WORLD3 Privacy Policy

Last updated:

This Privacy Policy (“Policy”) outlines the practices of **Matrix Global. Inc**, conducting business as **WORLD3**, with its principal office located at **British Virgin Islands**(“Matrix Global,” “we,” “us,” or “our”). It governs how we collect, use, and disclose personal information of users who access and interact with our website www.WORLD3.ai (the “Website”), any mobile applications (“Apps”), and related platforms or services (collectively, the “Services”).

Personal Information

Acceptance of the Policy: Your engagement with our Services indicates your acknowledgment and acceptance of this Policy. Continued use of the Services constitutes your agreement to the practices described herein. Should you disagree with any part of this Policy, please refrain from using our Services or providing any personal information (“Personal Information”)

For the purposes of this Policy, and in accordance with applicable Canadian data protection laws and the WORLD3 ecosystem guidelines, “Personal Information” refers to any data that can directly or indirectly identify an individual. This encompasses a wide range of identifiers and attributes associated with a specific individual or household. Personal Information under this definition includes, but is not limited to:

1. **Identifiers:**
    - **Basic Information:** Name, username, email address.
    - **Digital Identifiers:** Blockchain address, IP address, device identifiers.
2. **Customer Records:**
    - **Transactional Data:** Records of products or services purchased, obtained, or considered, and other purchasing or consuming histories or tendencies.
3. **Blockchain and Digital Activity Information:**
    - **Wallet Address:** Blockchain wallet addresses and related on-chain activities.
    - **Transaction Data:** Interactions with the blockchain through the WORLD3 ecosystem, including transactions, asset transfers, and usage data.
4. **Device and Network Information:**
    - **Device Details:** Information about the devices used to access our Services, such as device type, operating system, browser type, and version.

- **Network Activity:** Data related to browsing history, search history, and interactions with our Services.

5. **Protected Classifications:**
   - **Demographic Data:** Characteristics of protected classifications under applicable laws, including information related to race, ethnicity, gender identity, and age.
6. **Communications:**
   - **Direct Interactions:** Information derived from direct communications with us, including emails, chat logs, and customer support interactions.
   - **Public Communications:** Comments, posts, or other content you share publicly on forums or social media platforms connected to WORLD3.
7. **Commercial Information:**
   - **Usage Data:** Data about how you interact with our Services, including engagement metrics, frequency of use, and areas of interest.
8. **Geolocation Data:**
   - **General Location Information:** Geographic data inferred from IP addresses or other information provided through device settings. Precise geolocation data is not collected unless explicitly provided by you.
9. **Inference Data:**
   - **Profiles:** Inferences drawn from your use of the Services to create a profile reflecting preferences, characteristics, or behavior.
10. **Other Information:**
    - **Surveys and Feedback:** Responses to surveys, feedback forms, and other interactions that provide insights into user satisfaction and preferences.
    - **Contest and Promotion Entries:** Data collected from your participation in contests, promotions, and other marketing events.

Sources of Personal Information:

- **Direct Collection:** Information you provide directly to us through interactions, registrations, or transactions within the WORLD3 platform.
- **Third-Party Sources:** Information obtained from affiliated companies, service providers, or publicly available sources, including social media integrations and marketing partners.
- **Automated Collection:** Data automatically collected through cookies, tracking pixels, and other digital tools as you navigate and interact with our Services.

Usage of Personal Information:

Personal Information collected by WORLD3 is used in compliance with applicable data protection regulations to provide, enhance, and secure our Services, tailor user experiences, and for other purposes outlined in this Policy.

By using WORLD3 Services, you consent to the collection, use, and disclosure of your Personal Information as described in this Policy. If you have any questions or require further details, please refer to the contact information provided at the end of this Policy.

Scope

This Privacy Policy (“Policy”) delineates the parameters within which WORLD3, governed by Matrix Labs based in Edmonton, Alberta, Canada, collects, uses, and discloses Personal Information. The Policy is comprehensive in its application, encompassing all individuals and entities engaging with any facet of WORLD3’ s services, whether through the primary platform, affiliated digital interfaces, or other forms of interaction.

Applicability to Services

The scope of this Policy extends to all aspects of Personal Information management associated with WORLD3’ s Services. Specifically, it applies to:

1. **Platform Use:**
    - **Web-based Interactions:** All data exchanges, browsing activities, and transactional processes conducted on the WORLD3 website or related web platforms.
    - **Mobile Applications:** Use of any mobile applications affiliated with WORLD3, including any data collected through app interactions, permissions granted, and notifications.
2. **Digital and Physical Engagements:**
    - **Blockchain Interactions:** Activities and transactions recorded on the blockchain through the WORLD3 ecosystem, including but not limited to token transfers, smart contract executions, and other on-chain data exchanges.
    - **Offline Communications:** Personal Information gathered through offline methods, including in-person events, paper-based forms, and verbal communications related to WORLD3 Services.
3. **Third-Party Integrations:**
    - **External Platforms:** Data acquired through integration with third-party platforms, such as social media networks or blockchain wallet providers, when interacting with WORLD3 Services.
    - **Service Providers:** Information shared with or received from third-party service providers engaged to enhance or deliver WORLD3 Services.
4. **Marketing and Outreach:**

- **Promotional Activities:** Personal Information used in the context of marketing, advertising, and outreach efforts, including email campaigns, promotional events, and social media engagement.
- **Feedback and Surveys:** Data collected from user feedback, surveys, and similar tools intended to gather insights or preferences from the user base.

5. **Security and Compliance:**
    - **Monitoring and Auditing:** Data collection and usage for the purposes of maintaining security, performing audits, and ensuring compliance with legal and regulatory obligations.
    - **Incident Response:** Personal Information involved in incident management, such as breach notifications or compliance reporting.

Geographic Coverage

This Policy is applicable irrespective of the user’ s geographical location, with particular adherence to:

- **Canadian Privacy Laws:** Compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA) and any relevant provincial regulations, ensuring the protection of data for users located within Canada.
- **International Standards:** Adherence to applicable international data protection laws and standards for users accessing WORLD3 Services from outside Canada.

Comprehensive Inclusion

All users of WORLD3 Services, including but not limited to registered account holders, unregistered visitors, and participants in WORLD3’ s digital and offline initiatives, are subject to the provisions of this Policy. The coverage includes:

- **Registered Users:** Individuals who have created accounts or profiles on WORLD3 platforms and engaged in any transactions or interactions therein.
- **Unregistered Visitors:** Users who visit the WORLD3 website or app without creating an account but may still interact with the platform in a limited capacity.
- **Event Participants:** Individuals participating in WORLD3 events, surveys, or contests, either online or in-person, whose Personal Information is collected during such activities.

Policy Limitations

While this Policy governs the collection, use, and disclosure of Personal Information by WORLD3, it does not extend to:

- **Third-Party Services:** Personal Information collected by third-party services not directly affiliated with WORLD3, even if accessed via WORLD3 platforms or recommended by WORLD3.

- **Independent Entities:** Data practices of independent entities or individuals, even if those entities or individuals interact with WORLD3 Services or act as partners or affiliates.

By using WORLD3 Services, users acknowledge the applicability of this Policy to their Personal Information and consent to its terms. For detailed information on specific data practices or additional inquiries, users are encouraged to contact WORLD3 directly using the information provided in this Policy.

