VRAL.IO Privacy Policy

Effective Date: August 7, 2025
Last Updated: August 7, 2025
At VRAL.IO, we are committed to protecting your privacy. This Privacy Policy explains how VRAL.IO ("VRAL.IO," "we," "us," "our," or the "Company") collects, uses, shares, and protects your Personal Data when you access or use our AI-powered creative platform, including our website, mobile applications, AI-powered creation tools, business management features, payment processing systems, token-based economy, and all related services, features, content, and functionality (collectively, the "Platform" or "Services").

By accessing or using any part of the VRAL.IO Platform, you acknowledge that you have read, understood, and agree to be bound by the practices and policies outlined in this Privacy Policy. Your use of VRAL.IO's Services is at all times subject to our Terms of Service, which incorporates this Privacy Policy. Any terms used in this Policy without defining them have the definitions given to them in the Terms of Service.

If you have a disability and require this Privacy Policy in an alternative format, please contact us at privacy@VRAL.IO.com.

Table of Contents

11. Contact Information

1. What This Privacy Policy Covers

This Privacy Policy covers how we treat Personal Data that we gather when you access or use our Services. "Personal Data" means any information that identifies or relates to a particular individual and also includes information referred to as "personally identifiable information" or "personal information" under applicable data privacy laws, rules, or regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).[1]

This Privacy Policy does not cover the practices of companies or individuals we do not own or control, including third-party websites or services linked from our Platform, or the practices of Creators who act as independent data controllers for their customer data.

2. Personal Data We Collect

We collect Personal Data about you from various sources, including directly from you, automatically through your use of our Services, and from third parties. The categories of Personal Data we collect depend on your relationship with VRAL.IO (e.g., Creator, Customer, or Website Visitor).

2.1 Categories of Personal Data We Collect

Over the past 12 months, we have collected and continue to collect the following categories of Personal Data:

Category of Personal Data	Examples of Specific Data Points

Account Information	Name, username, email address, phone number, physical address (P.O. boxes not accepted for payment processing), date of birth, government-issued ID (for verification), tax identification information (for Creators), business registration documents (for business accounts)
Profile Information	Information you put into your profile and updates, including images, tags, text updates, links to third-party websites or content, AI Avatar details, and AI-Generated Content
Transaction Data	Payment methods, purchase history, transaction amounts, billing addresses, invoice details, PayPal email, PayPal ID, Stripe ID, IP address associated with transactions
Usage Information	IP addresses, device information (type, operating system, browser), access logs, feature usage, performance metrics, web page interactions, referring webpage/source, statistics associated with device/browser interaction with Services
Communications	Support tickets, messages between users, feedback and reviews, email correspondence, chat transcripts, inquiry details
Location Data	IP-address-based location information, mobile device location (if using a location-enabled browser or mobile app)
Content Data	Photos, videos, audio recordings, text, and other content you upload, create, generate, offer, or distribute through the Platform, including Creator Content and AI-Generated Content
Marketing Data	Your marketing preferences, responses to surveys, and information related to your interaction with our marketing communications
Recruitment Data	Name, contact details, resume, right-to-work documentation, references, test results, qualifications, accreditations (for job applicants)

2.2 Categories of Sources of Personal Data

We collect Personal Data about you from the following categories of sources:

- **Directly from You:** When you provide information directly to us, such as when you create an account, use our interactive tools and Services, voluntarily provide information in free-form text boxes or survey responses, send us an email, or otherwise contact us.
- **Automatically from Your Use of Services:** Through Cookies (as defined in Section 8), when you download our mobile application, use a location-enabled browser, or use our Services, and information is collected automatically from your computing device.
- **Public Records:** From government or other publicly available sources, particularly for verification purposes.
- **Third Parties:**
    - **Vendors:** Analytics providers (to analyze how you interact with Services), and vendors who help us generate leads or create user profiles.
    - **Advertising Partners:** Information related to how you interact with our websites, applications, products, Services, advertisements, or communications.
    - **Social Networks:** If you provide social network account credentials or sign in through a third-party site (e.g., Google, Facebook, X, Twitch), some content and/or information from those accounts may be transmitted to your VRAL.IO account.
    - **Payment Processors:** Our payment processing partners (Stripe, Approvely) collect payment card information necessary to process your payments.
    - **Business Partners:** Businesses with whom you have a relationship or companies we partner with for joint promotional offers.

