

# TokenSoft

## Privacy Policy

Last Modified: October 4, 2019

This Privacy Policy (the “Policy”) explains how TokenSoft, Inc. (“TokenSoft,” “we,” “us” or “our”) handles and protects your personal information when you access or use our websites ([www.tokensoft.io](http://www.tokensoft.io)), content, features, pages, or our applications such as Knox Wallet owned or operated by us (collectively, the “Services”). This Policy only applies to users and customers that access or visit the Services owned or operated by TokenSoft. We may refer to users and customers collectively as “you” within this Policy.

This policy does not apply to customers of TokenSoft using its white-label platform. TokenSoft is a service provider and does not control how customers use information obtained via our products.

If you are an individual wishing to obtain information about the data handling practices of one of our customers, please contact the customer directly. We will forward any inquiries relevant to our customers’ data handling practices directly to the customer.

### 1. CHANGES TO THE POLICY

We may modify or update this Policy from time to time by posting a revised version and updating the “Last Modified” date above. We may provide you with additional forms of notice as appropriate under the circumstances, such as email notices to the most recent email address we have on file for you. Your continued use of our Services after any modification to this Privacy Policy will constitute your acceptance of such modification.

In addition, we may provide you with “just-in-time” disclosures or additional information about the data handling practices of specific parts of our Services. Such notices may supplement this Policy or provide you with additional choices about how we process your personal information.

### 2. INFORMATION WE COLLECT

Personal information is any information that identifies you or makes you identifiable. Any information that is anonymized or aggregated is no longer personal information. We need to collect your personal information in order to provide you with our Services or support.

We may collect the following types of information:

- i. Information You Provide to Us. We collect any information that you voluntarily provide to us, such as your inquiries through our website, information you provide about your business, suggestions for improvements, referrals, or any other actions performed by you on our Services.
- ii. Transaction Information. When you purchase our Services, we will collect

information about your payment method, and any other relevant transaction data.

iii. Knox Wallet, When you use Knox Wallet, we will collect information relating to your addresses and accounts, transactions (e.g. amount, sender, receiver, and transaction descriptions), and any users or signers you provide us when using Knox Wallet and related services.

iv. Sign-up and Referral Information. In some cases, we may request information necessary to to sign up for a Service or be referred you to one our partners for a service. In these cases, we may collect your contact information, personal information, information relating to your business, its beneficial owners, its authorized signers, or other information requested by our partner or otherwise necessary to provide such Service or referral.

v. Job Application Information. We collect any information you provide to us when you apply for a job with us. For example, we collect your resume, references, or other relevant information.

vi. Information About Your Use of the Services. We collect information about your use of the Services, such as your Internet Protocol (“IP”) address, browser attributes and type, mobile device and operating system, the pages you visit on our Services, the content you view on the Services, the date and time of your visits, and other clickstream data that helps us understand how you interact with the Services. We may collect this information through third-party analytics tools.

vii. Geolocation Information. We may collect your geolocation information if your device has enabled sharing of your precise geolocation data.

viii. Cookie Information. We only use strictly necessary cookies and Google Analytics on our Services. Such cookies collect information about you, such as your IP address, user ID, and how you interact on our Services. Please see the Cookie section below for more information.

### 3. THIRD PARTY SOURCES OF INFORMATION

Upon your request, we may collect or share information about you or others from third-party products or services integrated into our Services. For example, you can post comments on our Medium blog by logging into your Medium account.

### 4. HOW WE USE YOUR INFORMATION

In addition to some of the specific uses of personal information we describe in this Privacy Policy, we may use information that we receive to:

i. Provide the Services. When accessing Knox Wallet, our website, or otherwise using our Services, we collect certain information about you to be able to support your requests. For example, we may collect information about you and your company when you complete

an inquiry form on our website or Knox Wallet to hear more about our products and services. An additional example includes we collect information relating to your use of Knox Wallet at your request such as transactions descriptions or other account and transaction information. In some cases, we cannot provide you with our Services without processing your personal information.

ii. Provide Service-related Communications. If you have purchased our Services, we will send you administrative or service-related information. Such communications may include confirmation of your transactions, technical notices, security updates, or other relevant information. Service-related communications are not promotional in nature, therefore they are not marketing communications. You cannot unsubscribe from service-related communications because they are important and can affect the way you use the Services.

iii. Enforce our Terms, Agreements or Policies. We process your personal information to enforce certain terms, agreements and policies relevant to our relationship with you, including any agreements with third party partners. We may collect fees based on your use of the Services or referral services, and actively monitor, investigate, prevent or mitigate any alleged or actual prohibited, illicit or illegal activities on our Services. This processing allows us to maintain a trusted environment for you. We cannot perform the Services without such processing.

