

UTOPPIA, INC.

PRIVACY POLICY

Last Updated: This Privacy Policy shall be effective from July 23rd, 2026.

This is the privacy statement for Utoppia Inc. and its affiliates and subsidiaries (collectively, “Utoppia,” “we,” “us,” or “our”).

Utoppia respects and protects the privacy of visitors to our website <https://www.utoppia.com> and our customers who use our services in our mobile phone application (the “Platform App”) (individually or collectively, “you”, “Customer” or “User”) which gives you access to our services and services provided by independent third-party service providers (the “Third-Party Service Providers” and “Third-Party Services” as defined within the [Terms of Service](#)).

To ensure transparency, this privacy policy describes how Utoppia collects, uses and discloses personal information, and your choices regarding this information (“Privacy Policy”).

If you are reading this Privacy Policy, it means you have applied for or created or will create an account (“Account”) using the Platform App and you are going to use the Platform App and the Third-Party Services under the Terms of Service.

Please take a moment to read through this Privacy Policy. If you have any specific questions about it, you’re welcome to contact us at privacy@utoppia.com.

1. Scope and applicability

This Privacy Policy applies to the services provided on the Platform App or our website or on any Utoppia API or third-party applications relying on such an API, and related services (collectively, the “Services”).

This Privacy Policy applies to Utoppia’s processing of any information or data that could potentially identify a specific individual (“Personal Information”) when using our Services.

This Privacy Policy does not apply to online websites or services that we do not own or control. Each Third-Party Service Provider is solely responsible for its own privacy policy (individually or collectively, the “Third-Party Provider Privacy Policy”). See the Third-Party Provider Privacy Policy at: [BVNK's Privacy Policy](#); [Lead Bank's Privacy Policy](#); [Payblr's Privacy Policy](#); [W2B's Privacy Policy](#); [Alpaca's Privacy Policy](#); [Auntapi's Privacy Policy](#).

In the event of any conflict between this Privacy Policy and any Third-Party Provider Privacy Policy, the Third-Party Provider Privacy Policy shall govern solely with respect to the relevant Third-Party Services, and this Privacy Policy shall govern in all other respects.

By using or accessing our Platform App, our website and our Services in any manner, you acknowledge that you have accessed and read our Privacy Policy and you acknowledge that you have been informed of Utoppia’s collection, use and disclosure of your Personal Information.

If you do not agree with the terms of this Policy, do not access or use the Services or any other aspect of our business.

2. When and How We Collect Information

We may collect the following information or data, which may be considered Personal Information, from you when:

Data you provide:

- You apply for or create an Account with us;
- You use our Services;
- You contact us for customer service or other purposes;
- You engage with interfaces such as our artificial-intelligence (“AI”) chatbots;
- You submit an entry in a contest sponsored by us, respond to one of our surveys, or participate in any feature of our website or Platform App; and/or
- You provide us with user reviews, comments, feedback or other submissions.

Data we collect:

- You visit and interact with our Platform App or website;
- You apply for or create an Account with us;
- You view email communications;
- You interact with Utoppia’s social media; and/or
- You click through a marketing promotion.

3. What Information we collect

We collect the following categories of personal information:

Data you provide:

- Contact and Demographic Information: such as your full legal name, date of birth, nationality, residential address, email address, and phone number.
- Identification Information: such as your driver’s license, federal/state ID card, Social Security Number, Tax ID number, photograph(s), or other government-issued ID information.
- Know your Customer and due diligence information, including but not limited to, proof of address documents (e.g., bank statements and utility bills); employment or professional information (e.g., employer, job title/position); and source of wealth (e.g., pay stubs, contracts, invoices, among other documentation).
- (For corporate clients) Institutional Information: such as Employer Identification Number (EIN), proof of legal formation (e.g., articles of incorporation/by-laws), and/or identification information for beneficial owners.
- Correspondence: such as your feedback, quiz, questionnaire, and other survey responses, and information you provide to our support teams, including via our chatbot(s).
- Information associated with your use of our AI chatbot: such as the input and output information including prompts used, market research or uploaded information.
- Biometric Data: such as facial recognition and facial geometry data derived from photographs or videos you submit to us during the onboarding process. We only use biometric data to verify

your identity for security and compliance purposes. You can learn more about our biometric data practices in our Biometric Data Privacy Policy.

