

FRAGMENT PRIVACY POLICY

Effective Date: March 31, 2023.

1. **Introduction and Overview.**

This Privacy Policy provides a comprehensive description of how Fragment Studios, Inc. (“**Fragment**” “**we,**” “**our,**” or “**us**”) collects, uses, and discloses information about you as well as your rights and choices regarding such information. It applies to any online location controlled by us that links to this Privacy Policy (the “**Service**”). Capitalized terms not defined in this Privacy Policy have the meaning given those terms in the Terms of Service.

By using the Service, you agree to our [Terms of Service](#) and to our collection, use, and disclosure practices, and other activities as described in this Privacy Policy. If you do not agree, discontinue use of the Service.

If you have any questions or wish to exercise your rights and choices, please contact us as set out in the “Contact Us” section.

You may have additional rights based on your jurisdiction. Please click the relevant link below for more information:

- [California](#)
- [Nevada](#)
- [Colorado, Connecticut, and Virginia](#)

2. **Information Collection.**

A. **Information You Provide.**

We collect information about you when you use the Service, including information you provide when you access our content. The categories of information we collect include:

- **Transaction Data** relating to the minting, purchase, sale, and transfer of non-fungible tokens (“**NFTs**”), including information regarding your digital or cryptocurrency wallet and the purchase price, date, and location of the transactions.
- **Contact Identifiers**, including your email address.

You may choose to voluntarily provide other information to us that we do not request, and, in such instances, you are solely responsible for such information.

B. **Information Collected Automatically.**

In addition, we automatically collect information when you use the Service. The categories of information we automatically collect include:

- **Device Identifiers**, including your device’s IP address.
- **Device Information**, including your device’s operating software and browser (e.g., type, version, and configuration), internet service provider, and regional and language settings.
- **Internet activity**, including information about your browsing history and interactions, such as the features you use, pages you visit, content you view, time of day you browse, and referring and exiting pages.
- **Non-precise location data**, such as location derived from an IP address or data that indicates a city or postal code level.

The types of tracking technologies we use to automatically collect this information include:

- **Cookies**, which are small data files stored on your browser that save data about your visit. Cookies often include a unique identifier (e.g., cookie #123). We use two types of cookies: session cookies and persistent cookies. Session cookies make it easier for you to navigate our website and expire when you close your browser. Persistent cookies help with personalizing your experience, remembering your preferences, and supporting security features. Persistent cookies may remain on your device for extended periods of time, and expire on a set expiration date or when they are deleted manually.
- **Pixels** (also known as web beacons), which is code embedded in a service that sends information about your use to a server. There are various types of pixels, including image pixels (which are small graphic images) and JavaScript pixels (which contains JavaScript code). When you access a service that contains a pixel, the pixel may permit us or a separate entity to drop or read cookies on your browser, or collect other information about your visit.
- **Device Fingerprinting**, which is the process of analyzing and combining sets of data elements from your device’s browser, such as JavaScript objects and installed fonts, to create a “fingerprint” of your device and uniquely identify your browser and device.

For further information on how we use tracking technologies for analytics, and your rights and choices regarding them, see the “Analytics” and “Your Rights and Choices” sections below.

C. Information from Other Sources.

We also collect information from other sources. The categories of sources from which we collect information include:

- **Social media platforms** with which you interact, including our Twitter profile and Discord server.
- **Publicly-available sources**, including data in the public domain.
- Through the AppliedPrimate intranet, from time to time we will request **User provided information**, including but not limited to email address, discord, telephone number, name and other information in order to participate in activations, games and events.

D. Information on the Blockchain

As part of the Service, we process certain personal data in a blockchain data record. This means that such personal data is stored in an immutable blockchain as part of a database called a distributed ledger. Anything stored in a ledger as part of the blockchain may not be changed or deleted. We use pseudonymization to reduce the risk to individuals whose personal data is processed in the blockchain. Please carefully review how the use of blockchain with our Service may limit the exercise of certain of your rights regarding personal data in the “California” section below.

3. Use of Information.

We collect and use information in accordance with the practices described in this Privacy Policy. Our purposes for collecting and using information include:

- Providing the Service to you.
- Preventing and addressing fraud, breach of policies or terms, or threats or harm.
- Understanding trends, usage, and activities, including through tracking technologies or surveys, to make business and marketing decisions.
- Communicating with you about updates, security alerts, changes to policies, and other transactional messages.
- Personalizing your experience to show you content we believe you will find interesting.
- Engaging in direct marketing, promotional communications, and non-personalized advertising.
- Fulfilling any purpose at your direction.

