MXD PRIVACY POLICY

Last Updated – 10/19/2023

Thank you for choosing to be part of our community at MxD USA. ("MxD", "Company", "we", "us", "our"). We are committed to protecting your personal information and your right to privacy. The purpose of this MxD Privacy Policy (“Policy”) is to inform you how we collect, use, and share the personal information we collect about you from your use of our (i) websites (“Website(s)”), (ii) mobile apps, if applicable, (iii) products and/or services (collectively, the “Services”); and (iv) when you otherwise interact with us or receive a communication from us. If there are any terms in this privacy notice that you do not agree with, please contact us, or discontinue your use of our Services immediately.

NOTE: USER REGISTRATION AND ACCESS TO INDIVIDUALS AND/OR ORGANIZATIONS LOCATED IN THE EU, UK, OR SWITZERLAND IS STRICTLY PROHIBITED. IF YOU RESIDE IN AND/OR ARE LOCATED IN ANY OF THOSE REGIONS, PLEASE DISCONTINUE YOUR REGISTRATION IMMEDIATELY.

TABLE OF CONTENTS

1. WHAT INFORMATION DO WE COLLECT?
2. HOW DO WE USE YOUR INFORMATION?
3. WILL YOUR INFORMATION BE SHARED WITH ANYONE?
4. HOW DO WE HANDLE YOUR SOCIAL LOGINS?
5. HOW LONG DO WE KEEP YOUR INFORMATION?
6. HOW DO WE KEEP YOUR INFORMATION SAFE?
7. DO WE COLLECT INFORMATION FROM MINORS?
8. WHAT ARE YOUR PRIVACY RIGHTS?
9. CONTROLS FOR DO-NOT-TRACK FEATURES
10. AUTHORIZED SERVICE PROVIDERS?
11. HOW CAN YOU CONTACT US ABOUT THIS NOTICE?
12. DO WE MAKE UPDATES TO THIS NOTICE?
13. STATE PRIVACY RIGHTS
1. WHAT INFORMATION DO WE COLLECT?

Information you provide directly

We collect and process personal information that you voluntarily provide to us when you register for Services on the Website, express an interest in obtaining information about us or our products and Services, when you participate in activities on the Website (such as by posting messages in our online forums or entering competitions, contests, or giveaways) or otherwise when you contact us. You are responsible for the accuracy and completeness of all information you provide to us directly.

The personal information that we collect depends on the context of your interactions with us and the Website, the choices you make and the products and features you use. For example, the personal information we collect may include first and last names, phone numbers, email addresses, job titles, mailing addresses, usernames, passwords or other user authentication data, contact preferences, and payment information and other information that is linked or reasonably linkable to you or your household (“personal information”). For clarity, information that has been de-identified or anonymized, as those terms are defined by applicable privacy laws, does not constitute personal information; Our use of such de-identified or anonymized information is not restricted by this Policy.

Information we receive from third parties

We may obtain information about you from other sources, including service providers, third-party services, and public sources. We are not responsible nor liable for the accuracy of the information provided by third parties or for third party policies or practices.

Additionally, we may provide you with the option to register with us using your existing social media account details, such as your Facebook, Twitter, or other social media account. If you choose to register, we will collect the information described in the section below titled "HOW DO WE HANDLE YOUR SOCIAL LOGINS?".

Information we collect automatically when you connect to our technology systems via your technology device

We, our service providers, and/or third-party services may also automatically collect certain information about you when you access or use the Website and/or Services (“Usage Information”). Usage Information may include IP address, device identifier, browser type, operating system, information about your use of the Website and/or Services, devices you use, the web page you visited before coming to our sites, and identifiers associated with your devices, and your devices (depending on their settings) may also transmit location information to us.

The methods that may be used on the Website and Services to collect Usage Information may include, without limitation, cookies, web beacons (also known as “tracking pixels”), embedded scripts, location-identifying technologies, device recognition technologies, in-app tracking methods, device and activity monitoring and other tracking technologies now and hereafter developed (collectively, “Tracking Technologies”). Tracking Technologies may be used to collect information about interactions with the Website or e-mails, including information about your browsing and purchasing behavior. Such Tracking Technologies may include cookies, web beacons, embedded scripts, location-identifying technologies, device-recognition technologies, and device and activity monitoring.
Some information about your use of the Website and/or Services may be collected using Tracking Technologies across time and websites, and used by us and third parties for purposes such as to associate different devices you use and deliver relevant ads and/or other content to you on the Website and certain other online websites.

2. HOW DO WE USE YOUR INFORMATION?

We use your personal information solely to develop, offer, deliver, and improve our products and services, to fulfill legal, regulatory and/or contractual requirements, and as otherwise permitted by applicable law. We do not sell personal information.

For example, we use personal information as follows:

• To Operate the Website and provide you with the Services.

• To Facilitate your account creation and login process. If you choose to link your account with us to a third-party account (such as your Google or Facebook account), we use the information you allow us to collect from those third parties to facilitate account creation and login process for the performance of the contract. See the section below headed "HOW DO WE HANDLE YOUR SOCIAL LOGINS?" for further information.

• To Post testimonials. We post testimonials on our Website that may contain personal information. Prior to posting a testimonial, we will obtain your consent to use your name and the content of the testimonial. If you wish to update, or delete your testimonial, please contact us and be sure to include your name, testimonial location, and contact information.

• To Request feedback. We may use your information to request feedback and to contact you about your use of our Website and/or Services.

• To enable user-to-user communications. We may use your information in order to enable user-to-user communications with each user’s consent.

• To send administrative information to you. We may use your personal information to send you product, service, and new feature information and/or information about changes to our terms, conditions, and policies.

• To identify, prevent, investigate, and take other actions with respect to suspected or actual fraud or illegal activity or other activity that violates our policies.

• To ensure the security and integrity of our personal information processing.

• To protect our rights, property, or safety and that of our users.

• To enforce our terms, conditions, and policies for business purposes.

• To comply with applicable laws, rules, regulations, and legal processes, as well as our company policies, including to respond to claims asserted against us and to enforce or administer terms and agreements.

• To respond to valid regulatory inquiries or other lawful requests not prohibited by law.
• To fulfill and manage your orders, payments, returns, and exchanges, if applicable.
• To administer prize draws and competitions if you elect to participate in our competitions.
• To respond to your inquiries
• To send you marketing and promotional communications. We and/or our third-party marketing partners may use the personal information you send to us for our marketing purposes if this is in accordance with your marketing preferences. For example, when expressing an interest in obtaining information about us or our Website, subscribing to marketing or otherwise contacting us, we will collect personal information from you. You can opt-out of our marketing emails at any time (see the "WHAT ARE YOUR PRIVACY RIGHTS?" below).
• Deliver targeted advertising to you. We may use your information to develop and display personalized content and advertising (and work with third parties who do so) tailored to your interests and/or location, and to measure the efficacy of such targeted advertising.
• For any other permitted business purposes, including those with your consent (if required), not inconsistent with our statements under this Policy or otherwise made by us in writing at the point of collection, and not prohibited by law. For example, we may use your personal information for data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns, evaluating and improving our Website, products, marketing and your experience.

