

PRIVACY POLICY

www.danuvia.pro

Effective date: 1st March 2023

Welcome to Danuvia Crypto Services Ltd (“Danuvia”, “we”, “us” and “our”). We are committed to protecting your privacy and personal information. This Privacy Policy explains how we collect, use, and share information about you when you use our crypto wallet app (“App”) and visit our website, www.danuvia.pro (“Site”).

Acceptance of Policy

By using Danuvia, including downloading one of our mobile applications or visiting our website (www.danuvia.pro), you agree to the use, disclosure, and procedures outlined in this Privacy Policy.

Personal Information Collection

We strive to minimize the amount of personal information we collect from Danuvia users. When you communicate with us for support, or if you report a bug or other error related to Danuvia, we may collect your contact information, such as your phone number or email address (depending on how you contact us). When you use our Services, we process public wallet addresses that you generate through Danuvia.

Categories of Personal Information

The categories of personal information we collect and the types of personal information captured by category are:

- Personal details, contact details, and identifiers.
- Name and contact details (such as e-mail, and phone numbers when you voluntarily have shared this information with us to be contacted)
- When you use our Services, we process PUBLIC wallet addresses that you generate through Danuvia.

Purpose of Collection of Personal Information/Data

- Providing services to users.
- Facilitating communication with you for customer support purposes.
- System and application access data and internet and electronic network activity information.
- The Internet protocol (IP) address used to connect your computer or mobile device to the Internet.
- Danuvia Services metrics (e.g., the occurrences of technical errors, your interactions with service features and content, and your setting preferences)

- Records of any contractual agreements between yourself and Danuvia
- Providing troubleshooting and improving Danuvia Services.
- Analyzing performance, fixing errors, and improving the usability and effectiveness of Danuvia Services.
- Necessary for the performance of a contract to which you are a party.
- Our legitimate interests and the interests of our users in, for example, detecting and preventing fraud and abuse in order to protect the security of our users, ourselves, or others. Our legitimate interests in keeping records and necessary for the performance of your contract.

HOW WE USE YOUR PERSONAL INFORMATION

We may use your personal information for the following purposes and as otherwise described in this Privacy Policy or at the time of collection:

Direct Marketing. We may use your personal information to send you Inadot-related marketing communications as permitted by law. You will have the ability to opt-out of our marketing and promotional communications as described in the Your Choices section below.

For research and development. We may use your personal information for research and development purposes, including to analyze and improve the Service and our business.

To create anonymous data. We may create aggregated, de-identified or other anonymous data records from your personal information and other individuals whose personal information we collect. We make personal information into anonymous data by excluding information (such as your name) that makes the data personally identifiable to you. We may use this anonymous data and share it with third parties for our lawful business purposes, including to analyze and improve the Service and promote our business.

To comply with laws and regulations. We use your personal information as we believe necessary or appropriate to comply with applicable laws, lawful requests, and legal process, such as to respond to subpoenas or requests from government authorities.

For compliance, fraud prevention and safety. We may use your personal information and disclose it to law enforcement, government authorities, and private parties as we believe necessary or appropriate to: (a) protect our, your or others' rights, privacy, safety or property (including by making and defending legal claims); (b) audit our internal processes for compliance with legal and contractual requirements; (c) enforce the terms and conditions that govern the Service; and (d) protect, investigate and deter against fraudulent, harmful, unauthorized, unethical or illegal activity, including cyber-attacks and identity theft.

With your consent. In some cases we may specifically ask for your consent to collect, use or share your personal information, such as when required by law.

HOW WE SHARE YOUR PERSONAL INFORMATION

We may share your personal information with the following third parties and as otherwise described in this Privacy Policy or at the time of collection:

Service providers. Companies and individuals that provide services on our behalf or help us operate the Service or our business (such as order fulfillment, shipping, payment processing, customer support, hosting, analytics, email delivery, marketing, database management services, returns processing and risk and fraud mitigation).

Third party platforms. Social media and other third party platforms that you connect to the Service, such as when you use options to access the Service by logging into a social media platform. Please note, we do not control the third party's use of your personal information.

The public. Other users of the Service and the public, when you disclose personal information for public use. We do not control how other users or third parties use any personal information that you make available to them. Please be aware that any information you post publicly can be cached, copied, screen captured or stored elsewhere by others (e.g., search engines) before you have a chance to edit or remove it.