- With notice to you and your consent.

Notwithstanding the above, we may use publicly available information (as that term is defined by applicable law) or information that does not identify you (including information that has been aggregated or de-identified as those terms are defined by applicable law) for any purpose to the extent permitted by applicable law. For information on your rights and choices regarding how we use information about you, please see the “Your Rights and Choices” section below.

4. Disclosure of Information.

We disclose the information we collect in accordance with the practices described in this Privacy Policy. The categories of persons to whom we disclose information include:

- **Service Providers and Contractors.** We disclose information to service providers and contractors that process information on our behalf. Service providers and contractors assist us with services such as payment processing, data analytics, marketing and advertising, website hosting, and technical support. To the extent required by law, we contractually prohibit our service providers and contractors from retaining, using, or disclosing information about you for any purpose other than performing the services for us, although we may permit them to use publicly available information (as that term is defined by applicable law) or information that does not identify you (including information that has been aggregated or de-identified as those terms are defined by applicable law) to the extent permitted by applicable law.
- **Analytics.** We disclose information for analytics related purposes. The receiving persons may act as our service providers, or in certain contexts, independently decide how to process your information. For more information on analytics, see the “Analytics” section below.
- **Affiliates.** We disclose information to our affiliates and related entities, including where they act as our service providers or for their own internal purposes.
- **Partners.** We disclose information to our partners in connection with offering co-branded services, selling or distributing our products, or engaging in joint marketing activities.
- **Public Forums.** We disclose information you make public through the Service, such as information that you post on Twitter or in our Discord server. Please think carefully before making information public as you are solely responsible for any information you make public. Once you have posted information, you may not be able to edit or delete such information, subject to additional rights set out in the “Your Rights and Choices” section below.

- **Merger or Acquisition.** We disclose information in connection with, or during negotiations of, any proposed or actual merger, purchase, sale or any other type of acquisition or business combination of all or any portion of our assets, or transfer of all or a portion of our business to another business.
- **Security and Compelled Disclosure.** We disclose information to comply with the law or other legal process, and where required, in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. We also disclose information to protect the rights, property, life, health, security and safety of us, the Service or anyone else.
- **Facilitating Requests.** We disclose information where you direct us to disclose the information.
- **Consent.** We disclose information with notice to you and your consent.

Notwithstanding the above, we may disclose publicly available information (as that term is defined by applicable law) or information that does not identify you (including information that has been aggregated or de-identified as those terms are defined by applicable law) to the extent permitted by applicable law. For information on your rights and choices regarding how we disclose information about you, please see the “Your Rights and Choices” section below.

5. **Other Parties.**

We offer parts of our Service through websites, platforms, and services operated or controlled by other parties. In addition, we integrate technologies operated or controlled by other parties into parts of our Service.

Some examples include:

- **Links.** Our Service includes links that hyperlink to websites, platforms, and other services not operated or controlled by us.
- **Brand Pages and Messaging.** We may offer our content through social media. Any information you provide to us when you engage with our content (such as through our brand pages or our Discord server) is treated in accordance with this Privacy Policy. Also, if you publicly reference our Service on social media (e.g., by using a hashtag associated with Fragment in a tweet or post), we may use your reference on or in connection with our Service.

Please note that when you interact with other parties, including when you leave our Service, those parties may independently collect information about you and solicit information from you. The information collected and stored by those parties remains subject to their own policies and

practices, including what information they share with us, your rights and choices on their services and devices, and whether they store information in the U.S. or elsewhere. We encourage you to familiarize yourself with and consult their privacy policies and terms of use.

6. **Analytics.**

We use analytics services, such as Google Analytics, to help us understand how users access and use the Service.

As indicated above, vendors and other parties may act as our service providers, or in certain contexts, independently decide how to process your information. We encourage you to familiarize yourself with and consult their privacy policies and terms of use.

For further information on the types of tracking technologies we use on the Service and your rights and choices regarding analytics, please see the “Information Collected Automatically” and “Your Rights and Choices” sections.

7. **Your Rights and Choices.**

In addition to the rights and choices below, you may have additional rights based on your jurisdiction. Please click the relevant link at the top of this Privacy Policy or visit the applicable section below for more information.