Collection of Personal Information

The collection of Personal Information by WORLD3 is essential for providing and enhancing our Services. Our data collection practices are structured to ensure compliance with applicable legal standards while safeguarding user privacy and supporting the operational needs of WORLD3.

Categories of Personal Information

The categories of Personal Information we collect vary based on the interactions and services utilized by users. The following outlines the principal categories:

- **Identifiers:** Includes but is not limited to name, username, account name, blockchain address, physical address, telephone number, date of birth, email address, and other unique identifiers such as online identifiers.
- **Customer Records:** Encompasses electronic customer records containing Personal Information, including payment details processed through third-party payment systems.
- **Blockchain Information:** Covers blockchain addresses, on-chain activities, and interactions with WORLD3’ s Services on the blockchain, reflecting user transactions and activities.
- **Device Information:** Data related to the user's device, such as IP address, browser type, operating system version, carrier and manufacturer details, app installations, device identifiers, mobile advertising identifiers, and push notification tokens.
- **Protected Classifications:** Characteristics under applicable law, including race, sex, age, and disability.
- **Communications:** Includes direct communications, web forms, online polls, and engagement with blogs and posts.
- **Commercial Information:** Records of products or services purchased, considered, or other purchasing and usage histories.
- **Usage Data:** Information on internet or other electronic network activities such as browsing history, search history, and interactions with WORLD3’ s websites, applications, or advertisements.
- **Location Data:** General geographic information inferred from your IP address, noting that it does not equate to precise geolocation.

- **Profiles and Inferences:** Insights derived to create profiles reflecting user preferences and behaviors.

Sources of Personal Information

WORLD3 acquires Personal Information from a variety of sources, ensuring comprehensive data to enhance service delivery and user experience. The sources include:

- **Directly from Users:** Information provided during account creation, blockchain wallet association, participation in transactions, interactions with chatbots, contest entries, communication on the Services, subscription to marketing communications, and customer support interactions.
- **From Third Parties:** Data obtained from affiliates, public records, third-party service providers (e.g., for fraud detection and identity verification), consumer data resellers, social networks, marketing partners, and affiliate companies.
- **Service-Related Interactions:** Information collected automatically during use of our Services, interactions on the Website, or data derived from user preferences and behaviors.

Detailed Data Collection Points

- **Registration, Accounts, and Profiles:** Collection occurs when users register for a User Account, including blockchain addresses, usernames, email addresses, and any linked third-party service information.
- **Marketing, Surveys, and Events:** Data collected when users subscribe to marketing communications or participate in events, including names, contact information, and preferences.
- **Communications and Requests:** Includes data from email, phone, or other communications, maintaining a record of user contact details, communications, and our responses.
- **Third-Party Data:** Information collected from third-party accounts (e.g., social media), transaction details for purchases or Services, social media interactions, and additional demographic or updated contact information from public records or third-party sources.
- **Automatic Collection:** Data collected through cookies, pixels, tags, and log-files on the Website and Apps, capturing information such as browser type, device details, operating system, phone model, referring URLs, and IP addresses.

Integration of Collected Data

The information collected from these sources may be combined to create a unified profile for each user, enhancing the relevance and personalization of WORLD3’ s Services. This data amalgamation supports accurate user identification, improved service delivery, and personalized user experiences.

Automated Collection Techniques

We employ cookies, pixel tags, log-files, and other technologies to automatically gather data regarding user interactions with our Services. This technology facilitates the collection of information about the user's browser or device, interactions with our content, and the user's IP address. This automated collection is essential for understanding user behaviors, improving our services, and personalizing content.

By clearly outlining these data collection practices, WORLD3 ensures transparency, compliance with legal standards, and the ability to deliver tailored and efficient services to our users.

Use of Personal Information

WORLD3 processes Personal Information under strict legal grounds, ensuring compliance with all relevant data protection laws. The following elaborates on how we use your Personal Information to provide, enhance, and protect our Services:

1. **Providing Support and Services:**
   We utilize Personal Information to deliver and manage our Services, including operating our website, application, and associated platforms. This encompasses updating your WORLD3 profile, responding to inquiries, troubleshooting issues, fulfilling orders, processing payments, and providing technical support. The lawful basis for this is the fulfillment of contractual obligations with you, ensuring that we can effectively deliver the services you have requested.
2. **Analyzing and Improving Our Business:**
   To enhance our understanding of how users interact with our Services, we analyze usage patterns and feedback. This includes evaluating and refining our Services and operations, developing new features, and conducting customer satisfaction surveys. Our aim is to improve service quality and user experience continually. The lawful basis for this activity is our legitimate business interest in understanding and improving our Services.
3. **Personalizing Content and Experiences:**
   Personal Information allows us to tailor content and interactions to individual preferences, enhancing user experience. By creating profiles based on your interests and activities, we can provide more relevant content and recommendations. Additionally, we will use data to fine-tune our AI model, offering users a more personalized experience as they use WORLD3. Our lawful basis for this is our legitimate interest in offering personalized services and making improvements based on user feedback.
4. **Advertising, Marketing, and Promotional Purposes:**
   We use Personal Information to reach users with targeted ads and evaluate the effectiveness of our marketing campaigns. This includes sending newsletters, offers, and other communications we believe will interest you. Users must consent to receive marketing communications, and they can opt out at any time. Our lawful basis for this processing is user consent and our interest in promoting our Services.

5. **Securing and Protecting Our Business:**
   Personal Information is essential for protecting our business operations, assets, and Services from fraud, unauthorized access, and other security threats. We use this information to investigate, detect, and prevent unauthorized activities or misconduct, ensuring the safety of our network and information. The lawful basis here is our legitimate business interest in maintaining security and compliance.
6. **Defending Our Legal Rights:**
   We process Personal Information to manage and respond to legal disputes, claims, and to protect our rights and interests. This includes actions necessary to establish, defend, or protect our rights in legal contexts. Our lawful basis is the legitimate interest in defending our business and legal positions.
7. **Auditing, Reporting, Corporate Governance, and Internal Operations:**
   To comply with legal obligations and manage our business, we conduct audits and assessments of our operations, privacy, security, and financial controls. This also includes preparing for any potential mergers, acquisitions, or restructuring. Our lawful basis for this processing is compliance with legal requirements and legitimate interests in governance and corporate management.
8. **Complying with Legal Obligations:**
   We use Personal Information to fulfill our legal duties, including compliance with subpoenas, court orders, and regulatory requests. This ensures adherence to applicable laws and regulations, with the lawful basis being compliance with these legal obligations.
9. **For Our Legitimate Business Interests:**
   We process Personal Information to manage our business effectively, providing the best possible services and ensuring a secure and optimized user experience. We carefully balance our business interests against potential impacts on users to ensure that processing is justified and compliant. Our lawful basis is the legitimate business interest in efficient service delivery and management.
10. **Aggregate and De-identified Data:**
    WORLD3 may de-identify Personal Information to create anonymous and aggregated data sets. These are used for business assessment, improvement, benchmarking, and other research purposes. Such de-identified data is not considered Personal Information and is used in compliance with applicable data protection laws.

Combining Information from Different Sources:
We may integrate information collected from various sources, both offline and online, to enrich our understanding and enhance the accuracy of our data. This comprehensive approach allows us to offer more consistent and effective services.

Authority to Submit Personal Information:

By providing Personal Information about others, you confirm that you have the authority to do so and that the individuals involved are aware of the terms of this Policy.