3. WILL YOUR INFORMATION BE SHARED WITH ANYONE?

We may disclose your personal information to our vendors, agents, or contractors in order to provide the Website or perform the Services. Our vendors, agents, and contractors are subject to data protection and confidentiality obligations when processing personal information on our behalf and may not use your personal information for any other purpose.

We may also share your personal information:
• To provide you with the Services,
• To Respond to your inquiries,
• To Advertise or market our Services to you,
• To perform marketing research,
• For sales, support, and service-related purposes,
• To protect rights, property, life, health, security, and safety,
• To respond to legal process, including to disclose personal information to a court, legal authority, opposing party in litigation, our legal counsel, or other advisors in connection with a judicial proceeding, court order, subpoena, or other legal process,
• To negotiate or complete any proposed or actual merger, purchase, sale, or any other type of acquisition or other transaction, including a transfer of all or a portion of our business to another organization,
• With your consent or at your direction; and
• To achieve any other purpose consistent with our statements in this Privacy Policy, other statements made to you at the time of collection, or otherwise allowed by applicable law.
We may disclose your personal information to comply with applicable law, such as in response to requests from law enforcement agencies, regulators, other public authorities, courts, and third-party litigants in connection with legal proceedings or investigations.

When you share personal information or otherwise interact with public areas of the Website (for example, by posting comments, contributions, or other content to the Website), such personal information may be viewed by all users and may be publicly made available outside the Website in perpetuity. If you interact with other users of our Website and register for our Website through a social network (such as Facebook), your contacts on the social network will see your name, profile photo, and descriptions of your activity. Similarly, other users will be able to view descriptions of your activity, communicate with you via our Website and/or Services, and view your profile.

4. HOW DO WE HANDLE YOUR SOCIAL LOGINS?

This section only applies to you if you choose to register or log in to our Services using a social media account, such as your Facebook or Twitter account.

Our Website offers you the ability to register and login to our Services using your third-party social media login credentials. If and when you choose to do this, we will receive certain personal information about you from your social media provider. The personal information we receive may vary depending on the social media provider, but will often include your name, email address, friends list, profile picture, and other information you choose to make public on such social media platform.

We will use your personal information received from such social media platform to provide the Services to you, provided that our use is consistent with our commitments to you under this Policy or otherwise made by us in writing at the point of collection, and not prohibited by law. We do not control, and are not responsible for, other uses of your personal information by your third-party social media providers. We recommend that you review their privacy notices to understand how they collect, use, and share your personal information, and how you can set your privacy preferences on their sites and apps.

5. HOW LONG DO WE KEEP YOUR INFORMATION?

We retain your personal information for no longer than is necessary to achieve the purposes for which the personal information was collected, or as may otherwise be permitted or required under applicable law.

6. HOW DO WE KEEP YOUR INFORMATION SAFE?

We maintain an information security program that contains appropriate administrative, technical, and physical measures designed to ensure a level of security appropriate to the nature of our business and the personal information we collect and process.

We restrict administrative access to our Services, and by extension your personal information, to authorized employees within our organization. We require secure VPN usage by all employees and perform background checks on all employees prior to employing them. We maintain an up-to-date security training program and employ multi-factor authentication measure wherever possible.

The platform utilized to host our Service is “Hivebrite”, wherein they have taken their own appropriate measures to ensure a level of security appropriate to the nature of our business and the personal
information we collect and process. Hivebrite’s hosting companies follow SOC 1/2/3 and ISO 27001 certifications, and Hivebrite has a Data Processing Agreement (“DPA”) in place covering their vendors and subprocessors. To find out more about what steps Hivebrite takes in maintaining their platform, you can visit this URL: https://blog.hivebrite.com/how-hivebrite-protects-your-communitys-data

Of course, there is no such thing as perfect security on the Internet. You are responsible for maintaining the secrecy of your passwords or any account information. Please be careful and responsible whenever you’re online. Please contact us at the contact information below if you have any questions about the security of your personal information.

7. DO WE COLLECT INFORMATION FROM MINORS?

We do not knowingly collect or solicit data from, or market to, children under 18 years of age. By using the Website and/or Services, you represent that you are at least 18 or that you are the parent or guardian of such a minor and consent to such minor dependent’s use of the Website. If we learn that personal information from users less than 18 years of age has been collected, we will deactivate the account and take reasonable measures to promptly delete such data from our records. Please contact us at the contact information below if you become aware of any data we may have collected from children under age 18.

8. WHAT ARE YOUR PRIVACY RIGHTS?

Opting Out of Marketing Communications

If you have requested information from us, we may send you e-mail communications with information about our Services. We will include instructions in each marketing e-mail message explaining how to unsubscribe from our marketing e-mail communications if you do not want to receive these in the future. At any time, you can opt out of receiving marketing communications from us by making such request by email to the contact information provided below. Please note that if you opt-out of marketing communications you may still receive transactional and legal communications from us.

You may limit the use of your browsing activities and interests for interest-based advertising by clicking http://optout.aboutads.info/ (or if located in the European Union, click http://www.youronlinechoices.edu/). Note that opting out of interest-based advertising through these tools does not opt you out of being served ads. You will continue to receive ads, but they are unlikely to be personalized to you. To learn more, please review our Cookie Policy Attached hereto as Exhibit A.

If you are a resident in the EEA or UK and you believe we are unlawfully processing your personal information, you also have the right to file a complaint with your local data protection supervisory authority. You can find their contact details here: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm. If you are a resident of Switzerland, the contact information for the data protection authority is available here: https://www.edoeb.admin.ch/edoeb/en/home.html.

Account Information

If you are a customer of ours, you may review or change the information in your account, or terminate your account, at any time by logging in and updating your account accordingly. In the event you request to terminate your account, we will deactivate and/or delete your account and personal information from our active databases in accordance with this Policy and the applicable agreement for Services.
9. CONTROLS FOR DO-NOT-TRACK FEATURES

Tracking Technologies Generally. Regular cookies may generally be disabled or removed by tools available as part of most commercial browsers, and in some instances blocked in the future by selecting certain settings. Browsers offer different functionalities and options, so you may need to set them separately. Also, tools from browsers may not be effective with regard to certain Tracking Technologies. Please be aware that if you disable or remove these technologies, some parts of the Website or Services may not work as intended. Additionally, your ability to limit browser-based Tracking Technologies is subject to your browser settings and limitations.

