NAXARA LLC
PRIVACY POLICY

Last modified: March 24, 2026

INTRODUCTION

Naxara LLC (**"Company"** or **"We"**) respects your privacy and are committed to protecting it through our compliance with this policy.

This Privacy Policy governs your access to and usage of our Platform at https://www.consultnaxara.com, and, if applicable, our mobile application download and use (the "Application" and collectively referred to as the "Platform").

You agree that by accessing the Platform that you have read, understood, and agreed to be bound by all of these Privacy Policy.

PLEASE READ THIS PRIVACY POLICY CAREFULLY, BEFORE YOU START USING THE COMPANY'S PLATFORM AS THEY CONSTITUTE A LEGAL AGREEMENT BETWEEN YOU AND THE COMPANY. IF YOU DO NOT AGREE WITH ALL OF THESE PRIVACY POLICY, THEN YOU ARE EXPRESSLY PROHIBITED FROM USING THE PLATFORM AND YOU MUST DISCONTINUE USE IMMEDIATELY.

This policy describes the types of information we may collect from you or that you may provide when you visit the Platform and our practices for collecting, using, maintaining, protecting, and disclosing that information.

This policy applies to information we collect:

- On this Platform.
- In email, text, and other electronic messages between you and this Platform.
- Through mobile and desktop applications you download from this Platform, which provide dedicated non-browser-based interaction between you and this Platform.
- When you interact with our advertising and applications on third-party websites and services, if those applications or advertising include links to this policy.
- Through social media platforms and integrations when you connect or interact with our accounts.
- From customer service interactions, including phone calls, chat sessions, and support tickets.
- Through surveys, contests, promotions, and feedback forms you participate in.
- From cookies, web beacons, and similar tracking technologies when you use our services.
- Through offline interactions, such as in-person events, phone conversations, or written correspondence.
- From third-party partners, vendors, and service providers who share information with us in accordance with their own privacy policies and applicable law.

It does not apply to information collected by:

- Us offline or through any other means, including on any other website operated by Company or any third party (including our affiliates and subsidiaries); or
- Any third party (including our affiliates and subsidiaries), including through any application or content (including advertising) that may link to or be accessible from or through the Platform.

Please read this policy carefully to understand our policies and practices regarding your information and how we will treat it. If you do not agree with our policies and practices, your choice is not to use our Platform. By accessing or using this Platform, you agree to this privacy policy. This policy may change from time to time (see Changes to Our Privacy Policy). Your continued use of this Platform after we make changes is deemed to be acceptance of those changes, so please check the policy periodically for updates.

CHILDREN UNDER THE AGE OF 18

Our Platform is intended for users aged 18 and older. We do not knowingly collect personal information from individuals under 18 years of age.

If you are under 18, do not use or provide any information on this Platform or through any of its features, register on the Platform, make any purchases, use any interactive features, or provide any information about yourself including your name, address, telephone number, email address, or any screen name or user name you may use.

If we learn that we have collected or received personal information from a person under 18 without verification of parental consent, we will delete that information. If you believe we might have any information from or about a person under 18, please contact us at privacy@consultnaxara.com.

California residents under 18 years of age who have inadvertently provided information may have additional rights. Please see Your State Privacy Rights for more information.

INFORMATION WE COLLECT ABOUT YOU AND HOW WE COLLECT IT

We collect several types of information from and about users of our Platform, including:

- **Personal Information:** Information by which you may be personally identified, such as name, postal address, email address, telephone number, date of birth, social security number, payment information, employment information, or any other identifier by which you may be contacted online or offline.
- **Non-Personal Information:** Information that is about you but individually does not identify you, such as demographic information, preferences and interests, website usage patterns, search queries, click-through data, time spent on pages, browser type and version, operating system, and general geographic location.
- **Sensitive Personal Information:** Certain data elements we may collect — including Social Security numbers and government-issued identification numbers — are classified as sensitive personal information under applicable U.S. state privacy laws (including

CCPA/CPRA). We collect sensitive personal information only where necessary to deliver consulting or document preparation services you have specifically requested, and we limit the use and disclosure of such information as described in the Your State Privacy Rights section below.

