Privacy Policy

Last Modified: May 5, 2025

1. Introduction

Replicats is committed to protecting your privacy. This Privacy Policy applies to all personal information collected when you interact with our website, use the Replicats Platform, and engage with our AI Investment Agents.

This policy describes:

- What information we collect and why
- How we use and protect your information
- Your rights regarding your personal information
- How you can contact us about privacy matters

"Personal Data" means any information relating to an identified or identifiable individual. If you don't agree with this Privacy Policy, please do not use our services.

We may update this policy periodically. When we make significant changes, we'll notify you via email or through a notice on our website.

For questions about this Privacy Policy or to exercise your privacy rights, please contact us at support@replicats.ai.

2. Information Collection

Information You Provide

We collect your wallet address when you access the Replicats Platform. This is necessary to link your portfolio and authenticate your access to our services.

When you create an account or sign up for our services, we collect your email address for account management and communication purposes. If you connect through our third-party authentication provider they may also collect your name and email address according to their privacy policy.

We also collect your investment preferences, risk tolerance, and portfolio customization choices. This information is essential for your AI Investment Agents to operate according to your specifications.

Automatically Collected Information

When you visit our website or use our platform, we automatically collect technical information including:

- IP address
- Browser type and version
- Operating system
- Referring website
- Pages visited and features used
- Time spent on pages
- Device information

This information helps us understand how users interact with our platform, identify technical issues, and improve user experience. From time to time, we may engage third-party analytics services to help us analyze this usage data. These analytics providers are bound by their own privacy policies and are only authorized to use this information to provide analytics services to us.

3. Use of Information

We use the information we collect to:

Provide Our Services

Your wallet address and investment preferences allow us to authenticate you and customize your experience on the Replicats Platform. This information is essential for creating and managing your AI Investment Agents.

Power Your AI Investment Agents

Our proprietary AI framework—utilizing deep learning, reinforcement learning, Graph Neural Networks (GNNs), Vector Error Correction Models (VECM), and Support Vector Machines (SVMs)—processes your investment preferences and portfolio data to make investment decisions aligned with your goals. Your data trains and customizes these AI agents according to your specific requirements and risk tolerance.

Improve Our Platform

We analyze usage patterns and feedback to enhance our services, develop new features, and optimize the user experience. When we share statistical information about platform usage, we aggregate the data and do not identify individual users.

Security and Compliance

We use your information to verify accounts, prevent fraud, and ensure platform security. We may also use this information to comply with legal obligations.

4. Information Sharing

We may share your Personal Data with third-party service providers who help us deliver and improve our services. These service providers include:

- Cloud infrastructure providers who host our platform
- Analytics providers who help us understand platform usage
- AI technology partners who support our investment agent functionality
- Payment processors who handle subscription transactions
- Authentication and wallet connection services, such as dynamic.xyz
- Blockchain integration services, such as crossmint.com
- Other third-party integrations we may engage from time to time to enhance our platform functionality

These service providers are contractually obligated to use your Personal Data only for the purposes of providing services to us and are required to maintain appropriate security measures to protect your information.

We may also disclose your Personal Data if required by law, court order, or other legal process, or if we have a good faith belief that disclosure is necessary to protect our rights, investigate fraud, or protect the safety of our users or the public.

We do not sell, rent, or lease your Personal Data to third parties.

5. Data Security and Storage

Data Security

We implement appropriate technical and organizational measures to protect your Personal Data against unauthorized access, accidental loss, destruction, or damage. These measures include:

- Encryption of data in transit and at rest
- Access controls and authentication measures
- Regular security assessments and penetration testing
- Employee training on data protection practices
- Incident response procedures

Your data is stored on secure servers provided by Google Cloud Platform in the United States. Google Cloud Platform maintains industry-leading security certifications and compliance standards, providing additional layers of protection for your information.

While we work hard to protect your information, no method of transmission over the Internet or electronic storage is 100% secure. We cannot guarantee absolute security but continuously strive to enhance our security measures.

Data Retention

We retain your Personal Data only for as long as necessary to fulfill the purposes for which it was collected, including legal, accounting, or reporting requirements. When determining retention periods, we consider various factors including the nature of the data, our ongoing relationship with you, and applicable legal requirements.