Some App-related Tracking Technologies in connection with non-browser usage (e.g., most functionality of a mobile app) can only be disabled by uninstalling the app. To uninstall an app, follow the instructions from your operating system or handset manufacturer. Apple and Google mobile device settings have settings to limit ad tracking, and other tracking, but these may not be completely effective.

Your browser settings may allow you to automatically transmit a “Do Not Track” signal to online Websites you visit. Like many online services and websites, we currently do not alter our practices when we receive a “Do Not Track” signal from a visitor’s browser. To find out more about “Do Not Track,” you can visit http://www.allaboutdnt.com, but we are not responsible for the completeness or accuracy of this third-party information. For specific information on some of the choice options offered by third party analytics and advertising providers, see the next section.

Analytics and Advertising Tracking Technologies. You may exercise choices regarding the use of cookies from Google Analytics by going to https://tools.google.com/dlpage/gaoptout or downloading the Google Analytics Opt-out Browser Add-on. You may exercise choices regarding the use of cookies from Adobe Analytics by going to http://www.adobe.com/privacy/opt-out.html under the section labeled “Tell our customers not to measure your use of their web sites or tailor their online ads for you.”

You may choose whether to receive some Interest-based Advertising by submitting opt-outs. Some of the advertisers and Service Providers that perform advertising-related Websites for us and third parties may participate in the Digital Advertising Alliance’s (“DAA”) Self-Regulatory Program for Online Behavioral Advertising. To learn more about how you can exercise certain choices regarding interest-based Advertising, including use of Cross-device Data for serving ads, visit http://www.aboutads.info/choices/, and http://www.aboutads.info/appchoices for information on the DAA’s opt-out program specifically for mobile apps (including use of precise location for third party ads). Some of these companies may also be members of the Network Advertising Initiative (“NAI”). To learn more about the NAI and your opt-out options for their members, see http://www.networkadvertising.org/choices/. Please be aware that, even if you are able to opt out of certain kinds of interest-based advertising, you may continue to receive other types of ads. Opting out only means that those selected members should no longer deliver certain interest-based advertising to you but does not mean you will no longer receive any targeted content and/or ads (e.g., from other ad networks). Also, if your browsers are configured to reject cookies when you visit these opt-out webpages, or you subsequently erase your cookies, use a different device or web browser or use a non-browser-based method of access (e.g., mobile app), your NAI / DAA browser-based opt-out may not, or may no longer, be effective. We support the ad industry’s Self-regulatory Principles for Online Behavioral Advertising and expect that ad networks we directly engage to serve you interest-based advertising will do so as well, though we cannot guaranty their compliance.
We may also use Google Ad Websites. To learn more about the data Google collects and how your data is used by it and to opt out of certain Google browser interest-based advertising, please visit http://www.google.com/settings/ads

10. AUTHORIZED SERVICE PROVIDERS

We may subcontract any processing of your personal data to our third-party subcontractors ("Service Provider/s") in accordance with applicable data protection law. Attached hereto as Exhibit B is a list of our current Service Providers.

The provisions in the bullets immediately below only apply (i) if you are a customer of our Services, and (ii) to the personal information collected by us pursuant to our agreement with you for such Services:

• We will not subcontract with any Service Providers for Services that include direct or indirect access to, storage or processing of, or other contact with your personal information, without first providing notice and obtaining your prior consent.

• In the event we make available an online list of our current Sub-Processors and a mechanism to subscribe to list update notifications, you agree to subscribe to such update notifications mechanism. At least ten (10) days before enabling any third party other than existing authorized Sub-Processors to access or participate in the processing of personal information, we will add such Service Provider to the List and notify you via email. You may object to such an engagement by informing us within ten (10) days of receipt of the aforementioned notice, provided such objection is in writing and based on reasonable grounds relating to data protection. You acknowledge that certain Service Providers are essential to providing the Services and that objecting to our use of a sub-processor may prevent us from offering the Services to you.

• If you reasonably object to an engagement in accordance with the provision immediately above, and we cannot provide a commercially reasonable alternative within a reasonable period of time, you may discontinue the use of the affected Service by providing written notice to us. Discontinuation shall not relieve you of any fees owed to us under the applicable agreement for Services.

• If you do not object to the engagement of a third party in accordance with this section within ten (10) days of notice, that subcontractor will be deemed an authorized Service Provider for the purposes of this Policy.

• We will enter into a written agreement with the authorized Service Providers imposing on them data protection obligations comparable to those imposed on us under this Policy and our agreement for Services with you with respect to the protection of personal information. In case an authorized Sub-Processor fails to fulfill its data protection obligations under such written agreement with us, we will remain liable to you for the performance of the authorized Service Provider’s obligations under such agreement.

11. HOW CAN YOU CONTACT US ABOUT THIS NOTICE?

If you have questions or comments about this Policy and/or your privacy rights, please email us at privacy@mxdusa.org or send postal mail to:
12. DO WE MAKE UPDATES TO THIS POLICY?

Yes, we may update this Policy from time to time, and as necessary to stay compliant with relevant laws. The updated version will be indicated by an updated "Last Updated" date and the updated version will be effective as soon as it is accessible. If we make material changes to this Policy, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this Policy frequently to be informed of how we are protecting your information.

13. STATE PRIVACY RIGHTS

If your state of residence has privacy laws related to your personal information, and you have questions or would like to exercise such rights, please refer to your applicable state’s Privacy Statement section below:

If there is no Privacy Statement section listed for your state, that means no additional privacy rights, beyond current federal statutes or regulations, exist within your state at this time.

The state Privacy Statements below includes California, Colorado, Connecticut, Utah, and Virginia.

**PRIVACY STATEMENT – CALIFORNIA**

This PRIVACY NOTICE FOR CALIFORNIA RESIDENTS supplements the information contained in the MxD Privacy Policy and applies solely to those who reside in the State of California (“consumers” or “you”). UI LABS d/b/a MXD USA (“MxD,” “we,” or “us”) adopt this notice to comply with the California Consumer Privacy Act of 2018 and its implementing regulations, as amended by the California Privacy Rights Act (“CPRA”). Any terms defined in the CPRA have the same meaning when used in this statement.

**Note that we never sell your personal information. We also do not disclose your personal information unless permitted or required by law or contract.**

**Information We Collect**

We collect personal information. For purposes of the CPRA, personal information is information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked directly or indirectly with a particular consumer or device. In particular, we’ve collected for a business purpose, the following categories of personal information from consumers within the last 12 months:

1. A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.
2. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)). A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.