Data we collect:

- Financial Information: such as your bank account number, external financial institution name, account name, account type, branch number, account number, routing number, international bank account number ("IBAN"), information, data, passwords, authentication questions, materials or other content, transaction and available balance information, transaction history, and/or trading data.
- Background Check Data: background check information including credit and criminal checks, supporting research, and screenings, to the extent required or permitted by local law;
- Recipients' or Senders' Data: when you send or request money through the Platform App Services, we may collect data such as name, postal address, telephone number, IP address, date of birth, and financial account information about the recipient or sender of the funds;
- Log Data: our servers may automatically collect information about your visit to the Platform App, including IP addresses and associated information, browser type and settings, the date and time the Third-Party Services were accessed and used, information about browser configuration and plugins, language preferences.
- Device Information: your device "fingerprint" (e.g. hardware model, operating system and version, unique device identifiers and mobile network information) when you access our Platform App.
- Location Information: we may receive information from you that helps approximate your location, such as using an IP address received from your browser to determine an approximate location. Further, we may also collect location information from devices in accordance with the consent process provided by your device.
- Transaction Information: including information about the transactions you make using Third-Party Provider Services, such as the names of the recipient, transaction amount, and timestamp.
- Website or App Metadata and Analytics: including Internet Protocol (IP) addresses and location data, device information, date/time of visits, new or returning visits, products viewed, page response times, URL clickstreams, how long you stay on our pages, what you do on those pages.
- Cookies and Other Tracking Technologies: We, and third parties we authorize, may use cookies, web beacons, and similar technologies (collectively, "cookies") to record your preferences, track the use of our Platform App or website, and collect information about the use of the Third-Party Services, as well as about our interactions with you. This information may include IP addresses, browser type, Internet Service Provider (ISP), referring/exit pages and operating system, date/time stamp, and clickstream data, and information about your interactions with the communications we send to you. We may combine this automatically collected log information with other information we collect about you. Learn more about our cookie use below, or see Utoppia's Cookie Policy for additional details on how we handle cookies.
- Blockchain Data: We may analyze public blockchain data, including wallet addresses, transaction IDs, timestamps of transactions or events, transaction amounts, and digital signatures.
- Additional Information from third-parties, such as information about you from other sources as required or permitted by applicable law, including identity verification services and public

databases. We may combine the information collected from these sources with the information we get from our Services and Third-Party Service Providers in order to verify your identity, comply with our legal obligations, and ensure our Platform App and Services are not used fraudulently or for other illicit activities.

4. How We Use Information

We use your information, including your Personal Information, in accordance with your instructions, including any applicable terms you agree to in our Terms of Service, and as required or restricted by applicable law.

If you stop using the Services, we reserve our ability to retain and access the data as provided in this Policy. We will continue to use and disclose such data in accordance with this Privacy Policy.

All data is stored in encrypted format in Utoppia's database.

We use machine learning and facial recognition to verify the legitimacy of your identification documents, verify the factualness and credibility of the information you provide to us, and avoid fraud, by, among other actions, comparing biometric data with data previously or separately obtained. Based on the submitted identification document, Utoppia programmatically creates a feature vector of the face displayed in such document and stores it in encrypted format in Utoppia's database. The vector cannot be used to reconstruct the original image. When a new user creates an Account, Utoppia programmatically compares that user's vector against others in its database to help detect potential cases of identity theft. As with all data, Utoppia does not sell or rent the image, likeness, or vector to anyone, including marketers or other third parties, and does not use your data for commercial purposes other than identity verification, financial loss mitigation, and regulatory compliance.

We may also use the information we collect for:

Providing our Services. We may use the information we collect to provide, personalize, maintain, and improve our products, the Third-Party Services, including as described in the Terms of Service. This includes using information to:

- operate, maintain, customize, measure, and improve our Services, and manage our business;
- create and update Accounts;
- send information including confirmations, notices, invoices, technical notices, updates, security alerts, and support and administrative messages;
- provide interactive responses and content through our AI chatbot that includes market research and portfolio-specific analysis;
- collect inferences about your use of our Services; and
- create de-identified or aggregated data.