In handling Personal Information, WORLD3 is committed to upholding user privacy and data protection, ensuring that all processing activities are conducted transparently, lawfully, and with respect for user rights.

Disclosure of Personal Information

At WORLD3, we adhere to stringent standards when it comes to the disclosure of Personal Information. We may share or disclose Personal Information collected through our Services under the following circumstances:

1. **Service Providers:**
   We may engage third-party service providers to perform services on our behalf. These providers may access and use your Personal Information as necessary to perform tasks such as hosting, auditing, consulting, customer support, and technical services. For instance, a third-party hosting provider may store our data securely, while an auditing firm may review our compliance with legal requirements.
2. **Advertising and Marketing Partners:**
   To enhance our advertising efforts and reach relevant audiences, we may share Personal Information with third-party advertising and marketing partners. These partners assist in delivering targeted ads, measuring the effectiveness of campaigns, and analyzing online and mobile interactions. They may collect browsing data and other usage information to tailor advertisements to user preferences. This helps us understand how individuals engage with our Services over time and across different devices.
3. **Subsidiaries, Affiliates, and Business Partners:**
   We may share Personal Information with affiliated companies, including our parent company, subsidiaries, or entities under common control. These affiliates may use the information for purposes consistent with this Policy, such as offering exclusive content or coordinating marketing efforts. Additionally, we may collaborate with business partners to enhance service offerings, which may involve sharing data to deliver integrated solutions or joint promotions.
4. **Legal Compliance:**
   We may disclose Personal Information to comply with applicable laws, regulations, legal processes, or enforceable governmental requests. This includes responding to valid court orders, subpoenas, or government investigations. Furthermore, we reserve the right to report any activities we believe, in good faith, to be unlawful to law enforcement agencies. For example, if we are legally required to provide information about suspicious activities, we will comply with such requirements.

5. **Business Transfers:**
   In the event of a merger, acquisition, asset sale, restructuring, or similar business transaction, Personal Information may be transferred as part of the transaction. This includes due diligence conducted prior to such events. For example, if WORLD3 is acquired by another company, your data may be transferred to the new entity to ensure continuity of service. Such transfers will comply with applicable legal requirements and safeguard your information.
6. **Protecting Our Rights:**
   We may disclose Personal Information as necessary to protect our legal rights and interests. This includes responding to claims or disputes, enforcing our agreements and terms, and preventing fraud. For instance, if a claim is made against WORLD3, we may disclose relevant information to defend against the claim. Similarly, we may use your information to investigate and prevent fraudulent activities or unauthorized access.
7. **Aggregated and De-Identified Data:**
   We may share aggregated or de-identified information with third parties for research, marketing, advertising, and analytics purposes. This information does not identify individual users and is used to generate insights into industry trends, customer preferences, and marketing strategies. For example, we may share aggregated data on user behavior to help advertisers understand market trends without revealing personal identities.

What happens if you do not provide us with the Personal Information we request or ask that we stop processing your Personal Information?

If you choose not to provide the requested Personal Information or withdraw your consent for processing, you may be unable to use certain features or functionalities of our Services. This may include access to personalized content, targeted advertisements, or specific support services. Your ability to fully utilize our Services may be limited, and certain interactions or transactions may not be completed without the necessary information.

WORLD3 is committed to respecting your privacy while ensuring compliance with legal and regulatory obligations regarding the disclosure and protection of Personal Information. Our practices are designed to provide transparency and control over how your information is shared.

Automated Decisions

WORLD3 does not currently engage in any form of automated decision-making that produces legal or similarly significant effects on users without human intervention. Automated decisions are defined as processes wherein decisions are made algorithmically or by a computer system without direct human oversight. Such processes can potentially impact users' legal rights, obligations, or access to services.

Here is an elaboration on our stance and policy regarding automated decisions:

1. **Definition and Scope of Automated Decisions:**
   Automated decisions refer to those made solely by technological means without any human involvement. These decisions are typically based on algorithms or artificial intelligence systems that process data to make determinations or predictions. For example, automated decisions might involve credit scoring systems, employment screening tools, or other systems that assess eligibility for services based on predefined criteria without human judgment.
2. **Absence of Automated Decision-Making at WORLD3:**
   As of now, WORLD3 does not utilize any systems that make such automated decisions about users. This means that all significant decisions affecting your legal rights, access to essential services, or similar critical outcomes involve human judgment and review. This approach ensures that all relevant factors are considered, and potential biases inherent in automated systems are mitigated. For instance, decisions about user access to particular services, eligibility for benefits, or compliance assessments are reviewed by our team to ensure fairness and accuracy.
3. **Commitment to Transparency and Fairness:**
   WORLD3 is committed to transparency in all its processes and ensuring that users' rights are safeguarded. If in the future, we decide to implement any automated decision-making tools, we will ensure that such systems are designed and tested to uphold fairness, accountability, and transparency. This includes providing users with clear information about the logic involved in any automated decision-making process and the potential implications. Additionally, we will ensure that users have the right to contest and seek human intervention in any decisions that significantly affect them.
4. **Data Protection and Privacy Considerations:**
   Any future implementation of automated decision-making will be conducted in compliance with applicable data protection and privacy laws. This includes taking measures to ensure that the processing of personal data is fair, lawful, and transparent. Users will be informed about the data being used for automated decisions, the purpose of such processing, and the impact on their rights and interests. We will also implement safeguards to protect personal data against unauthorized access or misuse.
5. **User Rights and Remedies:**
   Should WORLD3 adopt automated decision-making processes in the future, we will establish mechanisms to allow users to challenge and seek review of any automated decisions that affect them significantly. This may involve providing users with the right to request an explanation of the decision-making process, the criteria used, and the option to have a decision reviewed by a human. This aligns with our commitment to uphold users' rights and provide equitable and transparent services.

6. **Future Developments:**
   As the field of automated decision-making evolves, WORLD3 will continuously monitor advancements and regulatory changes to ensure compliance and adapt our practices accordingly. We are committed to integrating new technologies in ways that enhance our services while maintaining ethical standards and protecting user interests.

While WORLD3 does not currently engage in automated decision-making, we recognize the importance of responsible and transparent use of such technologies. Should this policy change, we are committed to ensuring that any automated processes are implemented with rigorous oversight, clear communication, and robust safeguards to protect our users' rights and interests.

Cookies and Analytics

In alignment with best practices and industry standards, WORLD3 employs various technologies, including cookies, pixels, tags, and other similar mechanisms, to enhance the functionality of our Services, ensure security, detect and prevent fraud, and gather usage information. These technologies are essential tools that enable us to provide a seamless and personalized experience for our users. Below is an elaboration on how these technologies are used:

1. **Purpose and Functionality of Cookies and Similar Technologies:**
   - **Cookies:** Cookies are small data files placed on your computer or mobile device when you visit a website. These alphanumeric identifiers are used for record-keeping and tracking purposes. They serve multiple functions, such as enabling users to log in to our Services, retaining user settings and preferences, and monitoring user interactions with our Services. Cookies help us understand user behavior, which allows us to tailor content and advertisements to better meet user needs and preferences.
   - **Pixels, Tags, and Embedded Scripts:** Pixels (also known as web beacons or clear GIFs) and tags are small graphic images or scripts embedded in web pages and emails. They work similarly to cookies but are used to track user behavior more precisely, such as when a user opens an email or visits a specific page. These tools provide critical data for analyzing the effectiveness of our marketing campaigns and the performance of our Services.
2. **Types of Cookies Utilized:**
   - **Essential Cookies:** These are necessary for the basic operation of our Services, such as logging in and accessing secure areas. Without these cookies, certain functionalities cannot be provided.
   - **Performance and Analytics Cookies:** These cookies collect information about how users interact with our Services, including the pages they visit and any errors encountered. This data is used to improve the performance and user experience of our Services.