A. Tracking Technology Management.

- **Cookies.** Most browsers accept cookies by default. You can instruct your browser, by changing its settings, to decline or delete cookies. If you use multiple browsers on your device, you will need to instruct each browser separately. Your ability to limit cookies is subject to your browser settings and limitations.
- **Do Not Track.** Your browser settings may allow you to automatically transmit a “Do Not Track” signal to online services you visit. Note, however, there is no industry consensus as to what site and app operators should do with regard to these signals. Accordingly, unless and until the law is interpreted to require us to do so, we do not monitor or take action with respect to “Do Not Track” signals. For more information on “Do Not Track,” visit <http://www.allaboutdnt.com>.

Please be aware that if you disable or remove tracking technologies some parts of the Service may not function correctly.

B. Analytics Management.

Google provides tools to allow you to opt out of the use of certain information collected by Google Analytics at <https://tools.google.com/dlpage/gaoptout>.

Please note that the above opt out only applies to the specific browser from which you opt out. We are not responsible for the effectiveness of any opt outs offered by other entities.

C. Communications.

- **E-mails.** You can unsubscribe from receiving promotional emails by following the unsubscribe instructions at the bottom of the email, or emailing us at hi@fragment.xyz with the word UNSUBSCRIBE in the subject field of the email. Please note that you cannot opt out of transactional messages.

Please note that your opt out is limited to the email address used and will not affect subsequent subscriptions.

8. Children.

The Service is not directed toward children under 13 years old, and we do not knowingly collect personal information (as that term is defined by the U.S. Children’s Privacy Protection Act, or “COPPA”) from children. If you are a parent or guardian and believe we have collected personal information from children, please contact us at hi@fragment.xyz. We will delete the personal information in accordance with COPPA.

9. Data Security.

We implement and maintain reasonable administrative, physical, and technical security safeguards to help protect information about you from loss, theft, misuse, and unauthorized access, disclosure, alteration, and destruction. Nevertheless, transmission via the internet is not completely secure and we cannot guarantee the security of information about you.

10. International Transfer.

We are based in the U.S. and the information we collect is governed by U.S. law. If you are accessing the Service from outside of the U.S., please be aware that information collected through the Service may be transferred to, processed, stored, and used in the U.S. and other jurisdictions. Data protection laws in the U.S. and other jurisdictions may be different from those of your country of residence. Your use of the Service or provision of any information therefore constitutes your consent to the transfer to and from, processing, usage, disclosure, and storage of information about you in the U.S. and other jurisdictions as set out in this Privacy Policy.

11. Changes to this Privacy Policy.

We reserve the right to revise and reissue this Privacy Policy at any time. Any changes will be effective immediately upon posting of the revised Privacy Policy. Your continued use of our Service indicates your consent to the Privacy Policy then posted. If the changes are material, we may provide you additional notice to your email address.

12. Contact Us.

If you have any questions about our data practices, or experience any difficulty accessing the information in this Privacy Policy, please contact us:

By email:

legal@fragment.xyz

By mail:

Fragment Studios
PO BOX 253
250 Merrick Road
Rockville Centre, NY 11570
United States

13. California.

The California Consumer Privacy Act (“CCPA”), and its replacement the California Privacy Rights Act (“CPRA”), provide additional rights to California residents. This section addresses those rights and applies only to California residents.

A. Notice of Collection.

At or before the time of collection of your personal information, you have a right to receive notice of our data practices. Our data practices are as follows:

- For the categories of personal information we have collected in the past 12 month, see the [Information Collection](#) section above.
- For the categories of sources from which personal information is collected, see the [Information Collection](#) section above.
- For the specific business and commercial purposes for collecting and using personal information, see the [Use of Information](#) section above.
- For the categories of third parties to whom information is disclosed, see the [Disclosure of Information](#) section above.
- For the criteria used to determine the period of time information will be retained, see the [Retention](#) section above.

We do not “sell” or “share” your personal information as those terms as defined by the CPRA.

We do not knowingly sell or share the personal information of minors under 16 years old who are California residents.

B. Retention.

We retain each category of personal information, for the length of time that is reasonably necessary for the purpose for which it was collected, and as necessary to comply with our legal obligations, resolve disputes, prevent fraud, and enforce our agreements.