- **Technical Information:** Information about your internet connection, the equipment you use to access our Platform, and usage details.

Business Client Data

- If you access the Platform as an employee, representative, or agent of a business entity ("Business User"), we may collect personal information about you in that professional capacity in connection with our consulting and document preparation services. Business User data is processed primarily to fulfill the consulting engagement and is subject to the terms of any applicable service agreement between the Company and the business entity. To the extent permitted by applicable state privacy law, personal information collected solely in a B2B context may be subject to different rights and obligations than personal information collected from individual consumers. We encourage Business Users to contact us at info@consultnaxara.com for questions about how their data is handled in the context of a business engagement.

How We Collect Information

Information You Provide Directly

We collect information that you voluntarily provide to us, including:

- **Registration and Account Information:** Information provided when registering to use our Platform, subscribing to our service, creating user profiles, including profile pictures, biographical information, and preferences
- **Communication Records:** Records and copies of your correspondence (including email addresses) when you contact us
- **Transaction Information:** Details of transactions you carry out through our Platform, fulfillment of orders, and financial information required for purchases
- **Content and Contributions:** Content you post, upload, or share on our Platform, including comments, reviews, photos, videos, and other user-generated content
- **Survey and Feedback Data:** Your responses to surveys, feedback, testimonials, and ratings you provide about our products or services
- **Contest and Promotion Data:** Information provided when you enter contests or promotions sponsored by us
- **Support Requests:** Information provided when you report problems with our Platform
- **Search Activity:** Your search queries on the Platform
- **Social Media Integration:** Information from your social media accounts when you choose to connect or link them to our Platform
- **Location Information:** Location data when you enable location services or provide location information

- **Communication Preferences:** Marketing opt-in/opt-out selections and communication preferences
- **User Contributions:** You may provide information to be published or displayed on public areas of the Platform or transmitted to other users or third parties (collectively, "User Contributions"). Your User Contributions are posted and transmitted at your own risk. Although we may limit access to certain pages and you may set privacy settings by logging into your account profile, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you may choose to share your User Contributions. Therefore, we cannot guarantee that your User Contributions will not be viewed by unauthorized persons.

Information We Collect Automatically

As you navigate through and interact with our Platform, we automatically collect certain information about your equipment, browsing actions, and patterns, including:

- **Visit Details:** Traffic data, location data, logs, communication data, and resources you access and use on the Platform
- **Device Information:** Information about your computer and internet connection, including IP address, operating system, and browser type
- **Usage Patterns:** Website navigation patterns, page views, time spent on pages, and click-through data

This automatically collected information may include personal information, or we may associate it with personal information we collect in other ways or receive from third parties. This information helps us improve our Platform and deliver a better, more personalized service by enabling us to:

- Estimate our audience size and usage patterns
- Store information about your preferences to customize our Platform according to your individual interests
- Speed up your searches
- Recognize you when you return to our Platform

Automatic Data Collection Technologies

The technologies we use for automatic data collection include:

- **Cookies (Browser Cookies):** Small files placed on your computer's hard drive. You may refuse to accept browser cookies by activating the appropriate setting on your browser. However, if you select this setting, you may be unable to access certain parts of our Platform. Unless you have adjusted your browser setting to refuse cookies, our system will issue cookies when you direct your browser to our Platform.
- **Web Beacons:** Small electronic files (also referred to as clear gifs, pixel tags, and single-pixel gifs) contained in our Platform pages and emails that permit us to count users who have visited those pages or opened emails and compile related website statistics (such as recording the popularity of certain website content and verifying system and server integrity).

- **Flash Cookies:** Local stored objects used by certain features of our Platform to collect and store information about your preferences and navigation. Flash cookies are not managed by the same browser settings used for browser cookies. For information about managing your privacy and security settings for Flash cookies, see "Choices About How We Use and Disclose Your Information."