When Personal Data is no longer necessary, we securely delete or anonymize it.

6. Cookie Policy

What Are Cookies

Cookies are small text files placed on your device when you visit our website. They help us recognize your device and remember certain information about your visit.

Types of Cookies We Use

We use the following types of cookies on our website:

- **Essential Cookies**: Required for the website to function properly. These enable basic functions like page navigation and access to secure areas of the website.
- **Analytical/Performance Cookies**: Help us understand how visitors interact with our website by collecting and reporting information anonymously. We use these to improve the way our website works.
- **Functionality Cookies**: Allow the website to remember choices you make and provide enhanced, personalized features.
- **Targeting Cookies**: Record your visit to our website, the pages you visit, and the links you follow. We use this information to make our website and advertising more relevant to your interests.

Managing Cookies

Most web browsers allow you to control cookies through their settings. You can usually find these settings in the "Options" or "Preferences" menu of your browser. You can delete existing cookies, allow or block all cookies, or block cookies from particular sites.

To learn more about cookies and how to manage them, visit www.allaboutcookies.org or your browser's help section.

7. User Rights

You have the following rights regarding your personal data:

Access and Portability

You can request a copy of the personal data we hold about you and information about how we process it.

Correction

You can ask us to correct inaccurate or incomplete information about you.

Deletion

You can request that we delete your personal data in certain circumstances, such as when the data is no longer necessary for the purposes for which it was collected.

Objection and Restriction

You can object to our processing of your data or ask us to restrict processing in certain situations.

Withdrawal of Consent

Where we process data based on your consent, you can withdraw that consent at any time.
To exercise these rights, please contact us at privacy@replicats.ai. We'll respond to your request within a reasonable timeframe. We may need to verify your identity before fulfilling your request.

8. International Considerations

When we transfer your personal data from one country to another, we implement appropriate safeguards to ensure your data remains protected according to this Privacy Policy.

We use our best efforts to comply with privacy regulations in our users' jurisdictions. However, as we continue to develop our platform, we may need to implement access restrictions in certain regions where we cannot yet ensure full compliance with local data protection requirements.

If you would like more information about the safeguards we have in place for international transfers, please contact us at support@replicats.ai.

9. Additional Information

Children's Privacy

Our services are not intended for or directed at children under 18 years of age. We do not knowingly collect personal information from children. If we become aware that we have collected personal data from a child without parental consent, we will take steps to delete that information.

No Selling of Personal Data

We do not sell your personal data to third parties under any circumstances.

Based on my research, implementing Standard Contractual Clauses (SCCs) would require your technical team to implement specific security measures and organizational practices. Here's what your team would need to do:

Technical Measures Required by SCCs

1. **Document and Implement Security Measures** Your team would need to document and implement appropriate technical measures to ensure data security. These measures must be specifically described in Annex II of the SCCs and should address protection against "accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to data." European Commission
2. **Assess Transfer Risks and Implement Supplementary Safeguards** If your assessment indicates risks in the destination country, your team may need to implement additional "supplementary safeguards" such as end-to-end encryption European Commission or other technical protections to ensure compliance.
3. **Data Security Controls** Your technical team would need to implement measures to "prevent unauthorized access, processing, or misuse of personal data" Centraleyes that's being transferred internationally. This includes:
    - Encryption for data in transit and at rest
    - Access controls and authentication systems
    - Pseudonymization where appropriate
    - Logging and monitoring systems
    - Regular security testing
4. **Data Subject Rights Implementation** Your systems must be capable of facilitating data subject rights, including access to personal data, ability to correct inaccuracies, and mechanisms to respond to requests. Kiteworks
5. **Data Breach Notification Systems** Your team would need to implement systems to detect and respond to "a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data." Oversight
6. **Data Deletion Capabilities** Your systems would need processes to ensure "data is erased and hard drives destroyed using NIST 800-88 or other secure methods" when required. Oversight
7. **Transfer Impact Assessment (TIA)** Your team would need to conduct and document a transfer impact assessment to evaluate whether additional safeguards are necessary based on the destination country's laws. Centraleyes