3. Protected classification characteristics under California or federal law. Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).

4. Commercial information. Records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

5. Internet or other similar network activity. Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.

6. Professional or employment-related information. Current or past job history; employer names and addresses.

7. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)). Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.

8. Inferences drawn from other personal information, which may include person's preferences, characteristic and predispositions.

9. Sensitive personal information Social security, driver's license, state identification card, or passport number; account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; union membership; contents of a consumer's mail, email, and text messages.

In the preceding twelve (12) months, we have not sold or shared any personal information, including personal information of individuals under the age of 16.

The categories of personal information noted above are obtained from the following categories of sources:

- Directly from our clients or their agents. For example, from documents that our clients provide to us related to the services for which they engage us.
- Indirectly from our clients or their agents. For example, through information we collect from our clients in the course of providing services to them.
- Directly and indirectly from activity on our websites. For example, from submissions through our website portal or website usage details collected automatically.
- From third parties that interact with us in connection with the services we perform for you. For example, from affiliated institutions that provide specified financial service products.
Use of Personal Information

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

- To provide you with information, products, or services that you request from us. For example, if we receive your personal information in order for us to maintain or administer your retirement or educational savings plan, we will use that information to provide you those services.
- To provide you with email alerts, event registrations and other notices concerning our products or services, or events or news, that may be of interest to you.
- To carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collections.
- To maintain and improve our website.
- To protect the rights, property or safety of MxD, our clients or others as is necessary or appropriate.
- To respond to law enforcement requests and as required by applicable law, rule, regulation, court order, or governmental regulations.
- To fulfill or meet the reason for which the information is provided.
- As described to you when collecting your personal information or as otherwise set forth in the CPRA.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, or similar proceeding, in which personal information held by us is among the assets transferred.

We won’t collect additional categories of personal information or use the personal information collected for materially different, unrelated, or incompatible purposes without providing you notice. Notice will be in the form of an update to this Policy.

Note that the following information is excluded from the scope of the CPRA:

- Publicly available information from government records (if used for a purpose compatible with the purpose for which the data is maintained and made available in the government records).
- De-identified or aggregated consumer information. De-identified information is information that can’t reasonably identify, relate to, or describe a particular consumer. In other words, the information can’t be traced to any particular person. Aggregated information is information about a group of consumers from which individual consumer identities have been removed.
- Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data; and
- Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver’s Privacy Protection Act of 1994.

Disclosing Personal Information

In order to effectively deliver our services to you, your personal information may be disclosed to a third party for a business purpose, in accordance with the Information We Collect section above. This may
include but not be limited to (i) our affiliates; (ii) service providers (e.g., a print vendor with responsibility to produce and/or mail paper statements and notices; or (iii) the applicable custodial banking institutions who hold your money); and third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.

Prior to any such disclosure to any third party, we require an executed contract that describes the specified purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose, except to perform the specific services stated within such contract.

Retention of Personal Information

We will retain each category of your personal information for as long as necessary to fulfill the purposes described in the “Use of Personal Information” section above, unless otherwise required by applicable laws. Criteria we will use to determine how long we will retain your information include whether: we need your information to provide you with products or services you have requested; we continue to have a relationship with you; you have requested information, products, or services from us; we have a legal right or obligation to continue to retain your information; we have an obligation to a third party that involves your information; our retention or recordkeeping policies and obligations dictate that we retain your information; we have an interest in providing you with information about our products or services; and we have another business purpose for retaining your information.

Your Rights and Choices

California law provides California residents with specific rights regarding their personal information. This section describes your California privacy rights and explains how to exercise those rights.

Access to Specific Information and Data Portability Rights

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and verify your request, we’ll disclose specific information to you as it relates to your account regarding:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting that personal information.
- The categories of third parties with whom we share that personal information.
- The specific items of personal information we collected about you which are subject to such disclosure.

Correction Request Rights

You have the right to request correction of any inaccurate personal information, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we’ll correct (and direct our service providers to correct) your personal information, unless an exception applies. Accordingly, we may deny your correction request if:

1. We cannot verify your identity.
2. We believe a request is fraudulent or abusive.
3. We are not the source of the personal information that you believe is inaccurate. In such cases, we will provide you the name of the source from which received the personal information.

**Deletion Request Rights**

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we’ll delete (and direct our service providers to delete) your personal information from our records, unless an exception applies. Accordingly, we may deny your deletion request if retaining the information is necessary for us or our service providers to:

1. Complete the transaction for which we collected the personal information, provide a good or service that you requested or that a third party requested on your behalf, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you or the sponsor of your plan or account.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Debug products to identify and repair errors that impair existing intended functionality.
4. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 seq.).
5. Comply with a legal obligation.
6. Make other internal and lawful uses of that information that are compatible with the context in which you provided the information.

**Opt Out of the Sale/Sharing of Your Personal Information**

The CPRA provides California consumers with the right to opt-out of the sale of their personal information to third parties. The CPRA defines “sale” or “sell” as disclosing or making available to a third-party personal information in exchange for monetary or other valuable consideration. We do not sell your personal information.

**Sensitive Personal Information**

Where we collect sensitive personal information about you, we only use it provide our products and services to you. California consumers also have the right to opt-out of the sharing of their personal information. MxD does not share your personal information as that term is defined under CPRA.

**Exercising Your Rights**

To receive access to your personal information or exercise your other rights:

**Method 1**

To access your personal information, please log into your existing account profile within the applicable secure portal, which enables you to view your account balance and other associated personal details.

**Method 2**

For general inquiries or requests with respect to your rights under CPRA, please submit a request to one of the following options:

Phone: 312-281-6900
Email Address: Privacy@mxdusa.org

Address: 1415 N. Cherry Ave., Chicago, IL 60642, Attention: Compliance Department

Please note that we’ll need to verify your identity before we can discuss your request any details about your account. Only you or an authorized agent registered with the California Secretary of State that you authorize to act on your behalf may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child. If you are an authorized agent making a request on behalf of a California resident, we will also need to verify your identity, which may require proof of your written authorization or evidence of a power of attorney.

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

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

We cannot respond to your request or provide you with any personal information if we cannot verify your identity or if we determine that you do not have the authority to make the request or confirm the personal information relates to you. Making a verifiable consumer request does not require you to create an account with us. To verify a consumer request, we’ll only use personal information previously provided to us to verify the requestor’s identity and authority to make the request.

Response Timing and Format

We try to respond to a verifiable consumer request within 45 days. If we require more time (up to 90 days), we’ll inform you of the reason and extension period in writing. If you have an account with us, we’ll deliver our written response to the address on record for that account. If you do not have an account with us, we’ll deliver our written response by mail or electronically. Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request’s receipt. The response we provide will also explain the reasons why we can’t comply with a request, if applicable, and instructions on how to appeal the decision. For data portability requests, we’ll select a format to provide your personal information that is secure and readily usable and should allow you to transmit the information from one entity to another entity without hindrance.

