

PRIVACY POLICY

[Last Modified: November 2023]

Radix Technologies Ltd. ("**Radix**", "**Company**", "**we**" or "**us**") is devoted to making sure that your privacy rights are respected and personal data is collected and used in accordance with the current and applicable privacy and data protection law.

Radix is the developer, owner and operator of an innovative technology and solutions designed to enable device management solutions (MDM/EMM), focusing on interactive touch screens, Android TV, enterprise single-purpose, VR/AR and further includes cloud-based solutions, browser extensions, OEM solutions and applications and cloud-based classroom management solution ("**Product**" or "**Products**").

This privacy policy ("**Privacy Policy**") governs our data processing practices in connection with:

- "**Visitors**": Individuals who visit or otherwise interact with our website available at radix-int.com ("**Site**");
- "**Customers**": Our customers implementing, downloading and using the Product, and each of their representative and authorized users, creating an account or logging-in to the Product's interface or dashboard ("**Platform**"), for the purpose of using the Products' functionalities.
- "**End Users**": Customers' end users interacting with the Product. Such users have been granted an access to our Product directly by our Customers.

Our Product, Platform and the Site shall be collectively referred to herein as the "**Services**". Visitors, Customers and End Users shall be further, separately and collectively, referred to herein as "**you**".

This Privacy Policy explains what data we collect when using our Services, how such data may be used or shared with others, how we safeguard it and how you may exercise your rights related to your Personal Data (as defined below), as required under applicable data protection laws.

Where your use of the Product is subject to our [End User License Agreement](#) ("**EULA**"), note that this Privacy Policy is an integral part thereof and incorporated by reference.

Additional Notice to California Residents: In the event you are a California resident – please review our [CCPA Privacy Notice](#) to learn more about our privacy practices with respect to the California Consumer Privacy Act.

Additional Notice to Colorado, Virginia, Connecticut or Utah Residents: In the event you are a resident of one of these US states – please also review Section 13 below "*Jurisdiction-Specific Notices*" to learn more about our privacy practices and your rights under the privacy and data protection legislation which applies in these states.

We recommend you to review this Privacy Policy periodically to ensure that you understand our most updated privacy practices.

1. CHANGES TO THE PRIVACY POLICY

We reserve the right to change this Privacy Policy from time to time, at our sole discretion. The most recent version of the Privacy Policy will always be posted on the website and the update

date will be reflected in the “Last Modified” heading. We will provide notice to you if these changes are material, and, where required by applicable law, we will obtain your consent. Any material amendments to the Privacy Policy will become effective within 30 days upon the display of the modified Privacy Policy. We recommend you review this Privacy Policy periodically to ensure that you understand our most updated privacy practices.

2. CONTACT INFORMATION AND DATA CONTROLLER INFORMATION

Radix Technologies Ltd. incorporated under the laws of Israel (and its affiliated companies and subsidiaries) is the “Data Controller” (as such term is defined under the EU General Data Protection Regulation known as the “GDPR” or equivalent privacy legislation) of the Personal Data processed by the Company related to:

- Visitors’ use and interaction with our Site;
- Customers interaction with the Services;

Note to Customer’s End Users: with regards to End-Users’ Personal Data, we process Personal Data as “Data Processors” on behalf of the Customers in their role as “Data Controllers” of such Personal Data – meaning, the Customer that obtained our Product will decide who will be granted with access and authorization to use, manage or interact with the Product as an End User, and shall further controller the use of Personal Data to be collected and used.

This Privacy Policy governs solely our data collection practices. However, given the above and to provide transparency to End Users interacting with our Product, this Privacy Policy further provides information regarding the Personal Data that might be collected with regards to End Users, however, solely directly related to the Product’s functionalities and the Customer is the party deciding and controlling its use and processing operations related to such Personal Data. You should further review the Customer’s policies and practices as they independently apply to its data collection and processing, as well as further contact the Customer, on behalf of which you use or interact with the Product, in connection with a request to exercise your rights related to your Personal Data and where applicable, we will work with the Customer to comply with your request.

If you have any question, inquiry, request or concern related to this Privacy Policy or the processing of your Personal Data, you may contact our privacy team as follows:

- **By Email** – to our Data Protection Officer: dpo@radix-int.com.
- **By Mail** - Radix Technologies Ltd, 1 Ariel Sharon St., Or Yehuda (Tel-Aviv area) Israel 6037608

3. DATA SETS WE COLLECT AND FOR WHAT PURPOSE

You will find below information regarding the types of data we collect, the purposes for which we process your data as well as our lawful basis for processing (where the GDPR applies to your data).

We collect two types of data, depending on your interaction with us:

“Non-Personal Data” meaning aggregated, non-identifiable information, which may be made available or gathered via your access to and interactions with the Services. We are not aware of the identity or other identifiers of the individual from which the Non-Personal Data is collected. The Non-Personal Data being collected may include aggregated usage information, such as views of certain Site pages and actions on the Site), as well as technical information transmitted by your

device, such as the type of browser or device, type of operation system, device settings and technical software data, etc.

“Personal Data” or “Personal Information” meaning, individually identifiable information, namely information that identifies an individual or may, with reasonable effort, be used to identify an individual.