Safety and Security. We may use your information to help maintain the safety, security, and integrity of our Services, including to:

- protect, investigate, respond to, and deter against fraudulent, unauthorized, or illegal activity;
- monitor and verify identity or service access;
- protect against spam, malware, or security risks;

- perform internal operations necessary to provide our Services, including to troubleshoot software bugs and operational issues;
- enforce our agreements with Third-Party Service Providers, third parties, and address violations of our Terms of Service or agreements for other services; and
- comply with applicable laws and regulations.

Customer Support. We may use information we collect to provide customer support, including to:

- direct questions to the appropriate customer support person;
- communicate with you, including via social media channels;
- investigate and address your concerns; and
- monitor and improve our customer support responses and processes.

Research and Development. We may use the information we collect for testing, research, analysis, and product development to improve your experience, enhance the safety and security of our Platform App and website, improve our ability to prevent the use of our Services for illegal or improper purposes, develop new features and products in connection with our Platform App and website.

Legal and Regulatory Compliance. Many of our Services are subject to laws and regulations requiring us to collect, use, and store your personal information in certain ways. For example, we must identify and verify Customers using our Services in order to comply with anti-money laundering and anti-terrorism laws. This may include collection and storage of your photo identification. We also use third parties to verify your identity by comparing the personal information you provide against third party, authoritative sources and databases, including public records. We may also use the information we collect to investigate or address claims or disputes relating to use of our Services, or as otherwise allowed by applicable law, or as requested by regulators, government entities, and official inquiries.

Direct Marketing. We may use the information we collect to market our Services to you. This may include sending you communications via emails or mobile in-app notifications about our Services, features, promotions, surveys, news, updates, and events; managing your participation in these promotions and events; and to deliver targeted marketing. Our marketing will be conducted according to your advertising and marketing preferences and as permitted by applicable law.

5. How and why we disclose information

We may disclose your information, including your Personal Information, in the following circumstances:

With Your Consent. You may permit us to disclose your Personal Information with others for any other purposes disclosed to you with your consent.

With Our Affiliates. Where appropriate, we may disclose your information with our affiliates, in the course of conducting business and offering our Services to you.

Third-Party Service Providers and business partners: We may engage third parties to perform certain functions on our behalf. To do so, we may disclose Personal Information to our Third-Party Service Providers, as well as service providers and vendors, in order to operate, improve, and personalize the Services, including to administer referral programs. We may also share Personal Information for other technical and processing functions, such as sending e-mails on our behalf or on behalf of our Third-Party Service Providers, fulfilling orders, technical support, for analytics, and for marketing and advertising

purposes. Where we share Personal Information with the Third-Party Service Providers and business partners, we will require them to honor this Privacy Policy.

Where you have provided or requested information regarding a particular product or service offered by the Third-Party Service Providers, we may share certain Personal Information with such Third-Party Service Providers. For example, when you create an Account, we may share certain information with the Third-Party Service Providers to verify your identity and eligibility to participate in certain Third-Party Services.

To comply with our legal obligations. We may disclose your information with courts, law enforcement authorities, regulators, attorneys or other parties: (i) to comply with laws and legal obligations; (ii) for the establishment, exercise, or defense of a legal or equitable claim; (iii) to respond to law enforcement and regulatory requests, including (a) when we are compelled to do so by a subpoena, court order, search or seizure warrant, or similar legal procedure, or (b) for international law enforcement requests, pursuant to a mutual legal assistance treaty or letter rogatory; (c) to investigate violations of our Terms of Service or other applicable policies; or (d) to report suspected illegal activity or to assist law enforcement in the investigation of suspected illegal or wrongful activity.

With Third-Party Identity Verification Services. We may disclose your information with third party identity verification service providers for the purposes of identity verification, fraud prevention, and denial of service to persons presenting an unacceptable level of fraud, money-laundering or terrorism-financing risks. These service providers confirm your identity by comparing the information you provide us to public records and other authoritative third-party databases (e.g., credit bureaus). These providers may create derivative data based on your personal information that they can use in connection with provision of identity verification and fraud prevention services. We do not control these providers' privacy policies and we contractually require these service providers to only use your information in accordance with our legal agreements.