Generally, we don’t charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine the request warrants a fee, we’ll tell you why that decision was made and provide you with a cost estimate before completing your request.

Non-Discrimination

We won’t discriminate against any California resident in the exercise of their CPRA rights. Unless permitted by the CPRA, we won’t do any of the following solely because you exercised your CPRA rights:

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

PRIVACY STATEMENT – COLORADO

This PRIVACY NOTICE FOR COLORADO RESIDENTS supplements the information contained in the MxD Privacy Policy and applies solely to those who reside in the State of Colorado (“you”). UI LABS d/b/a MxD USA (“MxD,” “we,” or “us”) adopt this notice to comply with the Colorado Privacy Act.

Note that we never sell your personal information. We also do not disclose your personal information unless permitted or required by law or contract.

Information We Collect

We collect personal information in accordance with our Privacy Policy.

We do not sell personal information.

Use of Personal Information

We use personal information in accordance with our Privacy Policy.

We won’t collect additional categories of personal information or use the personal information collected for materially different, unrelated, or incompatible purposes without providing you notice. Notice will be in the form of an update to this Policy.

Note that the following information is excluded from the scope of the above state laws:

• Publicly available information from government records (if used for a purpose compatible with the purpose for which the data is maintained and made available in the government records).
• De-identified or aggregated consumer information. De-identified information is information that can’t reasonably identify, relate to, or describe a particular consumer. In other words, the information can’t be traced to any particular person. Aggregated information is information about a group of consumers from which individual consumer identities have been removed.
• Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or clinical trial data; and
• Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA), and the Driver’s Privacy Protection Act of 1994.

Disclosing Personal Information

We disclose personal information in accordance with our Privacy Policy.

Prior to any such disclosure to any third party, we require an executed contract that describes the specified purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose, except to perform the specific services stated within such contract.
Your Rights and Choices

If you reside in Colorado, you have specific rights regarding your personal information. This section describes your privacy rights and explains how to exercise those rights.

Access to Specific Information and Data Portability Rights

You have the right to request that we disclose certain information to you about our collection and use of your personal information. Once we receive and verify your request, we’ll disclose specific information to you as it relates to your account.

Correction Request Rights

You have the right to request correction of any inaccurate personal information, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we’ll correct (and direct our service providers to correct) your personal information, unless an exception applies. Accordingly, we may deny your correction request if:

1. We cannot verify your identity.
2. We believe a request is fraudulent or abusive.
3. We are not the source of the personal information that you believe is inaccurate. In such cases, we will provide you the name of the source from which received the personal information.

Deletion Request Rights

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we’ll delete (and direct our service providers to delete) your personal information from our records, unless an exception applies. Accordingly, we may deny your deletion request if retaining the information is necessary for us or our service providers to:

1. Complete the transaction for which we collected the personal information, provide a good or service that you requested or that a third party requested on your behalf, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you or the sponsor of your plan or account.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Debug products to identify and repair errors that impair existing intended functionality.
5. Make other internal and lawful uses of that information that are compatible with the context in which you provided the information.

Opt Out of Profiling and Targeted Advertising

In addition, you have the right to opt out of targeted advertising and profiling, to the extent that profiling makes decisions that produce legal or similarly significant effects concerning you. MxD does not engage in targeted advertising or profiling as such terms are defined under Colorado Privacy Act. To the extent we do profile you, it will be related to our legal obligations under applicable financial laws and regulations (i.e., know your customer requirements).
Exercising Your Rights

To receive access to your personal information or exercise your other rights:

**Method 1**

To access your personal information, please log into your existing account profile within the applicable secure portal, which enables you to view your account balance and other associated personal details.

**Method 2**

For general inquiries or requests with respect to your rights, please submit a request to one of the following options:

Phone: 312-281-6900

Email Address: Privacy@mxdusa.org

Address: 1415 N. Cherry Ave., Chicago, IL 60642, Attention: Compliance Department

Please note that we’ll need to verify your identity before we can discuss your request any details about your account. Only you or an authorized agent that you authorize to act on your behalf may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child. If you are an authorized agent making a request on behalf of an individual, we will also need to verify your identity, which may require proof of your written authorization or evidence of a power of attorney.

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

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

We cannot respond to your request or provide you with any personal information if we cannot verify your identity or if we determine that you do not have the authority to make the request or confirm the personal information relates to you. Making a verifiable consumer request does not require you to create an account with us. To verify a consumer request, we’ll only use personal information previously provided to us to verify the requestor's identity and authority to make the request.

**Response Timing and Format**

We try to respond to a verifiable consumer request within 45 days. If we require more time (up to 90 days), we’ll inform you of the reason and extension period in writing. If you have an account with us, we’ll deliver our written response to the address on record for that account. If you do not have an account with us, we’ll deliver our written response by mail or electronically. Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request’s receipt. The response we provide will also explain the reasons why we can’t comply with a request, if applicable, and instructions on how to appeal the decision. For data portability requests, we’ll select a format to provide
your personal information that is secure and readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

Generally, we don’t charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine the request warrants a fee, we’ll tell you why that decision was made and provide you with a cost estimate before completing your request.

Non-Discrimination

We won’t discriminate against you for exercising your rights. Unless permitted, we won’t do any of the following solely because you exercised your rights:

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

Sensitive Personal Information

Where we collect sensitive personal information about you, we will only do so to perform a contracted service.

PRIVACY STATEMENT – CONNECTICUT

This PRIVACY NOTICE FOR CONNECTICUT RESIDENTS supplements the information contained in the MxD Privacy Policy and applies solely to those who reside in the State of Connecticut (“you”). UI LABS d/b/a MXD USA (“MxD,” “we,” or “us”) adopt this notice to comply with the Connecticut Act Concerning Personal Data Privacy and Online Monitoring.

Note that we never sell your personal information. We also do not disclose your personal information unless permitted or required by law or contract.

Information We Collect

We collect personal information in accordance with our Privacy Policy.

We do not sell personal information.

Use of Personal Information

We use personal information in accordance with our Privacy Policy.

We won’t collect additional categories of personal information or use the personal information collected for materially different, unrelated, or incompatible purposes without providing you notice. Notice will be in the form of an update to this Policy.

Note that the following information is excluded from the scope of the above state laws:
• Publicly available information from government records (if used for a purpose compatible with the purpose for which the data is maintained and made available in the government records).
• De-identified or aggregated consumer information. De-identified information is information that can’t reasonably identify, relate to, or describe a particular consumer. In other words, the information can’t be traced to any particular person. Aggregated information is information about a group of consumers from which individual consumer identities have been removed.
• Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or clinical trial data; and
• Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA), and the Driver’s Privacy Protection Act of 1994.