- **Functional Cookies:** These cookies remember user choices, such as language preference, to provide a more personalized experience.
- **Targeting Cookies:** These are used to deliver advertisements that are more relevant to the user and their interests. They also limit the number of times a user sees an ad and help measure the effectiveness of advertising campaigns.

3. **Third-Party Cookies and Advertising:**
   - We may allow third-party service providers to use cookies, web beacons, and similar technologies on our Services to collect or receive information and provide targeted advertising based on user interests and online behavior. These third parties may include advertising networks and analytics service providers who collect data to better understand user interactions with ads and websites.
   - Users can opt out of targeted advertising practices on their devices by visiting the Network Advertising Initiative at http://www.networkadvertising.org or the Digital Advertising Alliance at http://optout.aboutads.info. This opt-out mechanism does not eliminate all advertising but rather ensures that ads displayed are not personalized based on the user's browsing habits.
4. **Management of Cookies:**
   - Users have the ability to manage cookies through their web browser settings. Most browsers provide options to block cookies, receive notifications when cookies are set, or delete cookies altogether. Instructions for managing cookies can typically be found in the browser's help menu. It is important to note that disabling cookies may affect the functionality of our Services and certain features may become unavailable.
   - For more detailed information on how we use cookies and how you can manage them, please refer to our Cookie Policy available on our website.
5. **Use of Pixel Tags and Embedded Scripts:**
   - Pixel tags and embedded scripts are used to gather information about user interactions with our Services and emails. They allow us to track the activities of users on our Website, enhance the relevance of our advertisements, personalize content, and improve user engagement. For example, we may use these tools to monitor how users respond to our emails and to identify the most effective content and formats.
6. **Third-Party Analytics Tools:**

- Our Services utilize third-party analytics tools, such as Google Analytics, to analyze user behavior and gather insights on how our Services are used. These tools use cookies and similar technologies to collect data on user interactions and report on usage patterns and trends. Users can learn about Google’ s practices by going to www.google.com/policies/privacy/partners/, and you can opt out of them by downloading the Google Analytics opt-out browser add-on, available at https://tools.google.com/dlpage/gaoptout.

WORLD3 uses cookies and similar technologies to enhance user experience, improve our Services, and provide relevant content and advertising. We are committed to transparency regarding the use of these technologies and provide users with options to manage their preferences and opt-out where applicable. For further information or to review our detailed cookie policy, please visit our website.

Children’ s Privacy

The protection of children's privacy and safety online is of paramount importance to WORLD3. In accordance with applicable legal and regulatory standards, WORLD3 enforces strict policies regarding the collection and handling of personal information from children under the age of 18. The following provisions elaborate on our approach to children’ s privacy:

1. **Age Restriction Policy:**
   - **Access Prohibition:** Our Services are explicitly restricted to individuals who have attained the legal age of majority in their respective jurisdictions. Accordingly, children under the age of 18 are expressly prohibited from accessing or using any part of our Services, including our website, mobile applications, and related online platforms.
   - **Account Creation:** WORLD3 does not permit the registration or creation of user accounts by individuals under the age of 18. Any attempt to register by a minor will be denied, and any accounts suspected to be created by minors will be subject to immediate suspension or termination.
2. **Data Collection Practices:**
   - **No Intentional Collection:** WORLD3 does not knowingly collect or maintain personal information from individuals who are known to be under the age of 18. Our data collection practices are designed to comply with regulations aimed at protecting children's online privacy.
   - **Immediate Action:** Should we inadvertently collect personal information from a minor, we will take prompt measures to delete such information from our records. This includes the removal of any data collected inadvertently through user registration, participation in activities, or other means.
3. **Parental Involvement:**

- **Reporting Mechanism:** Parents or guardians who have concerns regarding the collection or potential collection of their child’ s personal information are encouraged to contact WORLD3 immediately. We are committed to addressing any such concerns expeditiously and ensuring the privacy of the child is safeguarded. Contact details for such inquiries can be found in the “Contact Us” section of our policy.
- **Review and Deletion Requests:** In cases where it is brought to our attention that a child under the age of 18 has used our Services, parents or guardians may request the review or deletion of their child's personal information. Such requests should be directed to the contact information provided under the “Contact Us” section. Upon verification, we will comply with such requests and ensure that the child’ s information is promptly deleted from our systems.

4. **Regulatory Compliance:**
   - **Adherence to Legal Standards:** Our policies and practices regarding children’ s privacy are designed to comply with relevant legal frameworks, including the Children’ s Online Privacy Protection Act (COPPA) in the United States and similar regulations globally. We regularly review and update our practices to ensure compliance with any new or amended regulations governing children's privacy.
   - **Regular Audits:** WORLD3 conducts regular audits of our data collection and handling practices to verify compliance with our children’ s privacy policy and to identify and address any potential vulnerabilities in our systems.
5. **Educational Initiatives:**
   - **User Education:** WORLD3 is committed to educating our user community about the importance of children’ s online safety and privacy. We provide resources and guidance to help users understand the risks associated with sharing personal information online and the measures that can be taken to protect minors from unauthorized data collection and exposure.

WORLD3 takes a proactive and stringent approach to protecting the privacy of children. By restricting access, avoiding the collection of personal information from minors, and providing mechanisms for parental control and intervention, we aim to uphold the highest standards of online safety and compliance with children's privacy laws. For any concerns or inquiries related to children's privacy, users and parents are encouraged to reach out to us directly using the provided contact information.

Security

At WORLD3, we prioritize the security and confidentiality of your Personal Information. We have established comprehensive security measures to guard against unauthorized access, misuse, or

disclosure of the Personal Information we collect. The following elaborates on our security protocols and your role in safeguarding your information:

1. **Implementation of Safeguards:**
    - **Technical Protections:** We employ advanced technical measures to secure your Personal Information, including encryption protocols, secure socket layer (SSL) technology, and multi-factor authentication (MFA). These measures ensure that data transmitted through our Services is protected against interception and unauthorized access.
    - **Access Controls:** We enforce strict access controls to restrict access to Personal Information to authorized personnel only. This includes role-based access controls (RBAC) and regular access audits to prevent unauthorized internal access and ensure compliance with security policies.
2. **Organizational and Physical Measures:**
    - **Employee Training:** Our employees, contractors, and agents are trained on data protection and privacy protocols. We conduct regular training sessions to update our staff on emerging security threats and best practices for handling Personal Information securely.
    - **Contractual Obligations:** We require third-party service providers and contractors to adhere to strict data protection standards through contractual agreements. These agreements mandate the implementation of equivalent security measures to those employed by WORLD3.
    - **Physical Security:** We implement physical security measures to protect data storage facilities and server environments. This includes restricted access to data centers, surveillance systems, and environmental controls to protect against physical breaches.
3. **Incident Response and Breach Notification:**
    - **Breach Detection and Response:** We have established incident detection systems and protocols for responding to potential data breaches. This includes monitoring systems for unusual activities, intrusion detection systems, and response teams trained to handle data security incidents promptly.
    - **Notification Procedures:** In the event of a data breach involving Personal Information, we will adhere to applicable legal requirements regarding breach notifications. We will notify affected individuals and relevant regulatory authorities as mandated by law, providing timely updates on the nature of the breach, affected data, and recommended steps to mitigate the impact.
4. **User Responsibilities:**

- **Password Management:** Users are encouraged to choose strong, unique passwords for their User Accounts and to update passwords regularly. A strong password typically includes a combination of letters, numbers, and special characters and should not be reused across multiple platforms.
- **Account Security:** Users should take precautions to safeguard their account credentials. This includes logging out of accounts after use, avoiding the use of public or shared computers for sensitive activities, and being cautious of phishing attempts and suspicious communications.
- **Software Updates:** It is recommended that users keep their operating systems, browsers, and security software up to date. Regular updates help protect against vulnerabilities and enhance the overall security of their devices and accounts.