We use SardineAI Corp. ("Sardine") for identity verification services to identify and authenticate you when you apply for, create or reactivate an Account with us. Specifically, Sardine will verify that the selfie you provide matches the photo on your government-issued ID. The information collected during this process may constitute biometric data (to learn more about our Biometric Data Practices, please review our Biometric Data Privacy Policy). To learn more about Sardine's privacy practices, please visit [Sardine's Privacy Policy](#). By submitting your information, you agree to Sardine's Privacy Policy.

For Regulatory Compliance Purposes. We may disclose your information to comply with these obligations, including with Third-Party Service Providers who use your Personal Information to determine whether or not to provide the Third-Party Services. Your information may be shared with Third-Party Service Providers for their compliance purposes.

With service providers. We may disclose your information on a confidential basis with service providers who help facilitate business operations such as marketing, security, information technology services, or providing certain AI features like chatbots. Our legal agreements require these service providers to only use your information according to our instructions.

We may disclose your information with our support platform provider, Zendesk Inc. who may receive information about you, your account and the contents of your communication as well as metadata

including cookie data uniquely associated with you. Such information will not be used for any purpose other than to support us, but are also subject to the service provider's applicable terms including their [privacy policy](#).

We may also disclose your information with our AI chatbot provider Google Gemini and/or Anthropic. These service providers may receive information about you, your Account and the contents of your communication as well as metadata including usage data uniquely associated with you. Such information will not be used for any purpose other than to support us in providing the AI chatbot, but are also subject to the Google Gemini and/or Anthropic's applicable terms including their privacy policy located at: [Google Gemini](#) and [Anthropic](#).

To Detect and Prevent Fraud. We may disclose your information with law enforcement, government agencies, regulators, financial institutions, industry partners, and other third parties in order to detect, prevent, and report actual or potential fraud, money laundering, terrorist financing, unauthorized transactions, and other financial crimes and illicit activities.

For Advertising Purposes. Certain data protection laws may classify service providers engaged in certain advertising services as third parties or independent controllers. You have the right, where applicable under the relevant laws, to restrict these types of advertising service providers' use of your personal information. Utoppia does not sell personal information for monetary consideration in connection with these advertising services, although the disclosure of personal information to such providers may be considered a sale or a similar form of data sharing under applicable data protection laws.

With Our Professional Advisors. We may disclose your information with our professional advisors such as accountants, auditors, lawyers, insurers, in order to complete third party audits and/or to comply with our legal and regulatory obligations.

With Other Utoppia Customers. We do not disclose your information to other Users for peer-to-peer transactions unless you choose to make your Utoppia Account discoverable. If you wish to allow other Customers to find your account for peer-to-peer transactions, you may go to Profile Account→Account Information→Privacy Settings → Set your privacy settings based on your preferences and toggle on the options for email and/or phone number. Your account will not be searchable by other Customers unless you affirmatively enable these settings.

During a change to our Business. If we engage in a merger, acquisition, bankruptcy, dissolution, reorganization, sale of some or all of our assets or stock, financing, public offering of securities, acquisition of all or a portion of our business, a similar transaction or proceeding, or steps in contemplation of such activities, some or all of your information may be disclosed or transferred.

Aggregated or De-identified Data. We may create de-identified or anonymous data from Personal Information by removing certain data components (such as your name or email address) that makes the data personally identifiable to you, or through obfuscation. We may disclose aggregated and/or anonymized data with third parties for their own uses.

6. International Transfers.

We may store and process your personal data in countries other than the country in which it was originally collected. Where we transfer personal data across borders, we will implement appropriate

safeguards and comply with applicable data protection laws to ensure that your personal data remains adequately protected. Where required, we will rely on legally recognized data transfer mechanisms or other appropriate safeguards permitted under applicable law. By using the Services, you acknowledge the data processing practices described in this Privacy Policy.

7. Security.

We maintain administrative, technical, and physical safeguards (“Security Controls”) designed to protect the personal information we maintain against unauthorized access or disclosure. While no system is completely secure due to real-time and emerging cyber threats and bad actors, we take reasonable steps to secure your information.