Information from Third Parties

We may collect information about you from third parties, including:

- Business partners and service providers
- Social media platforms when you interact with our accounts or integrate your accounts with our Platform
- Third-party vendors who provide services on our behalf
- Publicly available sources
- Other users who may provide information about you in connection with referrals or shared activities

LEGAL BASIS FOR PROCESSING YOUR INFORMATION

For U.S. residents, we process your personal information based on the following grounds. For EU/UK residents, separate GDPR-specific legal bases apply as described in the International Data Transfers section.

We process your personal information based on the following legal grounds:

Contractual Necessity: To fulfill our obligations under our Terms of Service, including:

- Providing access to courses and educational materials
- Processing payments and managing subscriptions
- Delivering customer support and technical assistance
- Maintaining your account and learning progress

Legitimate Business Interests: For U.S. purposes, we process certain personal information as reasonably necessary to operate our business, including:

- Improving our Platform and developing new features
- Conducting analytics to enhance user experience
- Detecting and preventing fraud or security threats
- Marketing our services to existing customers (where permitted)

Legal Compliance: To meet our legal obligations, including:

- Maintaining transaction records for tax purposes
- Responding to lawful requests from authorities
- Complying with industry regulations and standards

Consent: For optional activities such as:

- Sending promotional communications to non-customers
- Sharing data with third-party marketing partners
- Using cookies for non-essential purposes
- Processing sensitive personal information

You may withdraw your consent at any time where we rely on consent as the legal basis for processing.

DATA RETENTION PERIODS

We retain your personal information only as long as necessary to fulfill the purposes for which it was collected and to comply with legal obligations:

- **Account Information**: Retained for the duration of your active account, plus 3 years after account closure for legal compliance
- **Transaction Records**: Maintained for 2 years after transaction completion for tax and financial reporting requirements
- **Communication Records**: Stored for 2 years from last contact for customer service quality and dispute resolution
- **Consulting Engagement Records**: Documents and work product created in connection with consulting or document preparation services are retained for 5 years after completion of the engagement, unless a longer period is required by applicable law or agreed in a service agreement.
- **Learning Progress Data**: Kept for 2 years after course completion to maintain certification records and transcript requests
- **Marketing Data**: Retained until you opt out of communications, plus 1 year to honor suppression requests
- **Support Tickets**: Maintained for 2 years after resolution for service improvement and legal protection
- **Website Analytics**: Aggregated data retained indefinitely; individual tracking data deleted after 26 months
- **Security Logs**: Preserved for 1 year for fraud prevention and security monitoring

You may request early deletion of your personal information by contacting info@consultnaxara.com , subject to legal retention requirements.

THIRD-PARTY USE OF COOKIES AND OTHER TRACKING TECHNOLOGIES

Some content or applications, including advertisements, on the Platform are served by third-parties, including advertisers, ad networks and servers, content providers, and application providers. These third parties may use cookies alone or in conjunction with web beacons or other tracking technologies to collect information about you when you use our Platform. The information they collect may be associated with your personal information or they may collect

information, including personal information, about your online activities over time and across different websites and other online services. They may use this information to provide you with interest-based (behavioral) advertising or other targeted content.

We do not control these third parties' tracking technologies or how they may be used. If you have any questions about an advertisement or other targeted content, you should contact the responsible provider directly. For information about how you can opt out of receiving targeted advertising from many providers, see Choices About How We Use and Disclose Your Information.

Global Privacy Control (GPC) Signals

We recognize and honor Global Privacy Control (GPC) signals as opt-out requests from the sale or sharing of personal information for California residents, as required by the California Privacy Rights Act (CPRA). If your browser or device transmits a GPC signal when you visit our Platform, we will treat that signal as a valid opt-out of the sale or sharing of your personal information to the extent required by applicable law. Note that GPC signals apply per browser and per device; you may need to enable the signal on each browser or device you use.

THIRD-PARTY DATA SHARING AND YOUR CONTROLS

Our Data Sharing Policy

We do not sell your personal information to third parties. We do not share your personal information with third parties for their independent direct marketing purposes. Any references elsewhere in prior versions of this policy to contacting you about third-party goods and services referred solely to communications we send on behalf of vetted business partners as part of our own service communications not to sharing your personal information with those parties. We will only share your personal information as described in this section.