C. Right to Know, Correct, and Delete.

You have the right to know certain details about our data practices. In particular, you may request the following from us:

- The categories of personal information we have collected about you;
- The categories of sources from which the personal information was collected;
- The categories of personal information about you we disclosed for a business purpose or sold or shared;
- The categories of persons to whom the personal information was disclosed for a business purpose or sold or shared;
- The business or commercial purpose for collecting or selling or sharing the personal information; and
- The specific pieces of personal information we have collected about you.

In addition, you have the right to correct or delete the personal information we have collected from you.

Our Service may use blockchain technology to store certain personal data, including your digital wallet address, time of transactions, and other information that may be used to directly or indirectly identify you. In our Service, we may collect other data that enables us to identify you. We use pseudonymization in our blockchain records to reduce the risk to individuals whose personal data is processed in the blockchain. As a result, the way we respond to a request to exercise certain of your rights (i.e., access, correction, and deletion requests) will be limited. We cannot alter information stored in a blockchain, but, unless we have a legitimate interest or other valid legal basis in processing your personal data, if you request erasure, object to the processing of your personal data, or request that the processing of your personal data be limited by us, we will not include your personal data in our Service records that are added to the blockchain subsequent to such request. We may not be able to provide you the Service if you request that your personal data be deleted or you object to further processing of your personal data.

If you request that any such personal data be corrected when we validate the information as being correct, we will correct our records, including by creating a new record entry in the blockchain if appropriate. Additionally, although we cannot erase your personal data in Service records that have been added to the blockchain, we can, when appropriate (i.e., you no longer use the our Service), erase the mapping in our records and/or our service provider records pertaining to you, outside the blockchain in a manner that would render the pseudonymized data in the blockchain to be de-identified (anonymized).

To exercise any of these rights, please email us at legal@fragment.xyz. In the request, please specify which right you are seeking to exercise and the scope of the request. We will confirm receipt of your request within 10 days. We may require specific information from you to help us verify your identity and process your request. If we are unable to verify your identity, we may deny your request.

D. Authorized Agent.

You can designate an authorized agent to submit requests on your behalf. However, we will require written proof of the agent's permission to do so and verify your identity directly.

E. Right to Non-Discrimination.

You have the right not to receive discriminatory treatment by us for the exercise of any your rights.

F. Shine the Light.

Customers who are residents of California may request (i) a list of the categories of personal information (as that term is defined by Shine the Light) disclosed by us to third parties during the immediately preceding calendar year for those third parties' own direct marketing purposes; and (ii) a list of the categories of third parties to whom we disclosed such information. To exercise a request, please write us at the email or postal address set out in "Contact Us" above and specify that you are making a "California Shine the Light Request." We may require additional information from you to allow us to verify your identity and are only required to respond to requests once during any calendar year.

14. Nevada.

We do not sell and will not sell your covered information (as those terms are defined by NRS 603A.340).

15. Colorado, Connecticut, and Virginia.

These additional rights and disclosures apply only to residents of Colorado, Connecticut, and Virginia. Terms have the meaning ascribed to them in the Colorado Privacy Act (“CPA”), the Connecticut Data Privacy Act (“CTDPA”), and the Virginia Consumer Data Protection Act (“VCDPA”), as applicable.

In your region, you have the following rights under applicable law:

- To confirm whether or not we are processing your personal data
- To access your personal data
- To correct inaccuracies in your personal data
- To delete your personal data
- To obtain a copy of your personal data that you previously provided to us in a portable and readily usable format
- To opt out of the processing of personal data for purposes of profiling in furtherance of decisions that produce legal or similarly significant effects concerning you

To exercise any of these rights, please email us at legal@fragment.xyz and specify which right you are seeking to exercise. We will respond to your request within 45 days. If you have an account with us, we may require you to use the account to submit the request. We may require specific information from you to help us confirm your identity and process your request.

You can designate an authorized agent to submit requests on your behalf. Requests must be submitted through the designated methods listed above. Except for opt-out requests, we will require written proof of the agent’s permission to do so and may verify your identity directly.

If we refuse to take action on a request, you may appeal our decision within a reasonable period time by contacting us at legal@fragment.xyz and specifying you wish to appeal. Within 60 days of our receipt of your appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, you may submit a complaint as follows:

- For Colorado residents, to the Colorado AG at <https://coag.gov/file-complaint/>
- For Connecticut residents, to the Connecticut AG at <https://www.dir.ct.gov/ag/complaint/>
- For Virginia residents, to the AG at <https://www.oag.state.va.us/consumercomplaintform>