When registering for our Services, choose a complex password and turn on advanced security features, such as two-factor authentication. Never share your account credentials with third-parties and submit a customer support ticket to support@utoppia.zendesk.com if you become aware of unauthorized access to or use of your account.

You are responsible for all activity on the account that is associated with your login credentials.

8. Data Retention.

Utoppia retains your Personal Information for as long as is necessary for the purposes set out in this Privacy Policy and to the extent necessary to comply with our legal and regulatory obligations (i.e., if we are required to retain your data or the information you provided to us to comply with applicable laws, including fraud, anti-money-laundering, anti-terrorism, or other financial laws and regulations). In addition, we will retain and use your personal information to resolve disputes and enforce our legal agreements and policies.

To determine how long we will retain your personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of your Personal Information, the purposes for which we process your personal information, and whether we can achieve those purposes through other means, and applicable legal, regulatory, tax, accounting, or other requirements.

Utoppia will retain your Personal information for marketing purposes, where applicable, until you unsubscribe from our marketing communications. At that time, we may retain the Services’ usage data for internal analysis purposes. Usage data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of our Services, or we are legally obligated to retain this data for longer periods.

Utoppia will retain biometric data as part of Customer identification information for the retention period required by financial laws and regulations. You can learn more about our biometric data practices in our Biometric Data Privacy Policy.

Additionally, Third-Party Service Providers may also retain your information to perform certain services or processes (e.g., AI assistant technologies, Know Your Customer, etc.) in accordance with applicable laws and regulations (e.g., the Bank Secrecy Act), and in compliance with contractual obligations and their own Third-Party Privacy Policy.

Utoppia limits access to your information to employees that have a business reason to know such information, and further implements security practices and procedures designed to protect the confidentiality and security of such information and prohibit unlawful disclosure of such information in accordance with its policies.

9. Your Privacy Rights.

It is Utoppia's policy to offer certain privacy rights to all individuals, regardless of whether a statutory right exists. The rights that Utoppia offers to all individuals include the following:

Right to know: you have the right to request what Personal Information we collect, use, disclose, or share about you, as applicable.

Right to access/portability: you can request access to and/or a copy of the personal information that we maintain about you.

Right to delete: you can ask us to delete the Personal Information that we have collected or maintain about you, subject to exceptions. Please note that we are required to retain certain Personal Information and related data to comply with our legal obligations, including compliance with recordkeeping requirements contained in anti-money laundering, anti-terrorism, or other financial laws and regulations.

Right to correct: you can ask us to correct inaccurate personal information we maintain about you. To request corrections to your personal information, please contact customer support at support@utoppia.zendesk.com. You can also update certain account profile information by logging into your Account.

Right to opt-out: you can opt out of certain uses of your personal information:

Marketing and Promotional Communications. If you would like to stop receiving marketing or promotional messages, notifications, or updates, you may do so by following the unsubscribe instructions that appear in these email communications, or you may contact us at privacy@utoppia.com to opt out of direct marketing. Please be advised that you may not be able to opt out of receiving certain service or transactional messages from us, including legal notices.

Targeted Advertising Using Cookies, Email, or other identifiers: you may opt out of targeted advertising.

You can exercise these rights by contacting us at privacy@utoppia.com or by submitting a privacy rights request to support@utoppia.zendesk.com. To protect your privacy and security, we may request specific information from you to help us verify your identity before complying with your request. We are not obliged to provide or to delete any information pursuant to your request if we are unable to adequately verify your identity.

Limit the Use and Disclosure of Your Sensitive Personal Information. Utoppia only collects that sensitive personal information which is necessary for us to provide our Services. As such, limiting our use of your sensitive personal information would result in us not being able to provide our Services.

10. Controller Designation.

Utoppia does not currently have a nexus to the European Union sufficient to trigger obligations under the General Data Protection Regulation (“GDPR”), and Utoppia does not process personal information of U.S. residents. Utoppia will update this determination if its processing activities or user base change such that these frameworks become applicable.

11. Online Tracking Opt-Out Guide.

Like many companies, we use cookies, pixels, web beacons, SDKs, and other tracking technologies (“cookies”) to collect information about your browsing activities, your interactions with our website and Platform App, and to serve tailored ads. You can opt out of our use of cookies via by emailing us at privacy@utoppia.com.