For avoidance of doubt, any Non-Personal Data connected or linked to any Personal Data shall be deemed as Personal Data as long as such connection or linkage exists.

We do not knowingly collect or process any Personal Data constituting or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning a person's health or data concerning a person’s sex life or sexual orientation (**“Special Categories of Personal Data”**).

The tables below detail the processing of Personal Data we collect, the purpose, lawful basis, and processing operations:

VISITORS & CUSTOMERS		
Data Sets	Purpose And Operations	Lawful Basis (Where the GDPR applies)
<p><u>Contact Communications:</u></p> <p>In the event you contact us for support or other inquiries, either through the online forms available on the Site, by sending us an email or by other means of communications we make available, you will be requested to provide us with your name, email address, phone number, the name of the company on behalf of which you are contacting us, country, and any other information you choose to share with us.</p> <p>Furthermore, if you use our live chat feature, you may be sharing additional information with the representative assisting you through the chat.</p> <p>(collectively “Contact Communications”)</p>	<p>We process such Contact Communications data solely for the purpose of contacting you, responding to your inquiries and provide you with the support or information you have requested.</p> <p>The correspondence with you may be processed and stored by us in order to improve our customer service, as well as in the event we reasonably determine it is needed for future assistance or to handle any dispute you might have with us.</p>	<p>We process such Contact Details data subject to our legitimate interest in order to respond to your inquiry.</p>

<p><u>Online Identifiers and Usage Data:</u></p> <p>When you access our Site or interact with the Platform, we collect certain online identifiers such as IP address, and cookie ID (“Online Identifiers”). We may further collect information related to your use and interaction with our Site and Platform such as directing campaign and URLs, pages viewed, access time and date, duration, clickstream, WiFi network, DNS name, etc. (“Usage Data”).</p> <p>In addition, we may use third party enrichment tools to provide us additional information based on your Online Identifiers (i.e. IP Address) such as the Company associated with the IP address</p>	<p>We process Online Identifiers and Usage Data through our or third-party cookies and tracking technologies for analytic, marketing and advertising purposes.</p> <p>For example, we process this data to understand how Visitors use our Site and how Customers use our Platform, as well as to measure effectiveness of our features and content.</p> <p>In addition, Usage Data related to our Site and Platform helps us to better understand our business, analyze our operations, maintain, improve, design, and develop the Service, conduct statistical analysis, etc.</p> <p>In addition, we process such data for operation, Site and Platform functionality, security and fraud prevention purposes, debugging purposes and to resolve technical problems.</p> <p>Note that, we do not attempt to analyze or determine your identity based on such information or otherwise combine it with any information such as your name or email address.</p>	<p>Where we collect Online Identifiers or Usage Data for analytic and advertising purposes, we process such data based on your consent which we will obtain through our cookie notice and consent management tool. You may withdraw consent or change your preferences at any time by using the cookie settings tool available on our Site.</p> <p>Where we collect Online Identifiers or Usage Data for operation and security, we process your data based on our legitimate interest.</p>
<p><u>Customer Registration and Account Data:</u></p> <p>In order for Customers to use our Product and access the Platform, Customers shall be required to sign up and create an account (independently, or otherwise provide information to our team, to designate the account). In order to create the account, the Customer shall be requested to provide</p>	<p>We process such Account Data to allow you to sign up to our Services, create or log-in to the Customer account, as well as enable access and use by your authorized users. We will further use such data to designate your Customer account and validate access, (e.g., account management, support and to provide other Services related to your relationship with us), as well as</p>	<p>We process such Account Data for the purpose of performing our contract with you, meaning, to provide the Product and to designate your account.</p> <p>Direct Marketing is based on our legitimate interest, you may opt-out at any time through the “unsubscribe” link within the email or by contacting us directly. Please note that</p>

<p>contact's full name, email address (of the account admin as well as each authorized user on behalf of the Customer), phone number, the name of the organization on behalf of which you are setting the account. If you choose to sign in through your Google account, we will be provided with your email address related to such account.</p> <p>Additionally, during the registration process you will be required to create a username and password. This information will be processed when you login as well.</p> <p>(collectively "Account Data")</p>	<p>to send you needed information related to our business engagement (e.g., send you a welcome message, notify you regarding any updates to our Product, send applicable invoices, etc.).</p> <p>In addition, we may use your contact information to send you additional occasional communications and updates related to the Product, as well as promotional and marketing emails, offers, materials and other marketing content ("Direct Marketing").</p>	<p>if you opt-out we will not send you our marketing materials however we will continue to send you Services related communications such as communications related to transactions, etc.</p>
<p><u>Location Data:</u></p> <p>When you access our Services we process location data that may include approximate location extracted from the IP or GPS location, where made available through your device.</p> <p>(collectively "Location Data")</p>	<p>We process Location Data for security and verification purposes, as well as to customize our Services.</p>	<p>Where we process Location Data for operation and security, we process your data based on our legitimate interest.</p> <p>Where required under applicable laws, we process Location Data through the GPS subject to your consent.</p>
<p><u>Recruitment Data:</u></p> <p>In the event you are interested in joining our team or apply for a position posted on our Site, you will be requested to provide us your contact details (such as name, email address, phone number, etc.) and CV.</p> <p>In addition, we may collect further information from public and online sources, referees, and former employers</p>	<p>We process Recruitment Data as part of our recruitment and screening efforts to decide whether you can suit a position in Radix. Further, we may process such data in order to comply with corporate governance and legal and regulatory requirements (including the retention of such information).</p>	<p>We process such Recruitment Data subject to our legitimate interest.</p> <p>If we process sensitive data to ensure diversity, we will do so upon your explicit consent, which you may withdraw at any time by contacting us.</p> <p>Further, if we reject your application, we will delete the Recruitment Data, unless we have requested your consent to keep you</p>