3. How We Use Your Personal Data (Lawful Basis)

We use your Personal Data for various commercial or business purposes, based on the following lawful bases:

- **Performance of a Contract:** To fulfill our contractual obligations to you, such as creating and managing your account, processing orders and transactions, providing the products, services, or information you request, providing support and assistance for the Services, and managing payments, fees, and charges.
- **Legal Obligation:** To comply with our legal obligations under applicable law, regulation, court order, or other legal process. This includes preventing, detecting, and investigating security incidents and potentially illegal or prohibited activities, responding to regulatory reporting requirements (e.g., platform tax reporting rules), and fulfilling AML/KYC obligations.
- **Legitimate Interests:** Where it is necessary for our legitimate interests or those of a third party, and your interests and fundamental rights do not override those interests. Our legitimate interests include:
    - **Providing, Customizing, and Improving the Services:** Improving the Services (including testing, research, internal analytics, and product development), personalizing content and communications, doing fraud protection, security, and debugging.
    - **Operating Our Business:** Administering and protecting our business and website (including troubleshooting, data analysis, testing, system maintenance, support, reporting, and hosting of data), ensuring network security, and preventing fraud.
    - **Marketing and Business Growth:** Marketing and selling the Services, showing you advertisements (including interest-based ads), studying how customers use our products/services, developing them, and informing our marketing strategy.
    - **Corresponding with You:** Responding to correspondence, contacting you when necessary, and sending you information about VRAL.IO or the Services.
    - **Protecting Rights and Safety:** Protecting the rights, property, or safety of you, VRAL.IO, or another party, and enforcing any agreements with you.
    - **Business Transfers:** In connection with a merger, acquisition, bankruptcy, or other transaction where a third party assumes control of our business.
- **Consent:** We do not generally rely on consent as a legal basis for processing your Personal Data, except where required by law (e.g., for certain marketing activities or non-essential cookies). Where we do rely on consent, you have the right to withdraw it at any time.[4]

We will not collect additional categories of Personal Data or use the Personal Data we collected for materially different, unrelated, or incompatible purposes without providing you notice.

4. How We Share Your Personal Data

We disclose your Personal Data to the categories of service providers and other parties listed in this section. Depending on state laws that may be applicable to you, some of these disclosures may constitute a "sale" or "sharing" of your Personal Data. For more information, please refer to the state-specific sections below.

- **Service Providers:** These parties help us provide the Services or perform business functions on our behalf. They include:
    - Hosting, technology, and communication providers (e.g., AWS, Google Cloud Platform, Microsoft Azure, Cloudflare).
    - Security and fraud prevention consultants (e.g., Auth0, reCAPTCHA, MaxMind).
    - Support and customer service vendors.
    - Product fulfillment and delivery providers.
    - Analytics providers.
    - AI and Machine Learning services (e.g., OpenAI API, Stable Diffusion, Google Cloud AI) for content generation and moderation.
    - We undertake due diligence on our third-party service providers and enter into appropriate data processing agreements (or similar contractual safeguards) to ensure they comply with applicable data protection laws when handling personal data shared by VRAL.IO.
- **Payment Processors:** Our payment processing partners collect your voluntarily-provided payment card information necessary to process your payment. We are not a payment processor; payments are facilitated directly between users via third-party payment providers. Please see their respective terms of service and privacy policies for information on their use and storage of your Personal Data.
- **Advertising Partners:** These parties help us market our services and provide you with other offers that may be of interest to you. They include ad networks, data brokers, and marketing providers.
- **Business Partners:** These parties partner with us in offering various services, including businesses you have a relationship with or companies we partner with for joint promotional offers.
- **Parties You Authorize, Access, or Authenticate:** Third parties you access through the Services, social media services, or other users.

- **Creators (when you are a Customer/Supporter):** When you purchase products or services from a Creator on VRAL.IO, your personal information (such as your name, email address, and transaction details) may be shared with that Creator so they can fulfill your request or respond to your support. This may include your name or username, email address, physical address (where requested by a Creator to deliver a product or calculate applicable taxes), and any transaction information required to facilitate direct communication, fulfillment, or tax calculation. By purchasing from a Creator, you are directing us to share your information in this way.
    - **Creators as Independent Data Controllers:** Creators are independent data controllers for their customer's personal information (e.g., transaction-specific data, communications with customers, customer preferences, and marketing data). VRAL.IO is not responsible for how Creators handle data outside the VRAL.IO service. We strongly advise you to review the Creator's own privacy policy or terms if you are unsure how your data will be used.
- **Legal Obligations:** We may share any Personal Data that we collect with third parties in conjunction with any activities set forth under "Meeting Legal Requirements and Enforcing Legal Terms" in Section , such as responding to court orders, subpoenas, or law enforcement requests, or for fraud protection or tax reporting purposes.
- **Professional Advisors:** We may disclose Personal Data to our professional advisors, such as lawyers, auditors, and insurers, if necessary as part of the professional services they provide us with.
- **Business Transfers:** All of your Personal Data that we collect may be transferred to a third party if we undergo a merger, acquisition, bankruptcy, or other transaction in which that third party assumes control of our business (in whole or in part). Should one of these events occur, we will make reasonable efforts to notify you before your information becomes subject to different privacy and security policies and practices.
- **Aggregated, De-identified, or Anonymized Data:** We may create aggregated, de-identified, or anonymized data from the Personal Data we collect, including by removing information that makes the data personally identifiable to a particular user. We may use such data and share it with third parties for our lawful business purposes, including to analyze, build, and improve the Services and promote our business, provided that we will not share such data in a manner that could identify you.