iv. Provide Customer Support. Whenever you contact us for customer support or any other reason (e.g., diagnose or fix technology problems, to provide feedback, notify us of a dispute, etc.), we process any information you provide to us and any information we already have about you. Without processing your personal information for such purposes, we cannot respond to you or ensure your continued use and enjoyment of the Services.

v. Provide Secure Services. We are committed to ensuring your personal information is processed securely on our Services. To maintain the security of our Services, we may process your personal information to investigate, detect, prevent or report fraud, misrepresentation, security incidents or breaches, spam, malware, malicious activities or other prohibited or illegal activities. In addition, we process your personal information to improve the security of our Services. We cannot provide the Services securely without such processing.

vi. Conduct Research and Product Development. We may process your personal information to improve, optimize or expand our Services or features of our Services. We do so by processing information about your use of the Services, any information you provide to us (e.g., feedback, survey responses, etc.) and by measuring, tracking and analyzing trends and usage in connection to your use or the performance of our Services. We take additional security measures when processing your personal information for such purposes, such as by de-identifying (or “pseudonymizing”) your personal information and limiting access to our personnel to such data. Without processing your information for such purposes, we may not be able to ensure your continued enjoyment of part or all of our Services.

vii. Engage in Marketing Activities. We engage in marketing activities with individuals

that may be interested in our products and services. Please note, TokenSoft does not engage in marketing activities for end-users of white-labeled products and services, including but not limited to end users of its customers' using the white-labeled platform. When TokenSoft provides services directly to the end user (e.g. Knox Wallet), TokenSoft may engage in marketing activities. When engaging in marketing activities, we may process personal information to: send you marketing communications; run contests, special offers or other events or activities; send you information about opportunities, products, services, contests, promotions, discounts, incentives, surveys, and rewards offered by us and select partners; or otherwise market our products and services, including targeted marketing. When you share your friends' or business partners' contact information with us, we may reach out to them on your behalf in accordance with applicable laws. You can unsubscribe from marketing communications at any time and without charge.

viii. **Maintain Legal or Regulatory Compliance.** We may be required to process your personal information under certain laws and regulations, such as compliance with recruitment and employment laws, tax laws or other business obligations, as otherwise required by applicable law. We cannot provide the Services to you without such processing. We will disclose any other purposes to you in connection with our Services prior to processing your personal information for such purposes. You may choose not to allow us to process your personal information for any purposes that are not compatible with the purposes for which we originally collected your personal information or subsequently obtained your consent. However, you should be aware that if you choose to limit how we use your personal information, some or all of our Services may not be available to you.

## 5. SHARING OF YOUR INFORMATION

We may share your information as follows.

i. **Affiliated Businesses.** We may share your personal information with group companies and affiliates. Affiliated businesses may use your information to help provide, understand, and improve the Services and Affiliates' own services.

ii. **Our Service Providers, Business Partners and Others.** We may share your personal information with our service providers, business partners or third-party organizations that help us provide the Services to you. Such entities will be given access to your information as is reasonably necessary to provide the Service under contractual obligations at least as protective as this Policy.

iii. **Anonymous or Aggregate Data.** TokenSoft or our service providers may share anonymized or aggregated information with any third parties. Such information no longer reasonably identifies you.

iv. **Your Actions.** Any information or content that you voluntarily disclose for posting to the Services, such as blog comments or social media posts on our social media profiles, become available to the public.

v. **Change of Control.** We may share your personal information with a subsequent

owner, co-owner, or operator of our Services, or in connection with a corporate merger, consolidation, or restructuring; financing, acquisition, divestiture, or dissolution of all or some portion of our business; or other corporate change. We will notify you with any choices you may have regarding your information.

vi. Safety and Legal Compliance. We may share your personal information if we believe that such disclosure is necessary to: comply with any applicable laws, regulations, legal processes or requests by public authorities (e.g., law enforcement, tax authorities, etc.); protect you, us or our other users' rights or property, or to protect our Services; comply or enforce our terms, agreements or policies.

vii. Knox Wallet. Transaction information you provide to us will be broadcast publicly the network necessary to confirm the transaction. Cryptocurrency transactions are by default public information and you should never consider such transactions private.

## 6. MARKETING CHOICES

Our customers or prospects can unsubscribe from marketing email communications from us by clicking on the "unsubscribe link" provided in such communications. As noted above, we do not collect customer end user information for marketing purposes. Also, you may not opt out of Service-related communications (e.g., account verification, purchase and billing confirmations and reminders, changes/updates to features of the Service, technical and security notices).

## 7. TRANSFER OF YOUR INFORMATION

When you access or use our Services, your information may be processed in the United States or any other country in which TokenSoft, its affiliates or service providers maintain facilities. Such countries or jurisdictions may have data protection laws that are less protective than the laws of the jurisdiction in which you reside. If you do not want your information transferred to, processed, or maintained outside of the country or jurisdiction where you are located, you should immediately stop using the Services.