5. **Limitations and User Awareness:**
   - **Inherent Risks:** While we strive to protect your Personal Information through robust security measures, it is important to acknowledge that no security system is impervious to all threats. Risks such as unauthorized access, hacking, or data loss can never be entirely eliminated.
   - **User Vigilance:** Users are urged to remain vigilant and proactive in protecting their Personal Information. This includes recognizing potential security threats, avoiding risky behaviors online, and promptly reporting any suspicious activities related to their accounts or personal data.
6. **Ongoing Security Enhancement:**
   - **Continuous Improvement:** We are committed to continually enhancing our security measures. This involves regular reviews of our security policies, adopting new technologies, and updating our practices in response to evolving threats and regulatory changes.
   - **Feedback and Collaboration:** We value feedback from our users regarding security concerns or potential vulnerabilities. Users are encouraged to report any security issues or suggestions for improvement to our support team to help us strengthen our security posture.

WORLD3 takes a proactive and multi-layered approach to protecting your Personal Information. Through the implementation of technical, organizational, and physical safeguards, coupled with robust incident response mechanisms and user education, we aim to provide a secure environment for your interactions with our Services. For further inquiries or to report security concerns, please contact us using the information provided in the "Contact Us" section of our Privacy Policy.

Transfers outside the UK/Europe

Cross-Border Data Transfers

For users within the United Kingdom and the European Economic Area (“EEA”), the transfer of Personal Information outside these jurisdictions requires careful handling to comply with applicable data protection laws. Below are the details concerning such transfers:

1. **Transfers to Non-Adequate Jurisdictions:**
    - **Nature of Transfers:** We may transfer your Personal Information to countries outside the UK and EEA when using service providers, partners, or data processing facilities located abroad. Such transfers may include, but are not limited to, data hosting, IT support, and cloud services.
    - **Legal Requirements:** The destination countries may have different or less stringent data protection laws compared to those in the UK and EEA. As such, the adequacy of data protection in these jurisdictions might not align with the rigorous standards set by UK and EEA laws.
2. **Safeguarding Measures:**
    - **Standard Contractual Clauses (SCCs):** To ensure an equivalent level of data protection, we implement safeguards such as the European Commission's approved Standard Contractual Clauses or the UK's International Data Transfer Agreement (IDTA) where applicable. These legal instruments oblige the recipient of your Personal Information to adhere to stringent data protection standards and provide assurances regarding the security and confidentiality of your data.
    - **Supplementary Measures:** Where necessary, we may apply additional technical, organizational, or contractual measures to further protect your data. This may include data encryption, pseudonymization, and regular audits of data protection practices at the recipient's end.
    - **Data Transfer Impact Assessments:** Before initiating any transfer, we conduct thorough assessments to evaluate the potential risks and ensure compliance with data protection requirements. This assessment includes reviewing the recipient's data protection capabilities and the legal context of the destination country.
3. **User Rights and Notification:**
    - **Information on Safeguards:** Users have the right to request detailed information about the safeguards in place for international data transfers. This includes a summary of the contractual obligations and protections afforded to the transferred data. To request such information, please contact us using the details provided in the "Contact Us" section of our Privacy Policy.

- **Regulatory Compliance:** We commit to notifying users if there are significant changes in the legal framework or safeguards affecting cross-border data transfers. This includes any amendments to the SCCs, IDTA, or other protective measures that may impact the security or lawful processing of Personal Information.

4. **Transfers Outside the UK/EEA:**
   - **Compliance with Local Laws:** For users outside the UK and EEA, we ensure that data transfers to countries beyond your home jurisdiction comply with local legal requirements. This may involve adhering to national data protection laws, obtaining necessary consents, and implementing equivalent safeguards to those used for UK and EEA transfers.
   - **Global Data Protection Practices:** We maintain a global data protection strategy to uphold consistent security and privacy standards across all jurisdictions. This strategy includes regular reviews and updates to our policies and practices to reflect changes in international data protection regulations and best practices.
5. **Further Information:**
   - **Data Protection Inquiries:** Users seeking more information about our cross-border data transfer practices, including details on the specific safeguards employed, are encouraged to contact our Data Protection Officer (DPO) or the designated contact point mentioned in our Privacy Policy. We strive to provide comprehensive transparency regarding our data handling procedures and compliance measures.

WORLD3 is committed to ensuring that all cross-border transfers of Personal Information comply with applicable data protection laws and provide robust protection to users' data. We employ a combination of legal instruments, technical safeguards, and rigorous assessments to secure Personal Information during international transfers, thereby maintaining our commitment to data privacy and security. For further details or specific inquiries, please reach out to us through the contact information provided.

Links to Third-party Websites

In providing our Services, we may offer links to websites operated by third parties, including but not limited to those that might display WORLD3 or Matrix Labs branding. These links are intended to enhance user experience by providing additional resources or services. However, it is essential to recognize the distinctions and limitations of our Privacy Policy in relation to these third-party websites.

1. **Scope of Our Privacy Policy:**

- **Exclusivity:** This Privacy Policy exclusively governs the collection, use, and disclosure of Personal Information within the scope of WORLD3 Services. This encompasses our website, platforms, and any associated online or offline interactions directly managed by us.
- **Third-Party Domains:** Once you access third-party websites through links provided in our Services, this Privacy Policy no longer applies. The data handling practices, privacy standards, and security measures of those websites are beyond our control and responsibility.

2. **Third-Party Website Control:**
   - **Autonomy of Third-Party Sites:** Each third-party website maintains its own privacy policies, terms of use, and data protection practices. Despite any affiliation or partnership with WORLD3, we do not influence or oversee the management of these external sites.
   - **No Endorsement:** The inclusion of links to third-party websites does not imply an endorsement or recommendation of their content, policies, or practices by WORLD3. The presence of such links is solely for user convenience and informational purposes.
3. **User Discretion and Responsibility:**
   - **Due Diligence:** Users are encouraged to exercise due diligence when navigating to third-party websites. This includes reviewing the privacy policies and terms of use specific to those sites to understand how they collect, use, and safeguard Personal Information.
   - **Informed Consent:** Before providing any Personal Information on third-party websites, users should ensure they are comfortable with the site's privacy practices and data security measures. This is crucial for maintaining personal privacy and data integrity.
4. **Risk Management:**
   - **Potential Risks:** Engaging with third-party websites entails certain risks, including differing privacy protections and data handling standards. Users should be aware of these risks and manage their interactions accordingly.
   - **Security Practices:** While WORLD3 strives to partner with reputable third parties, we cannot guarantee the security or confidentiality of Personal Information shared on external sites. Users are advised to take necessary precautions, such as using secure connections and avoiding the submission of sensitive information unless absolutely necessary.
5. **Third-Party Policies:**
   - **Independent Policies:** Third-party websites operate under their own privacy frameworks, which may significantly differ from WORLD3’ s practices. Users should familiarize themselves with these policies to understand how their data will be treated and protected.