To learn more about our use of cookies and similar tracking technologies, visit our Cookie and other Technologies Policy.

Additionally, if we have collected your email address or other identifier, it may be used for tailored advertising on other websites, including through social media. To opt out of this use, please email us at privacy@utoppia.com or submit a privacy rights request to support@utoppia.zendesk.com.

12. Mobile Privacy.

The Platform App uses software code provided by our business partners (software development kits or SDKs) that let our software interact with the services those partners provide. Sometimes these interactions will involve that business partner collecting some information from the device on which the software is run.

To learn more, visit our Cookie and other Technologies Policy or email us at privacy@utoppia.com.

13. Children’s Privacy.

We do not allow use of our Services and access to the Platform App by anyone younger than 18 years old. If you learn that anyone younger than 18 has unlawfully provided us with Personal Information, please contact us at privacy@utoppia.com and we will take steps to delete such information, close any such Accounts, and prevent the Customer from continuing to use our Services/Platform App.

14. “Do Not Track” Signals.

Some internet browsers incorporate a “Do Not Track” feature that signals to websites you visit that you do not want to have your online activity tracked. Given that there is not a uniform way that browsers communicate the “Do Not Track” signal, the Platform App does not currently interpret, respond to or alter its practices when it receives “Do Not Track” signals.

15. Links to Third-Party Sites.

Our Platform App may contain links to other websites. We do not exercise control over the information you provide or is collected by Third-Party Service Providers. We encourage you to read the Third-Party Privacy Policies you visit.

16. Amendments.

We may revise and update this notice from time to time at our sole discretion. Where appropriate, we may provide advance notice of an update. You agree that we may provide notice of updates by posting a new notice on the Services/Platform App and that your subsequent use of the Services/Platform App constitutes agreement to the updated policy.

17. Contact Us.

Please contact us if you have any questions about this Privacy Policy or if you are seeking to exercise any of your privacy rights.

You may contact us at privacy@utoppia.com or at phone number +1 (650) 495-2468 or at our mailing address: 601 Brickell Key Dr., Suite 501, Miami, FL 33131, United States of America.

Biometric Data Privacy Policy

Effective as of July 23rd, 2026.

Utoppia Inc. and its affiliates and subsidiaries (collectively, “Utoppia,” “we,” “us,” or “our”) have instituted the following policy related to any biometric data that we collect.

If you are reading this Biometric Data Privacy Policy, that means you have [applied for] or created or will create an account (“Account”) using the Platform App and you are going to use the Platform App and the Third-Party Services under the Terms of Service as defined therein <https://storage.googleapis.com/utoppia-static-files/UtoppiaToS.pdf>.

In addition to the information we have provided you in our Privacy Policy, we want to help you better understand how Utoppia collects and treats biometric data.

Utoppia cares about the security of your personal information and seeks to protect you and us against fraud. Where permitted by law, Utoppia and certain of our service providers use ID scanning and facial recognition technology to verify your identity and safeguard personal information as part of our security, compliance, and fraud prevention efforts.

This notice describes our collection and use of biometric data.

Definition

As used in this policy, “biometric data” means data generated by the technological processing, measurement, or analysis of an individual’s biological, physical, or behavioral characteristics processed for the purpose of uniquely identifying an individual, including but not limited to a fingerprint, a voiceprint, scans or records of eye retinas or irises, facial mapping, facial geometry, facial templates, or other unique biological, physical, or behavioral patterns or characteristics, or as otherwise defined by law. Unless such data is used for identification purposes, “biometric data” does not include a digital or physical photograph, an audio or voice recording, or any data generated from a digital or physical photograph or an audio or video recording.

Information Collected

When you consent to Utoppia’s use of your biometric data, Utoppia (or service providers, such as technology vendors, working on our behalf) collects face scan information—face geometry data and related information—necessary to accomplish the purposes stated in this policy, as disclosed at the time of collection, and/or in our Privacy Policy. Unless required by law, Utoppia does not otherwise collect, use, store, or disclose your biometric data without your consent.