<p>(collectively “Recruitment Data”).</p>		<p>information for a future opportunity or if we are required by law.</p>
<p><u>Webinar Registration:</u> In the event you register to our webinars you will be requested to provide us with your full name, email address, phone number, country, and any other information you choose to share with us.</p>	<p>We process such data in order to register you as a participant and enable your participation. We may further process your data to send you needed information related to our webinar as well as additional occasional communications and updates related to our Services, promotional and marketing emails (i.e., Direct Marketing, as defined above).</p>	<p>We process such information subject to our legitimate interest. We may record the webinar, subject to your request and consent. Direct Marketing is further based on our legitimate interest, you may opt-out at any time through the “unsubscribe” link within the email or by contacting us directly. Please note that if you opt-out we will not send you our marketing materials.</p>
<p><u>Resellers:</u> If you wish to collaborate with the Company as a reseller of the Products, you will first be asked to submit an appropriate application for our review. As part of the application, you will be asked to provide information such as full name, contact information (phone, email, etc.), country, organization, field of operation, experience, etc.</p>	<p>We process such data for the purpose of reviewing and to examine your organization’s applicability your application for this collaboration.</p>	<p>We process such information subject to our legitimate interest.</p>
<p><u>Survey and Feedback:</u> We may ask you to provide feedback on our Services, including any alpha/beta services or free demo services. If you choose to address our request for such feedback or participate in our survey, we will collect your feedback and contact</p>	<p>We use this information to improve, revise and enhance our Service, as well as optimize and customize the Services.</p>	<p>We process such information subject to your consent. You may withdraw your consent at any time.</p>

information such as your name, email address, etc.		
--	--	--

END USERS – MDM PRODUCTS		
Data Sets	Purpose And Operations	Lawful Basis (Where the GDPR applies)
<p>If you are an End User of a device in which our MDM Product was implemented by a Customer, the following data sets are collected on behalf of the Customer from your device:</p> <ul style="list-style-type: none"> • Device Geolocation (approximate location extracted from the IP, time zone, or GPS location, where made available through your device); • Online Identifiers (IP address, MAC address); • Device Information (operating system type and version, device model, manufacturer, serial number, memory, storage, CPU model, screen size and resolution, device settings such as language, etc.); • Network Information (connected WiFi) • Usage Data and Installed Apps (access time and date, apps installed on the device, apps' usage statistics) • Filesystems Information; 	<p>We process such data for the purpose of providing the Customer with the Service.</p>	<p>As detailed above, we act as the “<i>Data Processor</i>” on behalf of the Customer, and thus, the Customer, as the “<i>Data Controller</i>” of your Personal Data, will determine the lawful basis, and shall be responsible to provide you with all needed data collection related policies, as well as, where applicable, obtain your consent.</p>
END USERS – CLASSROOM MANAGEMENT (“TEACHER VIEW”) PRODUCT		

Data Sets	Purpose And Operations	Lawful Basis (Where the GDPR applies)
<p>If you are an End User of our “Teacher View” Product, the following data sets are collected on behalf of the Customer:</p> <p>In order to access the features of the Techer View Product, the Customer will send you a designated link through which you will be requested to register with your Google or Microsoft account. We will collect your user name, image/avatar and email address, as provided by under such account.</p> <p>Please further note that, depending on the permissions requested by the Customer, you may need to provide access to your camera, microphone and Google drive. We will not store or use this Personal Data in any case.</p>	<p>We process such data for the purpose of providing the Customer with the Service.</p>	<p>As detailed above, we act as the “<i>Data Processor</i>” on behalf of the Customer, and thus, the Customer, as the “<i>Data Controller</i>” of your Personal Data, will determine the lawful basis, and shall be responsible to provide you with all needed data collection related policies, as well as, where applicable, obtain your consent.</p>

Please note that the actual **processing operation** per each purpose of use and lawful basis detailed in the table above may differ, and we are only responsible for the Personal Data we collect and process as the controller of the Personal Data. Such processing operation usually includes a set of operations made by automated means, such as collection, storage, use, disclosure by transmission, erasure, or destruction. The transfer of Personal Data to third-party countries, as further detailed in the “*Data Transfer*” Section below, is based on the same lawful basis as stipulated in the table above.

In addition, we may use certain Personal Data to prevent potentially prohibited or illegal activities, fraud, misappropriation, infringements, identity thefts, and any other misuse of the Services and to enforce our agreements, as well as to protect the security or integrity of our databases and the Product, and to take precautions against legal liability. Such processing is based on our legitimate interests.

4. GOOGLE PLAY STORE NOTICE

Radix Viso MDM allows the central management and support of mobile devices.