Prohibited Sharing: We will NEVER share your personal information with:

- Data brokers or list rental companies
- Companies for general marketing purposes without your explicit opt-in consent
- Social media platforms for advertising targeting (unless you specifically authorize)
- Any party for purposes unrelated to your use of our Platform

Essential Service Providers:

- Payment processors (transaction data only)
- Email delivery services (contact information only)
- Cloud hosting providers (encrypted data with strict access controls)
- Customer support platforms (support interaction data only)

Educational Partners (Opt-in Required):

- Certification bodies for credential verification
- Industry associations for continuing education credits
- Employer training programs (with employee consent)

Your Sharing Controls:

- **Granular Opt-out:** Choose specific third-party categories to exclude
- **Purpose Limitation:** Restrict sharing to specific business functions
- **Time Limits:** Set expiration dates for third-party data sharing agreements
- **Audit Rights:** Request quarterly reports of data sharing activities

Contractual Protections: All third parties must:

- Sign comprehensive data processing agreements
- Implement equivalent security measures
- Limit data use to specified purposes only
- Delete data upon contract termination
- Submit to regular security audits

No Marketing or Data Broker Sharing

We will NEVER share your personal information with:

- Data brokers or list rental companies
- Third-party companies for their marketing purposes
- Social media platforms for advertising targeting
- Any party for purposes unrelated to your use of our Platform or our consulting services

HOW WE USE YOUR INFORMATION

We use information that we collect about you or that you provide to us, including any personal information:

- To present our Platform and its contents to you.
- To provide you with information, products, or services that you request from us.
- To fulfill any other purpose for which you provide it.
- To provide you with notices about your account/subscription, including expiration and renewal notices.
- To carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collection.
- To notify you about changes to our Platform or any products or services we offer or provide though it.
- To allow you to participate in interactive features on our Platform.
- To process transactions and manage payments.
- To respond to your customer service requests and provide technical support.
- To send you marketing communications about our products, services, and promotions (with your consent where required).

- To personalize your experience and deliver content and product offerings relevant to your interests.
- To conduct research and analytics to improve our Platform, products, and services.
- To detect, prevent, and address technical issues, fraud, and security threats.
- To comply with legal obligations and regulatory requirements.
- To protect our rights, property, and safety, as well as the rights, property, and safety of our users and others.
- To facilitate business transfers, such as mergers, acquisitions, or asset sales.
- To create aggregated or anonymized data for statistical analysis and business insights.
- To maintain records for business and legal purposes.
- For any other purpose with your consent or as otherwise permitted by applicable law.
- In any other way we may describe when you provide the information.
- For any other purpose with your consent.

We may also use your information to contact you about our own and third-parties' goods and services that may be of interest to you. If you do not want us to use your information in this way, please see Choices About How We Use and Disclose Your Information.

We may use the information we have collected from you to enable us to display advertisements to our advertisers' target audiences. Even though we do not disclose your personal information for these purposes without your consent, if you click on or otherwise interact with an advertisement, the advertiser may assume that you meet its target criteria.

DISCLOSURE OF YOUR INFORMATION

We may disclose aggregated information about our users, and information that does not identify any individual, without restriction.

We may disclose personal information that we collect, or you provide as described in this privacy policy:

- To our subsidiaries and affiliates.
- To contractors, service providers, and other third parties we use to support our business and who are bound by contractual obligations to keep personal information confidential and use it only for the purposes for which we disclose it to them.
- To a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of the Company's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by the Company about our Platform users is among the assets transferred.
- To third parties to market their products or services to you if you have not opted out of these disclosures. We contractually require these third parties to keep personal information

confidential and use it only for the purposes for which we disclose it to them. For more information, see Choices About How We Use and Disclose Your Information.

- For any other purpose disclosed by us when you provide the information.
- With your consent.

We may also disclose your personal information:

- To comply with any court order, law, or legal process, including to respond to any government or regulatory request.
- To enforce or apply our terms of use https://consultnaxara/terms-of-use and other agreements, including for billing and collection purposes.
- If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of the Company, our customers, or others. This includes exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction.