5. Data Security and Retention

5.1 Data Security Measures

We are committed to protecting your Personal Data from unauthorized access, use, and disclosure. We implement a comprehensive set of physical, technical, organizational, and administrative security measures based on the type of Personal Data and how we are processing that data.

- **Technical Safeguards:** Multi-factor authentication, regular security audits, penetration testing, vulnerability scanning, intrusion detection systems, DDoS protection, and encryption of personal data.[1]
- **Organizational Measures:** Limited access controls, employee training, confidentiality agreements, vendor assessments, incident response plans, business continuity planning, regular policy reviews, and security awareness programs.
- **Physical Security:** Secured data centers, 24/7 monitoring, biometric access controls, environmental controls, redundant systems, backup procedures, and disaster recovery.

While we work to protect the security of your account and other data that we hold in our records, please be aware that no method of transmitting data over the internet or storing data is completely secure. You should also help protect your data by appropriately selecting and protecting your password and/or other sign-on mechanism, limiting access to your computer or device and browser, and signing off after you have finished accessing your account.

5.2 Data Breach Procedures

In the event of a data breach, we will follow a clear response plan :

- **Immediate Actions (0-24 hours):** Contain the breach, assess the scope, secure systems, preserve evidence, and initiate investigation.
- **Notification (24-72 hours):** Inform affected users without undue delay, provide breach details, explain potential impact, and offer protection measures, as required by applicable laws like GDPR.[1]
- **Follow-up Actions:** Complete investigation, implement improvements, provide updates, offer support services, and document lessons learned.

5. Data Retention

We retain Personal Data about you for as long as you have an open account with us or as otherwise necessary to provide you with our Services. In some cases, we retain Personal Data for longer if doing so is necessary to comply with our legal obligations, resolve disputes, collect fees owed, or is otherwise permitted or required by applicable law, rule, or regulation.

- **Active Account Data:** Duration of account + 30 days.
- **Transaction Records:** 7 years.
- **Security Logs:** 1 year. Please note that certain system-generated logs, essential for security and fraud prevention, may be retained even after account deletion, as restricting or rectifying data in such logs is not supported and would compromise historical records and increase fraud and security risks.[2]
- **Marketing Data:** Until consent is withdrawn + 1 year.
- **Communications:** years.
- **Deleted Content:** 90 days in backups.

We may further retain information in an anonymous or aggregated form where that information would not identify you personally, and we may use this anonymized information indefinitely without notifying you to improve our services.

6. Your Privacy Rights

You have certain rights regarding your Personal Data, which you may exercise by contacting us at privacy@VRAL.IO.com. We will respond to legitimate requests within

0 days. We may request identity verification to ensure your right to access your personal information or to exercise any of your other rights.

Your rights include:

- **Right to Access:** You have the right to request a copy of your Personal Data, know how we use your data, know who we share data with, and receive it in a portable format.[2]
- **Right to Rectification:** You have the right to update inaccurate information, complete incomplete data, or annotate disputed information.[2]
- **Right to Erasure/Deletion ("Right to be Forgotten"):** You can ask us to delete or remove your Personal Data from our systems where there is no good reason for us to continue processing it.[2] Exceptions apply for legal requirements, retention for legitimate interests (e.g., financial records, security logs), or where data is necessary for legal obligations, security, or fraud prevention.[2]
- **Right to Object to Processing:** You have the right to object to the processing of your Personal Data at any time for direct marketing purposes. You can also object in certain other circumstances to our continued processing of your Personal Data.
- **Right to Restriction of Processing:** You have the right, under certain circumstances, to restrict the processing of your data.
- **Right to Data Portability:** You have the right under certain circumstances to be provided with a copy of the Personal Data we have on you in a structured, machine-readable, and commonly used format (e.g., CSV, JSON) and for us to transfer it to a third party.[2]
- **Right to Withdraw Consent:** You have the right to withdraw consent to our processing of your Personal Data where we have collected and processed it with your consent.