Functioning from the cloud, the Viso MDM agent collects data for which the Google Play Store policy requires your consent. In the device enrollment process you agree to your data being collected for the purposes of effective administration. This information will only be accessed by authorized account manager(s). No personal identifying data is required, no personal user data or personal app data is collected. The collected data is focused on the device, including the device Google account name, physical network address, IMEI, device settings, application list, application usage (duration and frequency), device location and OS version information. Any collected data is stored on the Viso MDM account only, with app statistics used anonymously for group statistics.

Radix Viso MDM server is collecting data that can be found under the following domains:

visomdm.com

glbth.com

App is using 'Device Admin' for the following reasons:

Security policy Limit Password - Needed for the Mobile Device Management Functionality 'Setting Password Restrictions'

Security policy Watch Login - Needed for the Mobile Device Management Functionality 'Monitoring and reporting failed Login Attempts'

Security policy Reset Password - Needed for the Mobile Device Management Functionality 'Anti Theft Lock' and 'Password recovery'

Security policy Force Lock - Needed for the Mobile Device Management Functionality 'Anti Theft Lock'

Security policy Wipe Data - Needed for the Mobile Device Management Functionality 'Anti Theft' and 'Wipe User Data'

Security policy Expire Password - Needed for the Mobile Device Management Functionality 'Setting Password Restrictions'

Security policy Encrypted Storage - Needed for the Mobile Device Management Functionality 'Setting Security Restrictions'

Security policy Disable Camera - Needed for the Mobile Device Management Functionality 'Setting Security Restrictions'

App is using the following Android permissions for:

android.permission.MANAGE_EXTERNAL_STORAGE – Needed for the Mobile Device Management Functionality, this will enable users to send and remove files from the device external storage

android.permission.QUERY_ALL_PACKAGES – Needed for the Mobile Device Management Functionality, this will enable users to manage the installed apps

android.permission.GET_ACCOUNTS - Needed for the Mobile Device Management Functionality, this will enable users to see who is currently logged in to the device for better identification and service (Email address, e.g. johnsmith@radix-int.com). Please note, we do not collect SOCIAL ACCOUNT information

android.permission.ACCESS_BACKGROUND_LOCATION - Needed for the Mobile Device Management Functionality 'Anti Theft Lock'

android.permission.ACCESS_FINE_LOCATION - Needed for the Mobile Device Management Functionality 'Anti Theft Lock'

android.permission.ACCESS_COARSE_LOCATION - Needed for the Mobile Device Management Functionality 'Anti Theft Lock'

5. HOW WE COLLECT INFORMATION

Depending on the nature of your interaction with the Site and Services, we may collect information as follows:

- **Automatically** – we may use cookies (as elaborated in the section below) or similar tracking technologies (such as pixels, tags, agent, etc.) to gather some information automatically.
- **Provided by you or about you voluntarily** – we will collect information if and when you choose to provide us with the information, such as through online registration, contact us communications, etc. all as detailed in this Privacy Policy.

6. SHARING INFORMATION WITH THIRD PARTIES

We share your Personal Data with third parties, including our affiliated companies and subsidiaries, as well as service providers that help us provide our Services. You can find in the table below information about the categories of such third-party recipients.

Category of Recipient	Data That Will Be Shared	Purpose of Sharing
Service Providers	All types of Personal Data	We share Personal Data with our trusted agents (such as legal counsel) and service providers (including, but not limited to, our Cloud Service Provider, Analytics Service Provider, CRM provider, etc.) so that they can perform the requested services on our behalf. Thus, we share your data with third party entities, for the purpose of storing such information on our behalf, or for other processing needs. These entities are prohibited from using your Personal Data for any purposes other than providing us with requested services
Any acquirer of our business	All types of Personal Data	We may share Personal Data, in the event of a corporate transaction (e.g., sale of a

		substantial part of our business, merger, consolidation or asset sale). In the event of the above, our affiliated companies or acquiring company will assume the rights and obligations as described in this Policy.
Affiliated companies	All types of Personal Data	We may share Personal Data with our affiliated companies in accordance with the terms of this Policy and for the purpose of providing the Services.
Legal and law enforcement	Subject to law enforcement authority request.	We may disclose certain data to law enforcement, governmental agencies, or authorized third parties, in response to a verified request relating to terror acts, criminal investigations or alleged illegal activity or any other activity that may expose us, you, or any other user to legal liability, and solely to the extent necessary to comply with such purpose.

For avoidance of doubt, we may transfer and disclose or otherwise use Non-Personal Information or information which is linked to anonymous random identifiers or information that is aggregated in a non-identifiable way, at its own discretion.

7. **COOKIES POLICY**

When you access or use the Site, we use “cookies” or similar tracking technologies, which store certain information on your device (i.e., locally stored). The use of cookies is a standard industry-wide practice. A “cookie” is a small piece of information that a website assigns and stores on your computer while you are viewing a website. Cookies are used by us for various purposes, including allowing you to navigate between pages efficiently, as well as for statistical purposes, analytic purposes and advertising. You can find more information about our use of cookies here: www.allaboutcookies.org.

please see our Cookies List at: <https://www.radix-int.com/cookies-policy/> which details the cookies we use on are Site. You may change your preferences at any time using the cookies settings tool available on our Site.