CHOICES ABOUT HOW WE USE AND DISCLOSE YOUR INFORMATION

We strive to provide you with choices regarding the personal information you provide to us. We have created mechanisms to provide you with the following control over your information:

- **Tracking Technologies and Advertising.** You can set your browser to refuse all or some browser cookies, or to alert you when cookies are being sent. If you disable or refuse cookies, please note that some parts of this site may then be inaccessible or not function properly.

We do not control third parties' collection or use of your information to serve interest-based advertising. However, these third parties may provide you with ways to choose not to have your information collected or used in this way. You can opt out of receiving targeted ads from members of the Network Advertising Initiative ("**NAI**") on the NAI's website.

Do Not Sell or Share My Personal Information

As stated in this policy, we do not sell or share personal information as defined under applicable U.S. state privacy laws. Nonetheless, if you are a California resident and wish to submit a formal Do Not Sell or Share request, you may do so by emailing info@consultnaxara.com with the subject line "Do Not Sell or Share Request." We will process your request within the timeframe required by applicable law. California residents may also exercise this right through a Global Privacy Control (GPC) signal as described above.

DATA SECURITY MEASURES

We take the security of your personal information seriously and work with industry-leading third-party hosting providers and security services to protect your data against unauthorized access, alteration, disclosure, or destruction. Our security approach combines our internal safeguards with the robust infrastructure and expertise of trusted third-party providers.

Technical Safeguards

Our hosting providers maintain enterprise-grade security infrastructure that protects your personal information through multiple layers of technical controls. All data transmission to and from our Platform is encrypted using industry-standard protocols, while sensitive information is encrypted

when stored in secure third-party data centers. Our hosting providers implement comprehensive network security measures including firewalls, intrusion detection systems, and continuous monitoring to protect against unauthorized access and cyber threats.

Access to systems containing personal information is strictly controlled through multi-factor authentication and role-based permissions managed by both our internal team and our hosting providers. Regular security assessments and vulnerability testing are conducted by qualified third-party security firms to identify and address potential weaknesses. All systems are maintained with current security patches and updates through coordinated efforts between our team and our hosting providers.

Administrative and Physical Safeguards

We work exclusively with hosting providers and service providers that maintain rigorous security standards equivalent to or exceeding industry best practices. All third-party providers are required to sign comprehensive data processing agreements that include specific security requirements, regular compliance audits, and strict confidentiality obligations. Our employees and any contractors with access to personal information receive privacy and security training and are bound by confidentiality agreements.

Physical security is managed by our hosting providers through secure data centers with 24/7 monitoring, biometric access controls, and environmental protections. These facilities maintain multiple redundancies and backup systems to ensure data availability and integrity. Equipment containing personal information is encrypted and protected through comprehensive physical and logical controls implemented by our hosting providers.

Limitations

The safety and security of your information also depends on you. Where we have given you (or where you have chosen) a password for access to certain parts of our Platform, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we do our best to protect your personal information, we cannot guarantee the security of your personal information transmitted to our Platform. Any transmission of personal information is at your own risk. We are not responsible for circumvention of any privacy settings or security measures contained on the Platform.

DATA BREACH NOTIFICATION PROCEDURES

In the event of a data security incident, we have established procedures to respond quickly in coordination with our hosting providers and third-party security services. Our incident response includes immediate containment measures, thorough investigation, and prompt notification to affected individuals and regulatory authorities as required by law.

Response and Investigation

Upon discovery of a potential breach, we immediately work with our hosting providers to contain the incident and secure affected systems. A comprehensive investigation is conducted to determine what information was involved, how many individuals may be affected, and the likelihood of data misuse. We maintain detailed documentation throughout the incident response process and coordinate with law enforcement when appropriate.

Notification and Remediation

We will provide written notification to affected individuals in accordance with the timeframes required by applicable federal and state law, which vary by jurisdiction. For example, California law requires notice in the most expedient time possible; other states allow 30 to 60 days from discovery. We will not delay notification beyond what is permitted by law, and we will notify law enforcement where such delay is authorized and appropriate. Notifications will include details about the incident, types of information involved, steps taken to address the breach, and specific actions individuals can take to protect themselves. Regulatory authorities will be notified in accordance with applicable state and federal requirements.