Professional advisors. Professional advisors, such as lawyers, bankers, auditors and insurers, where necessary in the course of the professional services that they render to us.

Authorities and others. Law enforcement, government authorities, and private parties, as we believe in good faith to be necessary or appropriate to comply with law or for the compliance, fraud prevention and safety purposes described above.

COOKIES

Our crypto wallet app and website use cookies to enhance your user experience and to collect data about your usage of our services. Cookies are small text files that are stored on your device when you access our website or app.

We use both session cookies and persistent cookies on our website and app. Session cookies are temporary and are automatically deleted when you close your browser, while persistent cookies remain on your device until they expire or are manually deleted.

The cookies we use on our app and website are used for various purposes, including:

- **Authentication and security:** We use cookies to authenticate users and prevent fraudulent use of our services.
- **Analytics:** We use cookies to collect data about how our website and app are used, including which pages are visited and for how long, which features are used most frequently, and which errors occur.
- **Personalization:** We use cookies to remember your preferences and settings, such as language preferences and display settings.
- **Advertising:** We may use cookies to personalize advertisements displayed to you on our app and website based on your interests and browsing behavior.

By using our app or website, you consent to the use of cookies as described in this Privacy Policy. You can control the use of cookies through your browser settings and other tools, such as ad preferences, but please note that disabling cookies may limit your ability to use certain features of our app and website.

YOUR CHOICES

In this section, we describe the rights and choices available to all users.

Access or update your account information. If you have registered for an account with us, you may review and update certain personal information in your account profile by logging into the account.

Do Not Track. Some Internet browsers may be configured to send “Do Not Track” signals to the online services that you visit. We currently do not respond to “Do Not Track” or similar signals. To find out more about “Do Not Track,” please visit <http://www.allaboutdnt.com>

Privacy settings and location data. Users of our App can disable our access to their device’s precise geo-location in their mobile device settings.

Choosing not to share your personal information. If you do not provide information that we need to provide the Service, we may not be able to provide you with the Service or certain features. We will tell you what information you must provide to receive the Service when we request it.

Third-party platforms or social media networks. If you choose to create an account through or connect the Service with another third-party platform, you may have the ability to limit the information that we may obtain from the third-party at the time you log in to the Service using the third-party’s authentication service or otherwise connect your account. You may also be able to control your settings through the third-party’s platform or service after you have connected your accounts.

DELETING DATA AND INFORMATION

Users on the App and Site can delete their Account. Once an account is deleted, we will erase ALL data of the User associated with their account including messages, their connections, and their personal information. The process cant be undone once the user proceeds with the deletion of data.

OTHER SITES AND SERVICES

The Sites may contain links to other websites and online services operated by third parties. These links are not an endorsement of, or representation that we are affiliated with, any third party. In addition, our content may be included on web pages or online services that are not associated with us. We do not control third party websites or online services, and we are not responsible for their actions. Other websites and services follow different rules regarding the collection, use and sharing of your personal information. We encourage you to read the privacy policies of the other websites and online services you use.

SECURITY PRACTICES

The security of your personal information is important to us. We employ a number of organizational, technical and physical safeguards designed to protect the personal information we collect. However, security risk is inherent in all internet and information technologies and we cannot guarantee the security of your personal information.

INTERNATIONAL DATA TRANSFERS

Inadot is headquartered in the United Kingdom and may have service providers in other countries. Your personal information may be transferred to the U.K. or other locations outside of your state, province, country, or other governmental jurisdiction where privacy laws may not be as protective as those in your jurisdiction.

GENERAL DATA PROTECTION REGULATION (GDPR)

If you are from the European Economic Area (EEA), Inadot legal basis for collecting and using the personal information described in this Privacy Policy depends on the Personal Data we collect and the specific context in which we collect it.

Inadot may process your Personal Data because:

- We need to perform a contract with you
- You have given us permission to do so
- The processing is in our legitimate interests and it's not overridden by your rights
- For payment processing purposes
- To comply with the law

Retention of Data

Inadot will retain your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy. We will retain and use your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

Inadot will also retain 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 Service, or we are legally obligated to retain this data for longer time periods.

Transfer of Data

Your information, including Personal Data, may be transferred to — and maintained on — computers located outside of your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from your jurisdiction.

Your consent to this Privacy Policy followed by your submission of such information represents your agreement to that transfer.

Inadot will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of your data and other personal information.