Disclosing Personal Information

We disclose personal information in accordance with our Privacy Policy.

Prior to any such disclosure to any third party, we require an executed contract that describes the specified purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose, except to perform the specific services stated within such contract.

Your Rights and Choices

If you reside in Connecticut, you have specific rights regarding your personal information. This section describes your privacy rights and explains how to exercise those rights.

Access to Specific Information and Data Portability Rights

You have the right to request that we disclose certain information to you about our collection and use of your personal information. Once we receive and verify your request, we’ll disclose specific information to you as it relates to your account.

Correction Request Rights

You have the right to request correction of any inaccurate personal information, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we’ll correct (and direct our service providers to correct) your personal information, unless an exception applies. Accordingly, we may deny your correction request if:

1. We cannot verify your identity.
2. We believe a request is fraudulent or abusive.
3. We are not the source of the personal information that you believe is inaccurate. In such cases, we will provide you the name of the source from which received the personal information.

Deletion Request Rights

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we’ll delete (and direct our service providers to delete) your personal information from our records, unless an exception applies. Accordingly, we may deny your deletion request if retaining the information is necessary for us or our service providers to:
1. Complete the transaction for which we collected the personal information, provide a good or service that you requested or that a third party requested on your behalf, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you or the sponsor of your plan or account.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Debug products to identify and repair errors that impair existing intended functionality.
5. Make other internal and lawful uses of that information that are compatible with the context in which you provided the information.

Opt Out of Profiling and Targeted Advertising

In addition, you have the right to opt out of targeted advertising and profiling, to the extent that profiling makes decisions that produce legal or similarly significant effects concerning you. MxD does not engage in targeted advertising and profiling as such terms are defined under the Connecticut Act Concerning Personal Data Privacy and Online Monitoring. To the extent we do profile you, it will be related to our legal obligations under applicable financial laws and regulations (i.e., know your customer requirements).

Exercising Your Rights

To receive access to your personal information or exercise your other rights:

Method 1

To access your personal information, please log into your existing account profile within the applicable secure portal, which enables you to view your account balance and other associated personal details.

Method 2

For general inquiries or requests with respect to your rights, please submit a request to one of the following options:

Phone: 312-281-6900

Email Address: Privacy@mxdusa.org

Address: 1415 N. Cherry Ave., Chicago, IL 60642, Attention: Compliance Department

Please note that we’ll need to verify your identity before we can discuss your request any details about your account. Only you or an authorized agent that you authorize to act on your behalf may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child. If you are an authorized agent making a request on behalf of an individual, we will also need to verify your identity, which may require proof of your written authorization or evidence of a power of attorney.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must:
• Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative; and
• Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with any personal information if we cannot verify your identity or if we determine that you do not have the authority to make the request or confirm the personal information relates to you. Making a verifiable consumer request does not require you to create an account with us. To verify a consumer request, we’ll only use personal information previously provided to us to verify the requestor’s identity and authority to make the request.

Response Timing and Format

We try to respond to a verifiable consumer request within 45 days. If we require more time (up to 90 days), we’ll inform you of the reason and extension period in writing. If you have an account with us, we’ll deliver our written response to the address on record for that account. If you do not have an account with us, we’ll deliver our written response by mail or electronically. Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request’s receipt. The response we provide will also explain the reasons why we can’t comply with a request, if applicable, and instructions on how to appeal the decision. For data portability requests, we’ll select a format to provide your personal information that is secure and readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

Generally, we don’t charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine the request warrants a fee, we’ll tell you why that decision was made and provide you with a cost estimate before completing your request.

Non-Discrimination

We won’t discriminate against you for exercising your rights. Unless permitted, we won’t do any of the following solely because you exercised your rights:

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

Sensitive Personal Information

Where we collect sensitive personal information about you, we will only do so to perform a contracted service.
This PRIVACY NOTICE FOR UTAH RESIDENTS supplements the information contained in the MxD Privacy Policy and applies solely to those who reside in the State of Utah (“you”). UI LABS d/b/a MXD USA (“MxD,” “we,” or “us”) adopt this notice to comply with the Utah Consumer Privacy Act.

**Note that we never sell your personal information. We also do not disclose your personal information unless permitted or required by law or contract.**

**Information We Collect**

We collect personal information in accordance with our Privacy Policy.

**We do not sell personal information.**

**Use of Personal Information**

We use personal information in accordance with our Privacy Policy.

We won’t collect additional categories of personal information or use the personal information collected for materially different, unrelated, or incompatible purposes without providing you notice. Notice will be in the form of an update to this Policy.

Note that the following information is excluded from the scope of the above state laws:

- Publicly available information from government records (if used for a purpose compatible with the purpose for which the data is maintained and made available in the government records).
- De-identified or aggregated consumer information. De-identified information is information that can’t reasonably identify, relate to, or describe a particular consumer. In other words, the information can’t be traced to any particular person. Aggregated information is information about a group of consumers from which individual consumer identities have been removed.
- Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or clinical trial data; and
- Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA), and the Driver’s Privacy Protection Act of 1994.

**Disclosing Personal Information**

We disclose personal information in accordance with our Privacy Policy.

Prior to any such disclosure to any third party, we require an executed contract that describes the specified purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose, except to perform the specific services stated within such contract.

**Your Rights and Choices**

If you reside in Utah, you have specific rights regarding your personal information. This section describes your privacy rights and explains how to exercise those rights.
Access to Specific Information and Data Portability Rights

You have the right to request that we disclose certain information to you about our collection and use of your personal information. Once we receive and verify your request, we’ll disclose specific information to you as it relates to your account.

Correction Request Rights

You have the right to request correction of any inaccurate personal information, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we’ll correct (and direct our service providers to correct) your personal information, unless an exception applies. Accordingly, we may deny your correction request if:

1. We cannot verify your identity.
2. We believe a request is fraudulent or abusive.
3. We are not the source of the personal information that you believe is inaccurate. In such cases, we will provide you the name of the source from which received the personal information.

Deletion Request Rights

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we’ll delete (and direct our service providers to delete) your personal information from our records, unless an exception applies. Accordingly, we may deny your deletion request if retaining the information is necessary for us or our service providers to:

1. Complete the transaction for which we collected the personal information, provide a good or service that you requested or that a third party requested on your behalf, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you or the sponsor of your plan or account.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Debug products to identify and repair errors that impair existing intended functionality.
5. Make other internal and lawful uses of that information that are compatible with the context in which you provided the information.