Use of your Biometric Data

We use your biometric data to verify or authenticate your identity, including when you apply for, create or reactivate your Account, to detect and prevent fraud, and to comply with applicable anti-money laundering and sanctions screening obligations (“AML Regulations”). Subject to the storage and retention guidelines below, we store and use your biometric data for these purposes for the duration of your engagement with us or as otherwise permitted by law.

Collection

By enabling use of your device's camera or other identification technology for the purposes of biometric data collection, you are authorizing Utoppia and/or our service providers to use your device technology, Internet connection, and any associated communications protocols to collect and share biometric data with Utoppia. Utoppia's authorized service providers are under contract to collect and/or store such information on Utoppia's behalf, and will not otherwise use your device-specific authorization to collect or use information for any other purposes without your specific consent.

Disclosure

Unless otherwise required by law, your biometric data is accessible only to us and our authorized service providers, which only process the data you provide us on our behalf to accomplish the purposes above, or to third parties engaged by Utoppia to audit or assess compliance with AML Regulations.

We use SardineAI Corp ("Sardine") for identity verification services to identify and authenticate you when you apply for, create or reactivate an Account with us. Specifically, Sardine will verify that the selfie you provide matches the photo on your government-issued ID. The information collected during this process may constitute biometric data, including facial recognition data and mathematical representations of your facial geometry. To learn more about Sardine's privacy practices, please visit [Sardine's Privacy Policy](#). By submitting your information, you agree to Sardine's Privacy Policy. We may disclose your biometric data to our authorized service providers or other third parties if:

You or your legally authorized representative consent to the disclosure;

The disclosure is required pursuant to a valid warrant, subpoena, or court order issued by a court of competent jurisdiction.

Retention and Storage

Utoppia will collect, store, transmit, and protect your biometric data using a reasonable standard of care that is at least as protective as the way Utoppia collects, stores, transmits, and protects other confidential and sensitive personal information.

Utoppia will retain biometric data for the retention period required by laws and regulations. Unless required by a valid warrant, subpoena, or as otherwise required by law to maintain any specific biometric data for longer, we will securely delete biometric data at the end of such retention period(s), rendering it no longer available for inspection or access. Our identity verification service providers may retain your biometric data until one of the following events occurs: the identity verification purposes for the collection have been satisfied or in accordance with the applicable contract, which may state the same retention period required by laws and regulations.

Please contact us if you have any questions about this Policy or if you are seeking to exercise any of your statutory rights.

You may contact us at privacy@utoppia.com or at phone number +1 (650) 495-2468 or at our mailing address: 601 Brickell Key Dr., Suite 501, Miami, FL 33131, United States of America.

Cookie and other Technologies Policy

Effective as of July 23rd, 2026.

This Policy explains how Utoppia Inc. and its affiliates and subsidiaries (collectively, “Utoppia,” “we,” “us,” or “our”) uses cookies and similar technologies when you visit our website at <https://www.utoppia.com> or when you use the Platform App (collectively, the “Services”).

This policy explains what cookies are, how and why we use them, and how you can exercise your options to limit our use of cookies. For more information on our privacy practices, please visit our Privacy Policy.

Cookies and Other Technologies

A cookie is a small data file that is stored on your computer or other device when you visit certain websites. Cookies help to track user-specific information and activities to ensure a consistent and efficient experience for visitors, and perform essential functions such as allowing users to register for an account and remain logged in. Cookies may be set by the site that you are visiting (known as “first party cookies”), or by third parties, such as those who serve content or provide advertising or analytics services on the website (“third party cookies”). For general information about cookies (including how to disable/enable them), visit <https://allaboutcookies.org/>. We may also employ other technologies including tracking pixels and code snippets that interact with external services to record online behaviors; we refer to cookies, pixels, and other similar technologies as “cookies” herein.

How We Use Cookies

We use cookies for a number of different purposes. Some cookies are necessary for technical reasons; some help us identify user behavior so that we may provide a more convenient and personalized experience for both visitors and registered users; and some allow the display of advertising from selected third party networks. Some of these cookies may be set when a page is loaded, or when a visitor takes a particular action.

In addition, we may use cookies, emails, or other identifiers for targeted advertising on other websites, including on social media platforms. To opt out of this use, please email us at privacy@utoppia.com.