California Resident Rights: If you are a California resident, you have specific rights under the CCPA, including the right to know about the personal information a business collects about you and how it is used and shared, the right to delete personal information collected from you (with some exceptions), and the right to opt-out of the sale or sharing of your personal information, including via the Global Privacy Control (GPC).[2] Please note that we do not currently sell your Personal Data as "sale" is defined under CCPA.

Nevada Resident Rights: If you are a resident of Nevada, you have the right to opt-out of the sale of certain Personal Data to third parties who intend to license or sell that Personal Data. You can exercise this right by contacting us at privacy@VRAL.IO.com with the subject line "Nevada Do Not Sell Request" and

providing us with your name and the email address associated with your account.

7. Children's Privacy

The VRAL.IO Platform is restricted to individuals aged 18 and older. We do not knowingly collect or solicit Personal Data about children under 18 years of age. If you are a child under the age of 18, please do not attempt to register for or otherwise use the Services or send us any Personal Data.

If we learn we have collected Personal Data from a child under 18 years of age, we will delete that information as quickly as possible. If you believe that a child under 18 years of age may have provided Personal Data to us, please contact us at privacy@VRAL.IO.com. We may implement proactive age verification measures, such as requiring date of birth input at registration or identity verification for access to specific features, to robustly prevent underage use and ensure compliance with child privacy laws.

8. Cookies and Tracking Technologies

The Services use cookies and similar technologies such as pixel tags, web beacons, clear GIFs, and JavaScript (collectively, "Cookies") to enable our servers to recognize your web browser, tell us how and when you visit and use our Services, analyze trends, learn about our user base, and operate and improve our Services. Cookies are small pieces of data—usually text files—placed on your computer, tablet, phone, or similar device when you use that device to access our Services.

We use the following types of Cookies :

- **Essential Cookies:** Required for providing you with features or services that you have requested. Disabling these Cookies may make certain features and services unavailable.
- **Functional Cookies:** Used to record your choices and settings regarding our Services, maintain your preferences over time, and recognize you when you return to our Services.

- **Performance/Analytical Cookies:** Allow us to understand how visitors use our Services by collecting information about the number of visitors, pages viewed, and viewing duration. These also help measure advertising campaign performance.
- **Marketing/Advertising Cookies:** Collect data about your online activity and identify your interests so that we can provide advertising that we believe is relevant to you.

Cookie Controls: You can decide whether or not to accept Cookies through your internet browser's settings. Most browsers have an option for turning off the Cookie feature. You can also delete all cookies that are already on your device. If you do this, however, you may have to manually adjust some preferences every time you visit our website, and some of the Services and functionalities may not work.

To comply with GDPR and CCPA, VRAL.IO provides granular cookie controls (e.g., via a cookie banner or a dedicated preference center) allowing users to accept or reject categories like analytics or marketing cookies. Non-essential cookies are blocked until consent is given.[6]

9. International Data Transfers

Where Personal Data is shared and disclosed as set out in this Privacy Policy, these parties may be established outside the European Economic Area ("EEA") and the United Kingdom (UK). Whenever we transfer your Personal Data outside the EEA and the United Kingdom, we ensure that a similar degree of protection is afforded to it by ensuring appropriate safeguards are implemented. This may include, where appropriate, signing up to safeguard mechanisms such as Standard Contractual Clauses endorsed by the UK Government or European Commission.

10. Changes to This Privacy Policy

We are constantly trying to improve our Services, so we may need to change this Privacy Policy from time to time. We will alert you to any such changes by placing a

notice on the VRAL.IO website, by sending you an email, and/or by some other means. Please note that if you've opted not to receive legal notice emails from us (or you haven't provided us with your email address), those legal notices will still govern your use of the Services, and you are still responsible for reading and understanding them. If you use the Services after any changes to the Privacy Policy have been posted, that means you agree to all of the changes. Use of information we collect is subject to the Privacy Policy in effect at the time such information is collected.

11. Contact Information

If you have any questions or comments about this Privacy Policy, the ways in which we collect and use your Personal Data, or your choices and rights regarding such collection and use, please do not hesitate to contact us at:

Email: privacy@VRAL.IO.com

For general inquiries: hello@VRAL.IO.com

For legal matters: legal@VRAL.IO.com