of such Personal Data (a "Data Subject"). As a result, when a customer or prospective customer shares Personal Data, the customer or prospective customer is solely responsible for satisfying all legal obligations owed directly to the Data Subject under applicable data protection laws.

It is the customer's or prospective customer's responsibility to ensure that the Personal Data it collects can be legally collected in the country of origin. The customer or prospective customer is also responsible for providing to the Data Subject any notices required by applicable law and for responding appropriately to the Data Subject's request to exercise his or her rights with respect to Personal Data. In addition, the customer or prospective customer is responsible for ensuring that its use of Omnigo's cloud offerings or Services is consistent with any privacy policy the customer or prospective customer has established and any notices it has provided to Data Subjects.

Omnigo is not responsible for its customers' or prospective customers' privacy policies or practices or for the customers' or prospective customers' compliance with such policies or practices. Omnigo does not review, comment upon, or monitor its customers' or prospective customers' privacy policies or compliance with such policies. Omnigo also does not review instructions or authorizations provided to Omnigo to determine whether the instructions or authorizations are in compliance with or conflict with the terms of a customer's or prospective customer's published privacy policy or of any notice provided to Data Subjects. Customers and prospective customers are responsible for providing instructions and authorizations that comply with their policies, notices, and applicable laws.

Omnigo employees located in the United States may provide Services for customers and prospective customers located in the EEA, Switzerland, or the United Kingdom. To provide such Services, Omnigo may process Personal Data. Omnigo will apply the following DPF Principles to Personal Data physically or remotely transferred from the EEA, Switzerland or the United Kingdom to the United States.

Data Subjects have the right to access the Personal Data an organization holds about them. If such Personal Data is inaccurate or processed in violation of the DPF Principles, a Data Subject may also request that Personal Data be corrected, amended, or deleted.

When Omnigo receives Personal Data, it does so on its customer's or prospective customer's behalf. To request access to, or correction, amendment, or deletion of, Personal Data, Data Subjects should contact the Omnigo customer or prospective customer that collected their Personal Data. Omnigo will cooperate with its customers and prospective customers' reasonable requests to assist Data Subjects in exercising their rights under the DPF.

Data subjects have the right to opt out of (a) disclosures of their Personal Data to third parties not identified at the time of collection or subsequently authorized and (b) uses of Personal Data for purposes materially different from those disclosed at the time of collection or subsequently authorized. Omnigo's customers and prospective customers are responsible for informing Data Subjects when they have the right to opt out of such uses or disclosures.

Data Subjects who wish to limit the use or disclosure of their Personal Data should submit that request to Omnigo's customer or prospective customer that controls the use and disclosure of their Personal Data. Omnigo will cooperate with its customers and prospective customers' instructions regarding Data Subjects' choices.

Omnigo is committed to safeguarding the Personal Data that it receives. While Omnigo cannot guarantee the security of Personal Data, Omnigo takes reasonable and appropriate measures to protect Personal Data in Omnigo's possession from loss, misuse, unauthorized access, disclosure, alteration, and destruction.

Omnigo utilizes a combination of online and offline security technologies, procedures, and organizational measures to help safeguard Personal Data. For example, facility security is designed to prevent unauthorized access to Omnigo computers. Electronic security measures — including, for example, network access controls, passwords, and access logging — provide protection from hacking and other unauthorized access. Omnigo also protects Personal Data through firewalls, role-based restrictions, and, where appropriate, encryption technology. Omnigo limits access to Personal Data to employees, subcontractors, and third-party agents with a specific business reason for accessing such Personal Data. Individuals granted access to Personal Data are aware of their responsibility to protect such information and are provided with appropriate training and instruction.

Omnigo's customers and prospective customers are responsible for limiting their collection of Personal Data to that which is necessary to accomplish the purposes disclosed to Data Subjects and compatible purposes. They are also responsible for providing Omnigo with instructions or authorization for the processing of Personal Data consistent with such purposes.

Omnigo's customers and prospective customers are also responsible for ensuring that (a) the Personal Data they collect is accurate, complete, current, and reliable for its intended uses and (b) Personal Data is retained only for as long as is necessary to accomplish the customer's or prospective customer's legitimate business purposes disclosed to the Data Subject and for compatible purposes. Omnigo will cooperate with customers' and prospective customers' reasonable requests for assistance in meeting these obligations.

In the performance of Services, Omnigo will request only the minimum amount of information required to perform the applicable Services and will retain such information only for as long as necessary to provide the Services or for compatible purposes, such as to provide additional Services, to comply with legal requirements, or to preserve or defend Omnigo's legal rights.

Omnigo may disclose Personal Data to subcontractors and third-party agents who assist Omnigo in providing Services to its customers and prospective customers. Before disclosing

Personal Data to a subcontractor or third-party agent, Omnigo will obtain assurances from the recipient that it will: (a) use the Personal Data only to assist Omnigo in providing the Services; (b) provide at least the same level of protection for Personal Data as required by the DPF Principles; and (c) notify Omnigo if the recipient is no longer able to provide the required protections. Upon notice, Omnigo will act promptly to stop and remediate unauthorized processing of Personal Date by a recipient. Omnigo will remain liable for onward transfers to its subcontractors and third-party agents.

Omnigo may also be required to disclose, and may disclose, Personal Data in response to lawful requests by public authorities, including for the purpose of meeting national security or law enforcement requirements. To the extent permitted, Omnigo will inform its relevant customer or prospective customer before making such disclosure and provide it with a reasonable opportunity to object to such disclosure.

Omnigo will not otherwise disclose Personal Data to third parties.

In compliance with the EU-U.S. DPF Principles, including the UK Extension of the EU-U.S. DPF Principles and the Swiss-U.S. DPF Principles, Omnigo commits to resolve complaints about your privacy and Omnigo's collection or use of Personal Data transferred to the United States pursuant to this Policy.

Individuals from the European Union, Switzerland, and the United Kingdom with DPF inquiries or complaints should first contact Omnigo's Privacy Department at compliance@omnigo.com or 866-421-2374.

Omnigo has further committed to refer unresolved privacy complaints under the DFP Principles to an independent recourse mechanism, Data Privacy Framework Services, operated by BBB National Programs. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit https://bbbprograms.org/programs/all-programs/dpf-consumers/ProcessForConsumers [https://bbbprograms.org] for more information and to file a complaint. This service is provided free of charge to you.

If your DFP complaint cannot be resolved through the above channels, you may invoke binding arbitration for some residual claims not otherwise resolved by other redress mechanisms under certain conditions. For more information about binding arbitration, visit https://www.dataprivacyframework.gov/s/article/G-Arbitration-Procedures-dpf?tabset-35584=2%20[dataprivacyframework.gov].

The Federal Trade Commission has jurisdiction over Omnigo's compliance with the DPF.

For More Information

Data Subjects with questions about how Omnigo processes Personal Data should first contact the Omnigo customer or prospective customer that collected the Personal Data. Omnigo's Data Protection & Privacy Department can be contacted by emailing compliance@omnigo.com or by calling 866-421-2374.

Changes to this Privacy Policy

This Privacy Policy may be updated periodically and without prior notice to you to reflect changes in our information management practices. Omnigo will indicate at the top of this Privacy Policy when it was most recently updated. We encourage you to periodically review this Privacy Policy for the latest information on our privacy practices.

How to Contact Us

If you have any questions or comments about this Privacy Policy or would like to exercise your privacy rights regarding personal information that Omnigo maintains about you or your preferences, please contact us by e-mail or the toll-free number below.

- compliance@omnigo.com
- 866-421-2374