- **Accessing Policies:** Most third-party websites provide accessible privacy statements or policies, often found in the footer of their webpages or through designated privacy links. Users are encouraged to read these documents thoroughly.

6. **No Liability:**
   - **Disclaimer of Responsibility:** WORLD3 disclaims any responsibility or liability for the privacy practices, data protection policies, or content of third-party websites accessed through our Services. Any transactions, interactions, or data exchanges conducted on these external sites are solely between the user and the third-party entity.
7. **Future Interactions:**
   - **Continuous Evaluation:** Users are advised to regularly evaluate the privacy practices of any third-party websites they engage with, especially if their services or data policies change over time. Staying informed about these changes can help users make better decisions regarding their data privacy.

While WORLD3 provides links to third-party websites for enhanced service and user convenience, we emphasize that our Privacy Policy does not extend to these external sites. Users are responsible for understanding and assessing the privacy practices of third-party websites and are encouraged to read their privacy policies carefully before engaging or sharing any Personal Information.

Retention

At WORLD3, we adhere to rigorous standards regarding the retention of Personal Information, ensuring compliance with legal obligations and maintaining the integrity and security of data throughout its lifecycle. Our policy on data retention is guided by both legal requirements and our commitment to responsible data management.

1. **Duration of Retention:**
   - **Service Provision:** Personal Information will be retained for as long as it is necessary to provide you with the services you have requested, to maintain communications, and to facilitate your access to our website and associated services.
   - **Business Relationship Documentation:** We will also retain Personal Information to document and support our ongoing business relationship with you. This includes maintaining records related to transactions, interactions, and communications necessary for the effective administration of our services and business operations.
2. **Compliance with Legal Obligations:**

- **Legal Requirements:** We retain Personal Information as needed to comply with applicable legal and regulatory requirements, including those related to tax, financial reporting, and audit obligations. This ensures that we meet our legal responsibilities and can respond appropriately to lawful requests from authorities.
- **Dispute Resolution:** Personal Information may also be retained to manage and resolve disputes, handle claims, and address any legal or regulatory inquiries or investigations. This is critical for protecting our legal interests and those of our users.

3. **Enforcement of Agreements:**
   - **Contractual Obligations:** We retain data to enforce our agreements with users and other parties, including terms of service, privacy policies, and other contractual commitments. This includes data necessary to ensure compliance with these agreements and to address any breaches or violations effectively.
4. **Data Minimization and Deletion:**
   - **Review and Deletion:** We regularly review the Personal Information we hold to ensure it is still necessary for the purposes outlined in this Policy. Once it is reasonable to assume that your Personal Information is no longer required for these purposes, we will either delete it or anonymize it so that it can no longer be associated with you.
   - **Retention Limits:** Retention periods are determined based on the type of data, the purposes for which it was collected, and any legal or regulatory requirements that may mandate specific retention durations.
5. **Security Measures for Retained Data:**
   - **Protection Standards:** Throughout the retention period, we apply robust security measures to protect Personal Information from unauthorized access, use, disclosure, or destruction. This includes both physical and technical safeguards appropriate to the sensitivity of the data.
   - **Access Controls:** Access to retained Personal Information is restricted to authorized personnel who need it for the specific purposes outlined in this Policy.
6. **Exceptions to Deletion:**
   - **Legal Prohibitions:** There may be circumstances where we are legally prohibited from deleting Personal Information, such as when the data is subject to legal holds or other mandatory retention requirements. In such cases, we will continue to protect and manage the data in compliance with applicable laws.
   - **Audit and Compliance:** Data may also be retained for longer periods if necessary for audit purposes or to ensure compliance with our internal policies and procedures.
7. **User Requests:**

- **Access and Deletion Requests:** Users have the right to request access to their Personal Information, as well as its deletion, in accordance with applicable laws. We will respond to such requests in compliance with legal standards and will take appropriate action to honor legitimate requests for data deletion or correction.

8. **Regular Review:**
    - **Retention Policies:** We periodically review our data retention policies and practices to ensure they remain effective and compliant with evolving legal standards and best practices in data management.
    - **Policy Updates:** Any updates or changes to our retention practices will be reflected in updates to this Policy, ensuring transparency and keeping users informed about how their data is managed.

WORLD3 is committed to the responsible retention of Personal Information, balancing the need to comply with legal obligations, maintain business operations, and protect user privacy. By retaining data only for as long as necessary and applying stringent security measures, we strive to uphold the highest standards of data protection and management.

Changes to this Policy

WORLD3 is committed to maintaining the transparency and accuracy of its Privacy Policy to reflect evolving regulatory requirements and industry standards. Consequently, this Policy is subject to periodic review and updates. The following outlines our procedures and commitments concerning changes to this Policy:

1. **Regular Review and Updates:**
    - **Periodic Assessments:** Our Privacy Policy undergoes regular assessments to ensure it remains aligned with current legal requirements, technological advancements, and changes in our services. These assessments are conducted by our compliance team and legal advisors to identify any necessary modifications.
    - **Revisions:** When revisions are required, they are implemented promptly to reflect the most accurate and effective privacy practices. Revisions may encompass changes in data handling practices, new regulatory compliance requirements, or updates to reflect enhancements in our services.
2. **Notification of Changes:**
    - **“Last Updated” Date:** For every update to this Policy, the "Last Updated" date at the beginning of the document will be amended to indicate the most recent revision. This date serves as an immediate reference for users to understand when the last changes were made.

- **Material Changes:** If changes to this Policy are significant, we may provide additional notice to ensure users are fully informed. This may include:
  - **Prominent Notices:** Posting a notice on the homepage of our website or the first page of this Privacy Policy, highlighting the changes. This approach ensures visibility and easy access to the updated information.
  - **Direct Communication:** Sending notifications to users via email to the address on record, detailing the changes. This method provides direct communication to ensure that all users are aware of significant updates and their implications.

3. **Advance Notice for Major Changes:**
   - **Material Modifications:** In cases where changes are material and could substantially affect the handling of Personal Information, we aim to provide advance notice before such changes take effect. This allows users to review the changes and understand how they may impact their interactions with our services.
   - **User Action:** Users will have the opportunity to review these material changes and, where necessary, make informed decisions regarding their continued use of our services. If users do not agree with the changes, they may choose to discontinue their use of the services as outlined in our Terms of Use.
4. **Continued Use of Services:**
   - **Acceptance of Changes:** Continued use of our services following the publication or notification of any changes to this Policy constitutes acceptance of those changes. Users are encouraged to review the Policy periodically to stay informed about how we are protecting their Personal Information.
   - **User Responsibilities:** It is the user’ s responsibility to ensure they are aware of the current version of the Privacy Policy and understand how their Personal Information is managed under any updates.
5. **Transparency and User Engagement:**
   - **Clarity:** We strive to present changes to this Policy clearly and concisely, avoiding technical jargon and ensuring that updates are comprehensible to all users.
   - **Feedback:** Users are encouraged to provide feedback or raise any questions they may have about the changes to this Policy. Our support team is available to address concerns and provide additional information as needed.
6. **Legal Compliance:**
   - **Regulatory Requirements:** Changes to this Policy will always be in compliance with applicable data protection laws and regulations. We take our obligations seriously and ensure that all updates are consistent with legal standards and best practices in data protection.