Categories of Cookies

a. Our Platform App uses Google Analytics, a web analytics service provided by Google, Inc. Google Analytics uses Cookies or other tracking technologies to help us analyze how users interact with our website and Services, compile reports on their activity, and provide other services related to their activity and usage. The technologies used by Google may collect information such as your IP address, time of visit, whether you are a returning visitor, and any referring website. The technologies used by Google Analytics do not gather information that personally identifies you. The information generated by Google Analytics will be transmitted to and stored by Google and will be subject to Google’s privacy policies. To learn more about Google’s partner services and to learn how to opt-out of tracking of analytics by Google, click [here](#).

c. Our Platform App uses Google reCAPTCHA, which is a free service that protects websites from spam and abuse using advanced risk analysis techniques to tell humans and bots apart. Google reCAPTCHA works differently depending on what version is deployed. For example, you may be asked to check a box

indicating that you are not a robot or Google reCAPTCHA may detect abusive traffic without user interaction. Google reCAPTCHA works by transmitting certain types of information to Google, such as the referrer URL, IP address, visitor behavior, operating system information, browser and length of the visit, cookies, and mouse movements. Your use of Google reCAPTCHA is subject to Google's Privacy Policy and Terms of Use. More information as to Google reCAPTCHA and how it works is available [here](#).

We use the following types of cookies:

Necessary Cookies. These cookies are essential for our Services to perform basic functions and are necessary for us to operate certain features.

Functional Cookies. These cookies are used to understand and analyze the key performance indexes of our website and Platform App which helps in delivering a better user experience for visitors. They also enable our website and Platform App to remember information about your preferences such as your selected language.

Analytics Cookies. These cookies help us understand how visitors interact with our website and Platform App by collecting and reporting information about your visit, including the pages viewed and time spent on the website and Platform App.

Advertisement Cookies. These cookies are used to remember a visitor to our website or Platform App in order to display ads that are relevant and engaging to you on other websites, as well as limit the number of times you see an advertisement. These cookies also help us measure our advertising or email marketing campaigns' effectiveness. You can learn more about how to opt out of these cookie uses below.

How to Opt Out of Our Cookie Use

You can opt out of cookie use in the following ways:

Through your browser. You can adjust your browser settings so that your browser blocks all or some cookies. You can also delete cookies that have already been placed. Please note that our website or Services may not recognize automated browser signals regarding tracking mechanisms, such as "do not track" instructions.

Through industry-wide opt-out mechanisms. Consumers can submit an industry-wide opt-out request for interest-based advertising through the Digital Advertising Alliance's (DAA) opt-out website which can be found at optout.aboutads.info.

Platform App Tracking

The Platform App uses software codes provided by our mobile application business partners (software development kits or SDKs) that let our mobile application software interact with the services those partners provide. Sometimes these interactions will involve that business partner collecting some information from the device on which the software is run.

To view our Platform App privacy disclosure:

On iOS:

Open the App Store. Go to the Platform App page. Scroll to the App Privacy section. Click See Details.

On Android:

Open Google Play. Browse or use the search bar to find the Platform App. Click on the app. Under Data safety, you'll find a summary of the app's data safety practices.

To opt out of 'tracking' through your mobile operating system:

On iOS:

When you download and open a new app, you'll get a notification that asks if you want to let the app track your activity across other companies' apps and websites. You'll also see information about what the app would track. You can tap Ask App not to Track to block that activity or Allow.

For apps that you've already downloaded and may have tracking permissions set up for, you can opt out of tracking if you go to Settings, tap an app, and then tap to turn off Allow Tracking. Alternatively, you may go to Settings > Privacy > Tracking. There you will see a list of apps that have requested permission to track your activity. You can tap to turn tracking on or off for each app.

On Android:

Go to the Settings app and navigate to Privacy > Ads. Tap Delete advertising ID, then tap it again on the next page to confirm. This will prevent any app on your phone from accessing it in the future.

Changes to this Policy

We may revise this Policy from time to time. If we make any changes, we will change the Last Updated date above. We encourage you to review and revisit this Policy to stay informed.

Contact Us

You may contact us at privacy@utoppia.com or at phone number +1 (650) 495-2468 or at our mailing address: 601 Brickell Key Dr., Suite 501, Miami, FL 33131, United States of America.