Also note that, most browsers will allow you to erase cookies from your computer’s hard drive, block acceptance of cookies, or receive a warning before a cookie is stored. You may set your browser to block all cookies, including cookies associated with our Site and Services, or to indicate when a cookie is being used by us, by adjusting the privacy and security settings of your web browser. Please refer to the support page of your browser to learn more about how you can adjust your privacy and security settings. Please note that once you choose to opt out or disable cookies, some features of the Services may not operate properly and your online experience may be limited. In addition, even if you do opt-out, you may still receive some content and advertising, however, it will not be targeted content or advertising.

Where we use third-party advertising cookies, such third-party may independently collect, through the use of such tracking technologies, some or all types of Personal Data detailed above, as well as additional data sets, including to combine such information with other information they have independently collected relating to your online activities across their network of websites, for the purpose of enhanced targeting functionality and delivering personalized ads, as well as providing aggregated analytics related to the performance of our advertising campaign you interacted with. These third parties collect and use this information under their own privacy policies, and are responsible for their practices.

8. DATA RETENTION

We retain the Personal Data we collect as long as it remains necessary for the purposes set forth above, all in accordance with applicable regulation, or until an individual expresses a preference to opt-out.

Other circumstances in which we will retain your Personal Data for longer periods of time include: (i) where we are required to do so in accordance with legal, regulatory, tax, or accounting requirements; (ii) for us to have an accurate record of your dealings with us in the event of any complaints or challenges; or (iii) if we reasonably believe there is a prospect of litigation relating to your Personal Data. Please note that except as required by applicable law, we may at our sole discretion, delete or amend information from our systems, without notice to you, once we deem it is no longer necessary for such purposes.

In case you are an End User it is hereby clarified that the Customer decides and instructs us when to delete Personal Data (or otherwise exercises its independent ability to delete data through its account).

9. DATA SECURITY

We work hard to protect the Personal Data we process from unauthorized access, alteration, disclosure, or destruction. We have implemented physical, technical, and administrative security measures that comply with applicable laws and industry standards, such as encryption, access restrictions and permissions, etc. Additional information regarding our data security practices is available [HERE](#).

Note that we cannot be held responsible for unauthorized or unintended access beyond our control, and we make no warranty, express, implied, or otherwise, that we will always be able to prevent such access.

Please contact us at: dpo@radix-int.com if you feel that your privacy was not dealt with properly, in a way that was in breach of our Privacy Policy, or if you become aware of a third party's attempt to gain unauthorized access to any of your Personal Data. We will make a reasonable effort to notify you and the appropriate authorities (if required by applicable law) in the event that we discover a security incident related to your Personal Data.

10. CROSS BORDER DATA TRANSFER

Due to our global business operation, we may store or process your Personal Data in the EU, United States or in other countries. Thus, any information you provide to us may be transferred

to and processed in countries other than the country from which you accessed our Service. In the event that we need to transfer your Personal Data out of your jurisdiction, we will take appropriate measures to ensure that your Personal Data receives an adequate level of protection as required under applicable law. Furthermore, when Personal Data that is collected within the European Economic Area (“EEA”) is transferred outside of the EEA to a country that has not received an adequacy decision from the European Commission, we will take necessary steps in order to ensure that sufficient safeguards are provided during the transferring of such Personal Data, in accordance with the provision of the standard contractual clauses approved by the European Union. Thus, we will obtain contractual commitments or assurances from the data importer to protect your Personal Information, using contractual protections that EEA and UK regulators have pre-approved to ensure your data is protected (known as standard contract clauses), or rely on adequacy decisions issued by the European Commission. Some of these assurances are well-recognized certification schemes.

11. YOUR RIGHTS

We acknowledge that different people have different privacy concerns and preferences. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used. We allow you to exercise certain choices, rights and controls in connection with your information. Depending on your relationship with us, your jurisdiction and the applicable data protection laws that apply to you, you have the right to control and request certain limitations or rights to be executed.

Please note, if you are an End User and you contact us regarding your rights, you will be directed to contact the applicable Customer as the “Data Controller” of the Personal Data.

The table below details some of the principal rights that may apply to (subject to your jurisdiction and additional conditions), how you can exercise them and appeal a decision we take in this regard:

Right to Be Informed	You have the right to be provided with information regarding our Personal Data collection and privacy practices. All is detailed under this Privacy Policy. If you have any additional questions, please contact us at: dpo@radix-int.com
Right to Know, Access Rights	You have the right to confirm whether we collect Personal Data about you and to know which Personal Data we specifically hold about you, and receive a copy of such or access it.
Right to Correction/ Rectification	You have the right to request the updating of Personal Data that is not correct, taking into account the nature of the processing and the purposes.
Right to Be Forgotten, Right to Deletion	You have the right to request the erasure of certain Personal Data if specific conditions are satisfied. This right is not absolute. We may reject your request under certain circumstances, including where we must retain the data in order to comply with legal obligations or defend against legal claims, other legitimate interests such as record keeping with regards to our engagements, completing transactions, providing a good or service that you requested, taking actions reasonably anticipated within the context of our