7. **Historical Versions:**
    - **Access to Previous Versions:** Where appropriate, we may provide access to previous versions of the Privacy Policy to ensure transparency and allow users to review historical changes. This can be useful for users who wish to compare how data practices have evolved over time.
8. **Commitment to Privacy:**
    - **Ongoing Protection:** Our commitment to safeguarding user privacy remains a priority, and any changes to this Policy are made with the intention of enhancing the protection of Personal Information and ensuring compliance with evolving privacy expectations.

Changes to your Information

Accurate and up-to-date Personal Information is critical for the effective operation and compliance of our services at WORLD3. We rely on the precision of the information provided by our users to maintain the integrity of our services and ensure compliance with applicable legal requirements. Therefore, the following outlines the procedures and user responsibilities regarding changes to Personal Information:

1. **User Responsibility for Updates:**
    - **Accuracy and Currency:** It is the responsibility of each user to ensure that the Personal Information they provide to WORLD3 is accurate, complete, and current. This responsibility includes promptly notifying us of any changes or inaccuracies in their Personal Information.
    - **Impact of Inaccurate Information:** Failure to provide accurate and current information can affect the delivery of our services, the effectiveness of our communications, and compliance with legal obligations. Users should be aware that outdated or incorrect information may hinder their ability to utilize our services fully.
2. **Notification of Changes:**
    - **Timely Updates:** Users are required to inform us as soon as possible if their Personal Information changes or if they become aware that the information we hold about them is inaccurate or incomplete. This prompt notification is essential for maintaining the accuracy of our records and ensuring compliance with legal and operational requirements.
    - **Method of Notification:** Users can update their Personal Information or notify us of any inaccuracies by using the contact details provided in this Policy or through their User Account settings, where applicable. Specific methods for updating information may include:

- **Account Settings:** Accessing and updating information directly through the User Account settings on our website or application.
- **Contacting Support:** Contacting our customer support team via email or other designated communication channels for assistance with updating Personal Information.

3. **Verification of Changes:**
   - **Verification Process:** When users notify us of changes to their Personal Information, we may require verification to ensure the authenticity and accuracy of the updates. This verification process helps protect against unauthorized changes and maintains the security of user data.
   - **Supporting Documentation:** In some cases, we may request additional documentation or information to verify the changes. Users should be prepared to provide such documentation if requested, as part of our commitment to data integrity and security.
4. **Legal Compliance:**
   - **Compliance with Regulations:** Ensuring that Personal Information is accurate and current is not only important for operational reasons but also for compliance with data protection laws and regulations. Maintaining accurate records helps us meet our legal obligations regarding data accuracy, retention, and user rights.
   - **Regulatory Requirements:** We are obligated to adhere to regulatory standards that require accurate data management. Users' cooperation in updating their information ensures compliance with these standards and helps avoid potential legal or regulatory issues.
5. **Impact on Services:**
   - **Service Continuity:** Accurate Personal Information is essential for the seamless provision of our services. Changes or inaccuracies in user data may affect service delivery, access to features, and communication efficacy. By keeping their information up-to-date, users help ensure that their experience with our services remains consistent and effective.
   - **Notification of Consequences:** If users fail to update their Personal Information as required, they may experience interruptions or limitations in service access. We may also be unable to fulfill certain legal requirements or respond adequately to user requests without accurate data.
6. **Privacy and Security Considerations:**
   - **Data Security:** Protecting user information is a priority. When processing updates to Personal Information, we adhere to strict security measures to safeguard data against unauthorized access, alteration, or misuse.

- **Confidentiality:** Any updates to Personal Information are handled with the same level of confidentiality and care as the original data. We ensure that all changes are processed in compliance with our privacy and security policies.

7. **User Support and Assistance:**
   - **Contact Points:** Users requiring assistance with updating their Personal Information can contact us through the support channels provided. Our support team is available to help with any questions or issues related to data updates.
   - **Guidance and Resources:** We provide guidance and resources to help users understand how to update their information and the importance of maintaining accurate records. This support helps users navigate the process and address any concerns they may have.

California Shine the Light Law

Under the "Shine the Light" law (Cal. Civ. Code § 1798.83), residents of California are granted specific rights pertaining to the disclosure of their personal information. As part of our compliance with this regulation, we provide the following detailed explanation of your rights and the procedures for exercising them:

1. **Right to Request Information:**
   - **Scope of Request:** California residents are entitled to submit a request, free of charge, to obtain information about the personal data we have disclosed to third parties for their direct marketing purposes. This right applies to the personal data shared during the preceding calendar year.
   - **Frequency of Requests:** Such requests may be made only once per calendar year. Each request should pertain to disclosures made in the prior calendar year.
2. **Contents of Request:**
   - **Attestation of Residency:** Your request must include a statement affirming that you are a resident of California. This attestation is crucial as the rights conferred by the "Shine the Light" law apply exclusively to California residents.
   - **Verification Information:** You must provide a current and valid California address to which we can respond. This information helps us verify your residency and ensures the delivery of our response to the correct address.
3. **Submission of Request:**
   - **Contact Details:** Requests should be directed to us via the contact information specified in this Privacy Policy. Ensure that your request includes all necessary information to facilitate processing, including your full name, California address, and the specific request for information disclosure.

- **Format of Request:** You may submit your request in writing or via email as specified in our contact details. Please use a clear subject line such as "California Shine the Light Request" to expedite the handling of your request.

4. **Response to Requests:**
   - **Timeframe:** We will respond to your request within the legally mandated timeframe. Typically, this will be within 30 days from the receipt of a valid request.
   - **Content of Response:** Our response will detail the categories of personal data disclosed to third parties for direct marketing purposes and provide information about the third parties to whom we have disclosed your personal data in the previous calendar year.
   - **Scope of Disclosure:** Not all data sharing activities are covered by the "Shine the Light" law. Our response will include only the information mandated by the law. We are not required to provide details about data sharing activities that fall outside the scope of direct marketing purposes as defined by the statute.
5. **Exemptions and Limitations:**
   - **Non-Marketing Disclosures:** The law does not obligate us to disclose information about personal data shared for purposes other than direct marketing. Consequently, our response will exclude data disclosures made for operational or transactional purposes, legal compliance, or other non-marketing activities.
   - **One Request Per Year:** As stipulated by law, we are only required to respond to one such request per customer each calendar year. Subsequent requests within the same year will not be fulfilled until the next calendar year.
6. **Additional Considerations:**
   - **Confidentiality:** All responses provided under the "Shine the Light" law are subject to our confidentiality obligations. We ensure that any disclosed information is handled in accordance with our data protection and privacy practices.
   - **No Charge for Requests:** You will not incur any charges for submitting a request or for receiving a response regarding our data sharing practices for direct marketing purposes. This service is provided free of charge to uphold your rights under California law.
7. **Further Information:**
   - **Regulatory Guidance:** For additional details about your rights under the "Shine the Light" law and how to exercise them, you may consult the official resources provided by the State of California, such as the California Attorney General's office or relevant consumer protection agencies.