Disclosure of Data

Legal Requirements

Inadot may disclose your Personal Data in the good faith belief that such action is necessary to:

- To comply with a legal obligation

- To protect and defend the rights or property of Inadot
- To prevent or investigate possible wrongdoing in connection with the Service
- To protect the personal safety of users of the Service or the public
- To protect against legal liability

Security of Data

The security of your data is important to us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Data, we cannot guarantee its absolute security.

Your rights under the GDPR

If you are a resident of the European Economic Area (EEA), you have certain data protection rights. Inadot aims to take reasonable steps to allow you to correct, amend, delete, or limit the use of your Personal Data.

If you wish to be informed what Personal Data we hold about you and if you want it to be removed from our systems, please contact us.

In certain circumstances, you have the following data protection rights:

- **The right to access, update or to delete the information we have on you.** Whenever made possible, you can access, update or request deletion of your Personal Data directly within your account settings section. If you are unable to perform these actions yourself, please contact us to assist you.
- **The right of rectification.** You have the right to have your information rectified if that information is inaccurate or incomplete.
- **The right to object.** You have the right to object to our processing of your Personal Data.
- **The right of restriction.** You have the right to request that we restrict the processing of your personal information.
- **The right to data portability.** You have the right to be provided with a copy of the information we have on you in a structured, machine-readable and commonly used format.
- **The right to withdraw consent.** You also have the right to withdraw your consent at any time where Inadot relied on your consent to process your personal information.

Please note that we may ask you to verify your identity before responding to such requests.

You have the right to complain to a Data Protection Authority about our collection and use of your Personal Data. For more information, please contact your local data protection authority in the European Economic Area (EEA).

Service Providers

We may employ third party companies and individuals to facilitate our Service (“Service Providers”), to provide the Service on our behalf, to perform Service-related services or to assist us in analyzing how our Service is used.

These third parties have access to your Personal Data only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose.

ANALYTICS

We may use third-party Service Providers to monitor and analyze the use of our Service.

- **Google Analytics**

Google Analytics is a web analytics service offered by Google that tracks and reports website traffic. Google uses the data collected to track and monitor the use of our Service. This data is shared with other Google services. Google may use the collected data to contextualize and personalize the ads of its own advertising network.

For more information on the privacy practices of Google, please visit the Google Privacy & Terms web page: <http://www.google.com/intl/en/policies/privacy/>

PAYMENTS

We may provide in-app purchase and/or paid services within the Service. In that case, we use third-party services for payment processing (e.g. payment processors).

We will not store or collect your payment card details. That information is provided directly to our third-party payment processors whose use of your personal information is governed by their Privacy Policy. These payment processors adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, Mastercard, American Express and Discover. PCI-DSS requirements help ensure the secure handling of payment information.

The payment processors we work with are:

- **Apple Store In-App Payments**

Their Privacy Policy can be viewed at <https://www.apple.com/legal/privacy/en-ww/>

- **Google Play In-App Payments**

Their Privacy Policy can be viewed at <https://www.google.com/policies/privacy/>

CHILDREN’S PRIVACY

Our Service does not address anyone under the age of 13 (“Children”).

We do not knowingly collect personally identifiable information from anyone under the age of 13. If you are a parent or guardian and you are aware that your Child has provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from children without verification of parental consent, we take steps to remove that information from our servers.

GOOGLE PLAY USER DATA COMPLIANCE

We understand and comply with Google Play User Data Policy which requires us to be transparent in handling user data including information collected from or about a user, including device information. This means we disclose the access, collection, use, handling, and sharing of user data from our crypto wallet app, and limit the use of the data to policy compliant purposes disclosed.

Furthermore, we understand that these Google Play requirements are in addition to any requirements prescribed by applicable privacy and data protection laws.

In addition, if our crypto wallet app includes third party code such as an SDK, we ensure that the third-party code used in our app and that third party's practices with respect to user data from our app, are compliant with Google Play Developer Program policies, which include use and disclosure requirements. For instance, we ensure that our SDK providers do not sell personal and sensitive user data from our app.

This requirement applies regardless of whether user data is transferred after being sent to a server, or by embedding third-party code in our app. We are committed to ensuring the safety and security of user data and we take all necessary measures to comply with Google Play User Data Policy.

CHANGES TO THIS PRIVACY POLICY

We may update our Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on this page.

We will let you know via email and/or a prominent notice on our Service, prior to the change becoming effective and update the "effective date" at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

CONTACT US

If you have any questions about this Privacy Policy, please contact us:

support@danuvia.pro