Following any security incident, we work with our hosting providers to implement additional protective measures and conduct thorough post-incident reviews. Enhanced monitoring and security controls are put in place to prevent similar incidents, and we may provide identity protection services to affected individuals when appropriate. Technology improvements and security enhancements are implemented based on lessons learned from each incident.

Compliance and Contact

We maintain compliance with all applicable breach notification laws through coordination with our hosting providers and legal counsel. Our security and privacy practices are regularly reviewed and updated to address evolving threats while meeting regulatory requirements.

For security concerns or to report potential vulnerabilities, contact our Security Team at info@consultnaxara.com . For general privacy questions, contact info@consultnaxara.com . We acknowledge security reports within 24 hours and provide regular updates until resolution.

INTERNATIONAL DATA TRANSFERS

Transfer Necessity: Your personal information may be transferred internationally to:

- United States (primary data processing)
- European Union (backup servers and support)
- Canada (secondary processing facilities)

Legal Safeguards:

For EU/UK Residents:

- Standard Contractual Clauses (SCCs) approved by the European Commission
- Adequacy decisions where available (Canada, EU-US Data Privacy Framework participants)
- Additional technical measures including encryption and access controls
- Regular adequacy assessments of third-country data protection laws

For All International Transfers:

- Binding corporate rules for affiliated entities
- Certification schemes (ISO 27001, SOC 2 Type II)

- Approved codes of conduct
- Contractual guarantees for data subject rights enforcement

Your Rights Regarding International Transfers:

- Right to obtain copies of applicable safeguards
- Right to object to transfers to specific countries
- Right to request data localization (subject to technical feasibility)
- Right to lodge complaints with supervisory authorities

Transfer Impact Assessments: We regularly assess:

- Political and legal environment in recipient countries
- Practical enforceability of data protection safeguards
- Risk of government access to personal data
- Availability of effective legal remedies

YOUR DATA CONTROL RIGHTS

Beyond account deletion, you have the following rights to control your personal information:

Selective Data Management:

- **Partial Data Deletion**: Request deletion of specific data categories (marketing preferences, uploaded content, optional profile information) while keeping your account active
- **Processing Controls**: Temporarily pause data processing or limit specific uses (analytics, personalization, research) while maintaining core service access
- **Download Restrictions**: Prevent other users from downloading your contributions

Communication and Sharing Controls:

- **Granular Email Preferences**: Choose specific types of communications you wish to receive
- **Third-party Sharing Opt-out**: Restrict data sharing with specific categories of third parties
- **Marketing Communications**: Stop promotional messages while maintaining service-related notifications

Data Portability: Request a copy of your personal information in a structured, machine-readable format for transfer to another service.

ACCESSING AND CORRECTING YOUR INFORMATION

You can review and change your personal information by logging into the Platform and visiting your account profile page.

You may also send us an email at info@consultnaxara.com to request access to, correct or delete any personal information that you have provided to us. We cannot delete your personal information

except by also deleting your user account. We may not accommodate a request to change information if we believe the change would violate any law or legal requirement or cause the information to be incorrect.

If you delete your User Contributions from the Platform, copies of your User Contributions may remain viewable in cached and archived pages or might have been copied or stored by other Platform users.

YOUR STATE PRIVACY RIGHTS

State consumer privacy laws may provide their residents with additional rights regarding our use of their personal information.

California Residents

California residents have specific rights under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), including:

- **Right to Know:** Request disclosure of personal information collected, sources, purposes, and third parties with whom it's shared
- **Right to Delete:** Request deletion of personal information (subject to certain exceptions)
- **Right to Correct:** Request correction of inaccurate personal information
- **Right to Opt-Out:** Opt out of the sale or sharing of personal information
- **Right to Limit Use of Sensitive Personal Information:** Limit use of sensitive personal information
- **Right to Non-Discrimination:** Not receive discriminatory treatment for exercising privacy rights

Note: We do not sell or share personal information as defined by California law.