Opt Out of Profiling and Targeted Advertising

In addition, you have the right to opt out of targeted advertising and profiling, to the extent that profiling makes decisions that produce legal or similarly significant effects concerning you. MxD does not engage in targeted advertising or profiling as such terms are defined under Utah Consumer Privacy Act. To the extent we do profile you, it will be related to our legal obligations under applicable financial laws and regulations (i.e., know your customer requirements).

Exercising Your Rights

To receive access to your personal information or exercise your other rights:
**Method 1**

To access your personal information, please log into your existing account profile within the applicable secure portal, which enables you to view your account balance and other associated personal details.

**Method 2**

For general inquiries or requests with respect to your rights, please submit a request to one of the following options:

Phone: 312-281-6900

Email Address: Privacy@mxdusa.org

Address: 1415 N. Cherry Ave., Chicago, IL 60642, Attention: Compliance Department

Please note that we’ll need to verify your identity before we can discuss your request any details about your account. Only you or an authorized agent that you authorize to act on your behalf may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child. If you are an authorized agent making a request on behalf of an individual, we will also need to verify your identity, which may require proof of your written authorization or evidence of a power of attorney.

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

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

We cannot respond to your request or provide you with any personal information if we cannot verify your identity or if we determine that you do not have the authority to make the request or confirm the personal information relates to you. Making a verifiable consumer request does not require you to create an account with us. To verify a consumer request, we’ll only use personal information previously provided to us to verify the requestor's identity and authority to make the request.

**Response Timing and Format**

We try to respond to a verifiable consumer request within 45 days. If we require more time (up to 90 days), we’ll inform you of the reason and extension period in writing. If you have an account with us, we’ll deliver our written response to the address on record for that account. If you do not have an account with us, we’ll deliver our written response by mail or electronically. Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons why we can’t comply with a request, if applicable, and instructions on how to appeal the decision. For data portability requests, we’ll select a format to provide your personal information that is secure and readily useable and should allow you to transmit the information from one entity to another entity without hindrance.
Generally, we don’t charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine the request warrants a fee, we’ll tell you why that decision was made and provide you with a cost estimate before completing your request.

**Non-Discrimination**

We won’t discriminate against you for exercising your rights. Unless permitted, we won’t do any of the following solely because you exercised your rights:

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

**Sensitive Personal Information**

Where we collect sensitive personal information about you, we will only do so to perform a contracted service.

---

**PRIVACY STATEMENT – VIRGINIA**

This PRIVACY NOTICE FOR VIRGINIA RESIDENTS supplements the information contained in the MxD Privacy Policy and applies solely to those who reside in the State of Virginia (“you”). UI LABS d/b/a MXD USA (“MxD,” “we,” or “us”) adopt this notice to comply with the Virginia Consumer Data Protection Act.

**Note that we never sell your personal information. We also do not disclose your personal information unless permitted or required by law or contract.**

**Information We Collect**

We collect personal information in accordance with our Privacy Policy.

**We do not sell personal information.**

**Use of Personal Information**

We use personal information in accordance with our Privacy Policy.

We won’t collect additional categories of personal information or use the personal information collected for materially different, unrelated, or incompatible purposes without providing you notice. Notice will be in the form of an update to this Policy.

Note that the following information is excluded from the scope of the above state laws:

- Publicly available information from government records (if used for a purpose compatible with the purpose for which the data is maintained and made available in the government records).
• De-identified or aggregated consumer information. De-identified information is information that can’t reasonably identify, relate to, or describe a particular consumer. In other words the information can’t be traced to any particular person. Aggregated information is information about a group of consumers from which individual consumer identities have been removed.

• Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or clinical trial data; and

• Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA), and the Driver’s Privacy Protection Act of 1994.

**Disclosing Personal Information**

We disclose personal information in accordance with our Privacy Policy.

Prior to any such disclosure to any third party, we require an executed contract that describes the specified purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose, except to perform the specific services stated within such contract.

**Your Rights and Choices**

If you reside in Virginia, you have specific rights regarding your personal information. This section describes your privacy rights and explains how to exercise those rights.

**Access to Specific Information and Data Portability Rights**

You have the right to request that we disclose certain information to you about our collection and use of your personal information. Once we receive and verify your request, we’ll disclose specific information to you as it relates to your account.

**Correction Request Rights**

You have the right to request correction of any inaccurate personal information, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we’ll correct (and direct our service providers to correct) your personal information, unless an exception applies. Accordingly, we may deny your correction request if:

1. We cannot verify your identity.
2. We believe a request is fraudulent or abusive.
3. We are not the source of the personal information that you believe is inaccurate. In such cases, we will provide you the name of the source from which received the personal information.

**Deletion Request Rights**

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we’ll delete (and direct our service providers to delete) your personal information from our records, unless an exception applies. Accordingly, we may deny your deletion request if retaining the information is necessary for us or our service providers to:
1. Complete the transaction for which we collected the personal information, provide a good or service that you requested or that a third party requested on your behalf, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you or the sponsor of your plan or account.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Debug products to identify and repair errors that impair existing intended functionality.
5. Make other internal and lawful uses of that information that are compatible with the context in which you provided the information.

Opt Out of Profiling and Targeted Advertising

In addition, you have the right to opt out of targeted advertising and profiling, to the extent that profiling makes decisions that produce legal or similarly significant effects concerning you. MxD does not engage in target advertising or profiling as such terms are defined under Virginia Consumer Data Protection Act. To the extent we do profile you, it will be related to our legal obligations under applicable financial laws and regulations (i.e., know your customer requirements).

Exercising Your Rights

To receive access to your personal information or exercise your other rights:

Method 1

To access your personal information, please log into your existing account profile within the applicable secure portal, which enables you to view your account balance and other associated personal details.

Method 2

For general inquiries or requests with respect to your rights, please submit a request to one of the following options:

Phone: 312-281-6900

Email Address: Privacy@mxdusa.org

Address: 1415 N. Cherry Ave., Chicago, IL 60642, Attention: Compliance Department

Please note that we’ll need to verify your identity before we can discuss your request or any details about your account. Only you or an authorized agent that you authorize to act on your behalf may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child. If you are an authorized agent making a request on behalf of an individual, we will also need to verify your identity, which may require proof of your written authorization or evidence of a power of attorney.

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

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

We cannot respond to your request or provide you with any personal information if we cannot verify your identity or if we determine that you do not have the authority to make the request or confirm the personal information relates to you. Making a verifiable consumer request does not require you to create an account with us. To verify a consumer request, we’ll only use personal information previously provided to us to verify the requestor’s identity and authority to make the request.