	<p>ongoing business relationship with you, fulfilling the terms of a written warranty, detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, or prosecuting those responsible for such activities; debugging products to identify and repair errors that impair existing intended functionality; exercising free speech, ensuring the right of another consumer to exercise their free speech rights, or exercising another right provided for by law; and engaging in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.</p> <p>You do not need to create an account with us to submit a deletion request.</p>
<p>Right to Restriction of Processing</p>	<p>You may be entitled to limit the purposes for which we process your Personal Data if one of the following conditions are satisfied: where the accuracy of the Personal Data is contested by you, for a period enabling us to verify the accuracy of the Personal Data; where the processing is unlawful and you oppose the erasure of the Personal Data and request the restriction of its use instead; where we no longer need the Personal Data for the purposes of the processing, but we are required by you to retain it for the establishment, exercise or defense of legal claims; where you objected to processing (as detailed below) pending the verification whether our legitimate grounds override your request.</p>
<p>Right to Data Portability</p>	<p>You have the right to get a copy of your Personal Data in a portable format and, to the extent technically feasible, readily usable format that allows you to transmit the Personal Data to another entity without hindrance. We will select the format in which we provide your copy.</p>
<p>Right to Withdraw Consent or Opt-Out (Object) Under the GDPR, and Specifically in the US the Right to Opt-Out From: (i) Selling Personal Data;</p>	<p>When the lawful basis for processing your Personal Data is your consent, you may withdraw such consent at any time. For example, you may unsubscribe at any time from our mailing list.</p> <p>You further have the right to object to the processing of Personal Data, in the event the basis for processing is our legitimate interests. However, we will be permitted to continue the processing if our legitimate interests override your rights, or when processing is necessary to establish, exercise, or defend a legal claim or right.</p> <p>You have the right to opt-out from direct marketing, if applicable, by unsubscribing through the email received.</p> <p>We do not profile you in a manner that has a significant effect on you or other individuals, therefore there isn't an opt-out option.</p> <p>We do not "sell" or "share" information as most people would commonly understand that term. We do not, and will not, disclose your Personal Data in direct exchange for money or some other form of payment; however, we do share Personal Data for analytic and marketing purposes, including targeted advertising, when we promote our Site or Services. In most cases we obtain Personal Data collected automatically from our Site and your</p>

<p>(ii) Targeted Advertising; and</p> <p>(iii) Profiling & Automated Decision Making</p>	<p>actions therein through our use of cookies, and do not combine it with your actions on other websites, however, our third-party partners might do so, when providing analytic or advertising services to us.</p> <p>You have the right to opt-out of the “selling” or “sharing” of your Personal Data for “cross-contextual behavioral advertising”, or “targeted advertising”, often referred to as “interest-based advertising” as well. You can exercise these rights by using the cookies setting tool available on our Site.</p> <p>You are able to install privacy-controls in the browser's settings to automatically signal the opt-out preference to all websites you visit (such as the “Global Privacy Control”).</p> <p>In any event, please keep in mind that opt-out tools are limited to the browser or device you use because they work off your browser ID and device ID and, accordingly, you will need to opt-out on each browser and device you use. Your browser may save some information in its cookies and cache to maintain your privacy preferences. Clearing these may remove opt-out preferences, requiring you to opt-out again.</p>
<p>Right To Appeal or Lodge Complaint</p>	<p>If we decline to take action on your request, we will inform you without undue delay as required under applicable laws. The notification will include a justification for declining to take action and instructions on how you may appeal, if applicable.</p> <p>Under the GDPR you have the right to lodge a complaint with the applicable Data Protection Authority in the EU or the Information Commissioner in the UK.</p>
<p>Non-Discrimination</p>	<p>Denying a good or service, providing a different level or quality of service, or charging different prices. We do not discriminate against our Visitors or Customers, but we reserve the right to deny a good or service, provide a different level or quality of service, or charge different prices, all subject to applicable laws.</p>

For additional information on your rights and how to exercise your rights, please see the Data Subject Request Form (“DSR”) available [HERE](#) or send it to: dpo@radix-int.com. For California residents, please further see our [CCPA Privacy Notice](#) to learn more about your rights.

Certain rights can be easily executed independently by you without the need to fill out the DSR Form, and for example: (i) If you are our Customer, you can correct certain data provided under your Customer account (such as contact information) through the account settings; (ii) You can opt-out from receiving our marketing emails by clicking “unsubscribe” link; (iii) You can use the cookie settings tool on our Site to change your preferences.

In the event you are a Customer – note that termination of the engagement or closing your Customer account does not automatically resolved in deletion of data. If you wish to deleted the data, please ensure to contact us with such request.

12. PROTECTING CHILDREN

Our Site and Services are not intended for Visitors or Customers under the age of eighteen (18). Therefore, we do not intend and does not knowingly collect directly Personal Data from children. We will discard any information we receive from a user that is considered a "child" immediately upon discovering that such a user shared information with us. Please contact us at: dpo@radix-int.com if you have reason to believe that a child has shared any information with us.

Under the use of our Product, we are not aware to the age of the End Users interacting with the Product on behalf of our Customers and it is the Customer's responsibility to provide you with needed notifications, disclosures, and where applicable, obtain consent (including, where applicable, parental consent). Without derogating from the above, we collect data related to the use of the Product by End Users solely for the purpose of providing the Customer with the Services.