To exercise these rights, please contact us at info@consultnaxara.com or write to us at: Privacy Department, Naxara LLC, 2824 N Power Rd Ste 113-252 Mesa, AZ 85215.

California Civil Code Section 1798.83 ("Shine the Light") permits California residents to request, once per year and free of charge, information about categories of personal information disclosed to third parties for their direct marketing purposes and the names and addresses of those third parties. We do not disclose personal information to third parties for their direct marketing purposes. If you are a California resident and wish to confirm this or request a written statement, please contact us at info@consultnaxara.com with the subject line "Shine the Light Request." We will respond in writing within 30 days of receiving your request.

Nevada Residents

Nevada residents have the right to opt out of the sale of certain personal information to third parties. **We do not sell personal information as defined by Nevada law.** If you still wish to submit an opt-out request, you can contact us at info@consultnaxara.com with the subject line "Nevada Do Not Sell Request."

Virginia, Colorado, Connecticut, and Utah Residents

Residents of Virginia, Colorado, Connecticut, and Utah have rights under their respective state privacy laws, including:

- Right to access personal information
- Right to delete personal information
- Right to correct inaccuracies
- Right to opt out of targeted advertising
- Right to opt out of the sale of personal information
- Right to opt out of profiling in furtherance of automated decisions with legal or similarly significant effects

Note: We do not sell personal information or engage in targeted advertising or profiling as defined by these state laws.
To exercise these rights, please contact us at info@consultnaxara.com.

Texas, Montana, Oregon, Iowa, Indiana, Tennessee, and Other State Residents

Residents of Texas, Montana, Oregon, Iowa, Indiana, Tennessee, and other states that have enacted comprehensive consumer privacy legislation may have rights similar to those described above, including rights to access, correct, delete, and opt out of the sale or sharing of personal information and profiling for consequential decisions. We do not sell personal information as defined under any applicable state law. To exercise available rights, please contact us at info@consultnaxara.com. We will respond in accordance with the timeframes required by the applicable state law governing your request. Where state law provides for an appeals process, we will inform you of that process if we decline to act on your request.

Biometric Data

We do not currently collect biometric identifiers or biometric information (such as facial recognition data, voiceprints, fingerprints, or retina scans) through the Platform. If we introduce any feature in the future that would require collection of biometric data, we will update this Privacy Policy in advance and obtain any consents required by applicable state law, including the Illinois Biometric Information Privacy Act (BIPA), the Texas Capture or Use of Biometric Identifier Act (CUBI), and analogous state statutes, prior to any such collection.

CHANGES TO OUR PRIVACY POLICY

It is our policy to post any changes we make to our privacy policy on this page with a notice that the privacy policy has been updated on the Platform home page. If we make material changes to how we treat our users' personal information, we will notify you through a notice on the Platform home page. The date the privacy policy was last revised is identified at the top of the page. You are responsible for ensuring we have an up-to-date active and deliverable email address for you, and for periodically visiting our Platform and this privacy policy to check for any changes.

CONTACT INFORMATION

Privacy Officer Contact: Email: info@consultnaxara.com Response Time: Within 48 hours for initial acknowledgment

Mailing Address: Naxara LLC Privacy Department 2824 N Power Rd Ste 113-252 Mesa, AZ 85215

Data Protection Officer (EU Residents): If you are an EU resident, you may contact our Data Protection Officer at email info@consultnaxara.com

Regulatory Complaints: You have the right to lodge complaints with:

- Your local data protection authority
- Federal Trade Commission (FTC) for US matters
- State Attorney General offices for state privacy law matters

Response Commitments:

- Privacy inquiries: 48-hour acknowledgment, 30-day resolution
- Data access requests: 30 days (may extend to 60 days for complex requests)
- Data deletion requests: 30 days verification, immediate technical deletion
- Security concerns: 24-hour acknowledgment, priority investigation

Office Hours: Monday-Friday, 9:00 AM - 5:00 PM MST

All privacy-related communications will be handled confidentially and in accordance with applicable privacy laws.