By providing this comprehensive framework, we aim to ensure transparency and compliance with the "Shine the Light" law, enabling California residents to exercise their rights regarding

personal data disclosure for direct marketing purposes effectively. If you have any questions or need further assistance, please refer to the contact information provided in this Privacy Policy.

Supplemental Notice for Nevada Residents

Under the Nevada Privacy Law (Nevada Revised Statutes Chapter 603A), residents of Nevada are afforded specific rights concerning the sale of their personal information. This section details those rights and provides the procedure for exercising them effectively.

1. **Right to Opt-Out of Sale:**
    - **Scope of Opt-Out:** As a Nevada resident, you have the legal right to opt out of the sale of certain personal information to third parties if the information is intended for licensing or selling. This opt-out right is applicable to personal information as defined under the Nevada Privacy Law.
    - **Definition of Sale:** For the purposes of Nevada law, "sale" refers to the exchange of personal information for monetary consideration by the operator to a third party for the third party to license or sell the personal information to additional third parties.
2. **Procedure to Exercise Opt-Out Rights:**
    - **Contact Information:** To exercise your opt-out rights, please contact us via email at contact@matrixlabs.org. Ensure the subject line of your email reads "Nevada Do Not Sell Request" to expedite processing.
    - **Required Information:** In your email, provide your full name and the email address associated with your account. This information is essential to accurately identify and process your request.
3. **Current Status of Personal Information Sales:**
    - **No Current Sales:** At present, we do not sell your personal information as "sale" is defined under the Nevada Revised Statutes Chapter 603A. Nevertheless, we provide the opt-out mechanism to adhere to statutory requirements and to facilitate your rights under Nevada law.
4. **Clarifications and Assistance:**
    - **Contact for Queries:** If you have any questions regarding the opt-out process or need further clarification about how your personal information is handled, please reach out to us using the contact information provided in this Policy.
    - **Implementation of Opt-Out Requests:** Upon receiving your valid opt-out request, we will promptly update our records and ensure that your personal information is not sold in accordance with your request.
5. **Verification and Confirmation:**

- **Verification Process:** We may implement a verification process to confirm your identity and ensure that the opt-out request is being made by you or an authorized representative. This may involve additional communications to verify the details provided in your request.
- **Confirmation of Request:** Following the successful processing of your opt-out request, you will receive a confirmation email acknowledging that your personal information will not be sold to third parties as per your instruction.

6. **Retention of Opt-Out Status:**
   - **Permanent Effect:** Once you have opted out of the sale of your personal information, this preference will be maintained in our records. Should you wish to change this preference in the future, you can contact us to modify your opt-out status.
7. **Non-Discrimination Clause:**
   - **No Discrimination:** Exercising your right to opt out of the sale of personal information will not affect your ability to use our Services. We will not discriminate against you for exercising this right, and your access to and quality of our Services will remain unchanged.
8. **Additional Provisions:**
   - **Updates to Policy:** This notice and our policies regarding the sale of personal information may be updated from time to time to reflect changes in our practices or legal requirements. We encourage you to review this section periodically to stay informed about your rights and our obligations under Nevada law.
   - **Legal Obligations:** We comply with applicable legal obligations regarding the protection and sale of personal information and ensure that any third parties with whom we interact are also compliant with relevant privacy laws.

By providing this supplemental notice, we aim to ensure that Nevada residents are fully informed about their rights concerning the sale of personal information and the processes for exercising those rights. If you have any concerns or require additional information, please contact us as outlined in this Policy.

Additional Information for EEA/UK Residents

As a resident of the European Economic Area ("EEA") or the United Kingdom ("UK"), you are entitled to certain rights concerning your Personal Information under the General Data Protection Regulation ("GDPR") and the UK Data Protection Act 2018. These rights are designed to provide you with more control over how your personal data is used and to ensure transparency in data processing activities. Below is a detailed elaboration of your rights and the procedures to exercise them.

1. **Right to Be Informed**

You are entitled to receive clear and transparent information regarding the collection, use, and processing of your Personal Information. This right ensures that you are fully informed about how your data is handled and the purposes for which it is used. To fulfill this right, we provide comprehensive details in this Policy. Should you have any additional queries regarding the nature or purpose of data processing, please contact us at the details provided in this Policy.

2. **Right of Access**

You have the right to request and obtain confirmation of whether your Personal Information is being processed, and if so, access to that information along with relevant details regarding its use. This right allows you to understand how and why your data is being used and to ensure it is being processed lawfully. You can request access to your data by contacting us through the provided channels, and we will respond within one month of receiving your request.

3. **Right to Rectification**

If any Personal Information we hold about you is inaccurate or incomplete, you have the right to request that we correct or complete this information. This right enables you to ensure that the data we process about you is accurate. You can make such a request by contacting us, and we will address your request promptly, typically within one month.

4. **Right to Erasure ("Right to be Forgotten")**

Under certain circumstances, you have the right to request the deletion of your Personal Information. These circumstances include situations where the data is no longer necessary for the purposes for which it was collected, where you withdraw consent on which the processing is based, or where the data has been unlawfully processed. Please note that this is not an absolute right and may be subject to legal obligations or other overriding reasons that require us to retain certain information.

5. **Right to Restrict Processing**

You have the right to request that we limit the processing of your Personal Information in specific circumstances, such as when you contest the accuracy of the data or when you object to the processing and we are considering whether our legitimate grounds override yours. This right allows you to control the extent to which your data is processed without requiring full deletion.

6. **Right to Data Portability**

You can request the transfer of your Personal Information to another data controller. This right applies to data that you have provided to us and which is processed by automated means. It allows you to obtain and reuse your data across different services. To exercise this right, please contact us, and we will provide your data in a structured, commonly used, and machine-readable format.

7. **Right to Object**

You have the right to object to the processing of your Personal Information where such processing is based on legitimate interests or for direct marketing purposes. Upon receiving your objection, we will cease processing your data for these purposes unless we can demonstrate compelling legitimate grounds for the processing that override your interests, rights, and freedoms, or for the establishment, exercise, or defense of legal claims.

8. **Right to Lodge a Complaint**

If you believe that our processing of your Personal Information violates applicable data protection laws, you have the right to file a complaint with your local data protection authority. In the UK, the Information Commissioner' s Office (ICO) handles such complaints. Details on how to contact the ICO can be found on their website https://ico.org.uk.

9. **Right to Withdraw Consent**

Where we rely on your consent to process your Personal Information, you have the right to withdraw that consent at any time. Withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal. You can withdraw consent by contacting us at the contact details provided in this Policy.

Request Submission and Response Time

To exercise any of these rights, please submit your request in writing or via email to the contact details provided below. We will generally respond to your request within one month. However, if your request is complex or involves numerous requests, we may extend this period by an additional two months, in which case you will be informed of the extension and the reasons for the delay.

Fees and Refusal of Requests

While we typically handle requests free of charge, we reserve the right to charge a reasonable fee for repetitive, excessive, or unfounded requests, or for additional copies of the same information. Alternatively, we may refuse to act on such requests. In any case, we will inform you of any fees or reasons for refusal in advance.

By understanding and exercising these rights, you can ensure that your Personal Information is handled in accordance with your expectations and applicable legal requirements. If you have any concerns or require further information, please contact us as outlined in this Policy.

Contact Information:

For questions or issues related to these Terms, please contact us at: contact@matrixlabs.org