13. JURISDICTION-SPECIFIC NOTICES

Additional Information for California Residents

This section applies only to California residents. Pursuant to the California Consumer Privacy Act of 2018 and as amended by the California Privacy Rights Act of 2020 effective January 1, 2023 ("CPRA") (collectively "CCPA").

Please see the [CCPA Privacy Notice](#), which discloses the categories of Personal Information collected, purpose of processing, source, categories of recipients with whom we share the Personal Information for a business purpose, whether the Personal Information is sold or shared, the retention period, and how to exercise your rights as a California resident.

Additional Information for Colorado Residents

This section applies to Colorado residents acting **only** as an individual or household context (and **not** in a commercial or employment context, as a job applicant or as a beneficiary of someone acting in an employment context). Pursuant to the Colorado Privacy Act ("CPA") please see below the disclosure of the categories of Personal Data that are collected or processed, the purposes, how consumers can exercise their rights, and appeal such decision, categories of third-parties the controller shares or sells the Personal Data, or sells the Personal Data for advertising and how to opt-out.

"Personal Data" as defined in the CPA means information that is linked or reasonably linkable to an identified or identifiable individual and does **not** include publicly available information that is lawfully made available from government records, or that a consumer has otherwise made available to the public; de-identified or aggregated consumer information; or information excluded from the CPA scope, such as: Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPPA) or 42 CFR Part 2- "Confidentiality Of Substance Use Disorder Patient Records", Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA) or and the Driver's Privacy Protection Act of 1994, Children's Online Policy Protection Act of 1998 (COPPA), Family Educational Rights and Privacy Act of 1974, national Security Exchange Act of 1934, higher education data and employment data.

“Sensitive Data” under the CPA means: racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation; genetic or biometric data that can be processed to uniquely identify an individual; or child data. We do not process Sensitive Data.

In Section 3 of this Privacy Policy **“Data Sets We Collect and For What Purpose”**, we describe our collection and processing of Personal Data, the categories of Personal Data that are collecting and processing, and the purposes for which Personal Data is processed, stored or used. We will not collect additional categories of Personal Data or use the Personal Data we collected for a materially different, unrelated, or incompatible purpose without obtaining your consent. Additionally, Section 6 of this Privacy Policy **“Sharing Information with Third Parties”** details and discloses the categories of third-parties we share Personal Data with for business purposes. Section 11 of this Privacy Policy **“Your Rights”** details and discloses your rights, including where shared or sold for targeted advertising.

Only you, or someone legally authorized to act on your behalf, may make a request to **know** or **delete** your Personal Data. If the request is submitted by someone other than you, proof of authorization (such as power of attorney or probate documents) will be required.

We will respond to a verifiable request within 45 days after receipt (no more than twice in a twelve-month period). We reserve the right to extend the response time by an additional 45 days when reasonably necessary and we will provide a notification of the extension within the first 45 days. If we refuse to take action, you **may appeal our decision** within a reasonable period time by sending us an applicable notice at: dpo@radix-int.com. Within 60 days of our receipt of your appeal, we will inform you in writing of any action taken or not taken in response to your appeal, including a written explanation of the reasons for our decisions. If the appeal is denied, you may submit a complaint as follows: Colorado AG at <https://coag.gov/file-complaint/>

If you have an account with us, we may deliver our written response to that account or via email at our sole discretion. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option. You do not need to create an account for submitting a request.

Any disclosures we provide will only cover the 12-months period preceding our receipt of your request. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

Additional Information for Connecticut Residents

Under the Connecticut Data Privacy Act, Public Act. No. 22-14 (the **“CDPA”**) if you are a resident of Connecticut, acting in an individual or household context (and **not** in a commercial or employment context or as a representative of business, non-profit or governmental entity), your rights with respect to your Personal Data are described below.

“Personal Data” means any information that is linked or reasonably linkable to an identified or identifiable individual and does **not** include publicly available information that is lawfully made available from government records, or that a consumer has otherwise made available to the public; de-identified or aggregated consumer information; or information excluded from the CDPA scope, such as: HIPAA, GBPA, non-profit entities, higher education, employment data and FCRA, Driver's Privacy Protection Act of 1994, Family Educational Rights and Privacy Act, Farm Credit Act.

“Sensitive Data” means data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, citizenship, or immigration status; The processing of genetic or biometric data for the purpose of uniquely identifying an individual;

Personal Data collected from a known child; Precise geolocation data. We do not process Sensitive Data.

Under CDPA, the Company is required to provide you with a clear and accessible privacy notice that includes: categories of Personal Data processed, purpose of processing, instructions for exercising consumer rights and appealing decisions, categories of Personal Data shared with third parties, categories of third parties with whom data is shared, and any sale of data or targeted advertising.

In Section 3 of this Privacy Policy "***Data Sets We Collect and For What Purpose***", we describe our collection and processing of Personal Data, the categories of Personal Data that are collecting and processing, and the purposes for which Personal Data is processed, stored or used. We will not collect additional categories of Personal Data or use the Personal Data we collected for a materially different, unrelated, or incompatible purpose without obtaining your consent. Additionally, Section 6 of this Privacy Policy "***Sharing Information with Third Parties***" details and discloses the categories of third-parties we share Personal Data with for business purposes. Section 11 of this Privacy Policy "***Your Rights***" details and discloses your rights, including where shared or sold for targeted advertising. Note, under CDPA consent can be withdrawn within 15-days of notice at any time.