Response Timing and Format

We try to respond to a verifiable consumer request within 45 days. If we require more time (up to 90 days), we’ll inform you of the reason and extension period in writing. If you have an account with us, we’ll deliver our written response to the address on record for that account. If you do not have an account with us, we’ll deliver our written response by mail or electronically. Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request’s receipt. The response we provide will also explain the reasons why we can’t comply with a request, if applicable, and instructions on how to appeal the decision. For data portability requests, we’ll select a format to provide your personal information that is secure and readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

Generally, we don’t charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine the request warrants a fee, we’ll tell you why that decision was made and provide you with a cost estimate before completing your request.

Non-Discrimination

We won’t discriminate against you for exercising your rights. Unless permitted, we won’t do any of the following solely because you exercised your rights:

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

Sensitive Personal Information

Where we collect sensitive personal information about you, we will only do so to perform a contracted service.
What are Cookies?

A cookie is a message that, subject to your settings, is sent to its terminal when you navigate on a website. The aim is to collect data regarding your internet navigation to send tailor-made services to its terminal (computer, mobile phone or tablet).

How does the Website use Cookies?

MxD and third parties use a tracking technology on its member portal, such as cookies, whenever the navigate throughout the Website. Cookies may be created and stored by the Website you are visiting (first-party cookie) or by third parties, such as those who serve content or analytics services on the Site (third-party cookies).

Categories of Cookies:

Strictly Necessary

These cookies are essential for the Website to perform its basic functions. The Website cannot function properly without these cookies. The user cannot refuse strictly necessary cookies.

<table>
<thead>
<tr>
<th>Service</th>
<th>Name</th>
<th>Purpose</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hivebrite</td>
<td>_alumni_connect_session</td>
<td>[Ex: Allow registered Users to authenticate and perform account related functions]</td>
<td>Session</td>
</tr>
<tr>
<td>Hivebrite</td>
<td>Cookies_consent_list</td>
<td>To record which cookies the user gives consent for</td>
<td>6 Months</td>
</tr>
<tr>
<td>Hivebrite</td>
<td>first_user_experience</td>
<td>To identify if it is the first connection of the user</td>
<td>Session</td>
</tr>
<tr>
<td>Hivebrite</td>
<td>remember_user_token</td>
<td>Allows the user session to remain active, without asking you to connect again</td>
<td>1 Year</td>
</tr>
</tbody>
</table>
### Social Network functional cookies

If you elect to link to social media, the Website uses social network functional cookies to enable functionality linked to third party social network cookies on the platform. These cookies enable to display third party features to the user, such as the Twitter and Facebook feeds/posts. These cookies may interact with the Twitter and/or Facebook account of the user.

<table>
<thead>
<tr>
<th>Service</th>
<th>Name</th>
<th>Purpose</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>fr</td>
<td>Displaying Facebook feeds/posts in the Live Feed of the Website</td>
<td>3 months</td>
</tr>
<tr>
<td>Twitter</td>
<td>LANG, Metrics_token, Personalization_id, Tfw_exp</td>
<td>Displaying Twitter feeds/posts in the Live Feed of the Website</td>
<td>Session 48 days, 2 years, 2 weeks</td>
</tr>
</tbody>
</table>

### Analytics and Performance

Analytical cookies help the MxD to understand how visitors gain access to or interact with the Website. These cookies collect information on how users interact with the Website and create statistics about the use of the Website. MxD uses these cookies to determine the kind of content and services the users value most, which in turn helps MxD to improve the quality of service proposed by the Website and usage as well as functionalities.

<table>
<thead>
<tr>
<th>Service</th>
<th>Name</th>
<th>Purpose</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Analytics</td>
<td>_gat_hivebriteTracker</td>
<td>For tracking the traffic</td>
<td>1 minute</td>
</tr>
</tbody>
</table>
| Google Analytics | • _ga  
|                 | • _gat  
|                 | • _gid  
| For tracking the traffic | 2 years  
|                   | 1 minutes  
|                   | 1 year  |

Cookies for admins only – Strictly Necessary

<table>
<thead>
<tr>
<th>Service</th>
<th>Name</th>
<th>Purpose</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hivebrite</td>
<td>Remember_backoffice_admin_token</td>
<td>Allows the admin session to remain active without asking you to connect again</td>
<td>Session</td>
</tr>
<tr>
<td>Hivebrite</td>
<td>Search_path</td>
<td>Used for the user search in the BO and when you assign user to a role</td>
<td>Session</td>
</tr>
</tbody>
</table>

Controlling Cookies

For cookies for which it is required to collect consent, you are informed of the purpose of these cookies and are given the ability to consent or refuse through a banner at the bottom of the Website homepage. After customizing their cookies settings, you are able to reselect your preferences at any time. From the Public Pages, this is possible by clicking ‘Reselect cookie consent’ in the footer. From the Front Office, you can do this in Settings > Privacy > Cookies > Reselect settings. In both of these cases, the your nonrequired cookies are destroyed, and the page refreshes, allowing you to select which cookies you accept.

To opt out of being tracked by Google Analytics across all websites, please visit https://tools.google.com/dlpage/gaoptout. On this website you’ll find information about a browser plugin that can be installed to prevent your data from being used by Google Analytics.

For cookies that do not require consent, you may at all times configure your navigator in order to prevent the creation of cookie files. However, certain functionalities of the services proposed by the Website may not function properly without cookies. In addition, even if most navigators are configured by default and accept the creation of cookie files, you have the possibility to choose to accept the creation of all cookies other than the functional cookies or to systematically decline them or to choose the cookies it accepts depending on the issuer by configuring the following settings:
Internet Explorer:
- Click on the settings menu, followed by “Internet Options”;
- Under the “General” tab on the upper-left hand side, scroll down to “Browsing history”;
- Check the “Temporary Internet files and website files,” “Cookies and website data,” “History,”
  and “Download History” boxes;
- Click on “Delete”;
- Close out of Internet Explorer and reopen it for changes to take effect.

Firefox:
- Click on your Tools bar;
- Click on “Preferences”;
- On the menu to the right, select “Privacy”;
- Under the “history option”, there is a shortcut titled “clear your recent history”, click on that;
- Select only the top four options and hit clear now.

Safari:
- Click on “Safari” in the top left corner of the finder bar;
- Click on “Preferences”;
- Click on the “Privacy” tab;
- Click on “Manage Website Data”;
- Click on “Remove All”;
- Click “Remove Now”.

Google Chrome:
- Click the Tools menu;
- Click on “More tools”;
- Clear browsing data;
- At the top, choose a time range.
- To delete everything, select “All time”;
- Next to “Cookies and other site data” and “Cached images and files”, check the boxes;
- Click on “Clear data”. 
Hivebrite also utilized a list of their Sub-processors, which can be found here: https://hivebrite.com/legal/subprocessors