We shall respond to your request within 45 days of receipt. The response period may be extended once by 45 additional days when reasonably necessary, taking into account the complexity and number of requests and we inform you of such extension within the initial 45-day response period, together with the reason for the extension.

If we decline to take action on your request, we shall so inform you without undue delay, within 45 days of receipt of your request. Our notification will include a justification for declining to take action and instructions on how you may appeal. Within 60 days of our receipt of your appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, you may submit a complaint to the Connecticut Attorney General at link: <https://www.dir.ct.gov/ag/complaint/> or (860) 808-5318.

We shall provide information in response to your request free of charge, up to twice annually, unless requests are manifestly unfounded, excessive or repetitive. If we are unable to authenticate your request using commercially reasonable efforts, we may request additional information reasonably necessary to authenticate you and your request. If we cannot authenticate you and your request, we will not be able to grant your request.

Additional Information for Virginia Residents

Under the Virginia Consumer Data Protection Act, as amended ("**VCDPA**") if you are a resident of Virginia acting in an individual or household context (and **not** in an employment or commercial context), you have certain rights with respect to your Personal Data, as described below.

"**Personal Data**" means any information that is linked or reasonably linkable to an identified or identifiable natural person, and does not include publicly available information that is lawfully made available from government records, that a consumer has otherwise made available to the public; de-identified or aggregated consumer information; Information excluded from the VCDPA scope, such as: HIPAA, GBPA, non-profit entities, higher education, employment data and FCRA, Driver's Privacy Protection Act of 1994, Family Educational Rights and Privacy Act, Farm Credit Act.

“Sensitive Data” under the VCDPA means data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; Personal Data collected from a known child; and precise geolocation data. We do not process Sensitive Data.

The VCDPA requires the Company to disclose the categories of Personal Data processed, purpose of processing, how you can exercise your rights, including how a you may appeal our decision with regard to the consumer request, the categories of Personal Data shared with third parties and with whom, and if the Company sells Personal Data to third parties or processes Personal Data for targeted advertising.

In Section 3 of this Privacy Policy **“Data Sets We Collect and For What Purpose”**, we describe our collection and processing of Personal Data, the categories of Personal Data that are collecting and processing, and the purposes for which Personal Data is processed, stored or used. We will not collect additional categories of Personal Data or use the Personal Data we collected for a materially different, unrelated, or incompatible purpose without obtaining your consent. Additionally, Section 6 of this Privacy Policy **“Sharing Information with Third Parties”** details and discloses the categories of third-parties we share Personal Data with for business purposes. Section 11 of this Privacy Policy **“Your Rights”** details and discloses your rights, including where shared or sold for targeted advertising. Note, under CDPA consent can be withdrawn within 15-days of notice at any time.

We will respond to a verifiable request within 45 days after receipt (no more than twice in a twelve-month period). We reserve the right to extend the response time by an additional 45 days when reasonably necessary and we will provide a notification of the extension within the first 45 days. If we refuse to take action on a request, you **may appeal our decision** within a reasonable period time by sending us an applicable notice at: dpo@radix-int.com. Within 60 days of our receipt of your appeal, we will inform you in writing of any action taken or not taken in response to your appeal, including a written explanation of the reasons for our decisions. If the appeal is denied, you may submit a complaint to the Virginia Attorney General at <https://www.oag.state.va.us/consumercomplaintform>.

If you have an account with us, we may deliver our written response to that account or via email at our sole discretion. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option. You do not need to create an account for submitting a request.

Any disclosures we provide will only cover the 12-months period preceding our receipt of your request. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

We shall provide information in response to your request free of charge, up to twice annually, unless requests are manifestly unfounded, excessive or repetitive. If we are unable to authenticate your request using commercially reasonable efforts, we may request additional information reasonably necessary to authenticate you and your request. If we cannot authenticate you and your request, we will not be able to grant your request.

Additional Information for Utah Residents (Effective January 2024)

Under the Utah Consumer Privacy Act (“**UCPA**”) if you are a resident of Utah, acting in an individual or household context (and **not** in a commercial or employment context) your rights with respect to your Personal Data are described below.

“**Personal Data**” means data which is linked or reasonably linkable to an identifiable individual, and does not include de-identified data and publicly available data or data that is processed not within the scope of UCPA.

In Section 3 of this Privacy Policy “***Data Sets We Collect and For What Purpose***”, we describe our collection and processing of Personal Data, the categories of Personal Data that are collecting and processing, and the purposes for which Personal Data is processed, stored or used. We will not collect additional categories of Personal Data or use the Personal Data we collected for a materially different, unrelated, or incompatible purpose without obtaining your consent. Additionally, Section 6 of this Privacy Policy “***Sharing Information with Third Parties***” details and discloses the categories of third-parties we share Personal Data with for business purposes. Section 11 of this Privacy Policy “***Your Rights***” details and discloses your rights, including where shared or sold for targeted advertising. Note, under CDPA consent can be withdrawn within 15-days of notice at any time.