## 8. ACCESS & MODIFICATION

You may access and update the information we have about you by contacting us directly at [privacy@tokensoft.io](mailto:privacy@tokensoft.io). We may need to verify your identity before we grant access or otherwise modify the information we have on file for you.

## 9. SECURITY

We use commercially reasonable safeguards to keep your personal information safe and require our service providers to do the same. However, the internet is not a secure environment and we cannot guarantee that your personal information is 100% safe.

## 10. RETENTION

We generally retain your personal information as long as necessary to fulfill the purposes of collection or to comply with applicable law. Otherwise we will try to delete your personal information upon your request or when we no longer need it for the purposes we originally collected it for. We will not delete any personal information that you share with other users, unless such other users also wish to delete their personal information at the same time.

We recognize that retention requirements can vary between jurisdictions, but we generally apply the retention periods described below.

- i. Customer and User Marketing Contact Information. We will retain your marketing contact information until you unsubscribe from our marketing communications. Upon your request to unsubscribe, we will store your contact information on our suppression list to ensure we do not send you marketing communications in the future.
- ii. Information About Your Use of the Services. We collect information about your interactions with our Services and we may store such information indefinitely for the establishment or defense of legal claims, audit, or fraud and/or crime prevention purposes.
- iii. Google Analytics Data. Any Google Analytics information is retained up to one year from expiry of the cookie or the date of collection.

## 11. LINKS TO THIRD PARTIES

We are not responsible for the practices employed by any websites or services linked to or from our Service, including the information or content contained within them. Please remember that when you use a link to go from our Service to another website or service, our Privacy Policy does not apply to those third-party websites or services, even if they are offered within or through our Services.

## 12. COOKIES

Cookies are small data files that we transfer to your device to collect information about your use of our Services. Cookies can be recognized by the website that downloaded them or other websites that use the same cookies. This helps websites know if your browsing device has visited them before.

We generally treat information collected by cookies and other tracking technologies as non-personal information. However, to the extent that IP addresses or similar identifiers are considered personal information by local law, we also treat cookie information with identifiers as personal information. If we combine non-personal information with personal information, then the combined information will be treated as your personal information for as long as it remains combined.

i. Purposes for Cookie Collection.

Cookies can be useful in many different ways, and we use cookies for a variety of purposes. TokenSoft uses cookies to help it understand how the Services are being used, such as whether you spent more time on a certain part of the Services, whether you experienced any technical issues, and more. Some of the functions performed by cookies are strictly necessary for us to be able to offer you our Services, while other cookies provide us with valuable insight about how we can improve our Services or help us with marketing our products and services to you based on your interests and preferences.

ii. Who Owns Cookie Data?

We use both first-party and third-party cookies on our Services. First-party cookies are cookies that are placed on your device by us, while third-party cookies are set by parties other than TokenSoft. Third-party cookies are operated by third parties that can recognize your device both when it visits our Services and when it visits other websites or mobile apps. TokenSoft does not control how third-party cookies are used, and we encourage you to check the websites of any third-party cookie providers for more information about how they use cookie information.

iii. How to Manage Cookies

- a. First-Party Cookies: You can enable, disable or delete cookies via your browser settings. To do this, follow the instructions provided by your browser, usually located within the “Help”, “Tools” or “Edit” settings of your browser. Please be aware that if you set disable cookies on your browser, you may not be able to access secure areas of the Services and parts of the Services may also not work properly (e.g., referral links or Service preferences).
- b. Third-Party Cookies: Any cookies that are placed on your browsing device by a third party can be managed through your browser (as described above) or by checking the third party’s website for more information about cookie management and how to “opt-out” of receiving cookies from them. For Google Analytics, you may opt out by going to: [https:// tools.google.com/dlpage/gaoptout](https://tools.google.com/dlpage/gaoptout) (requires you to install a browser add-on).

### 13. “DO-NOT-TRACK” SIGNALS

Do-Not-Track is an optional browser setting that allows you to express your preferences about online tracking across websites. We do not have a way to respond to Do-Not-Track signals.

### 14. YOUR CALIFORNIA PRIVACY RIGHTS

California law permits California residents to ask us for a notice identifying the categories of personal information which we share with our affiliates and/or third parties for marketing purposes, and providing contact information for such affiliates and/or third parties. If you

are a California resident and would like a copy of this notice, please submit a written request to us at the email address provided under the “Contact Us” section.

## 15. NOTICE TO INDIVIDUALS IN THE EUROPEAN ECONOMIC AREA AND SWITZERLAND

This section only applies to individuals using or accessing our Service while located in the European Economic Area, United Kingdom and/or Switzerland (collectively, the “Designated Countries”) at the time of data collection.

We may ask you to identify which country you are located in when you use or access some of the Services, or we may rely on your IP address to identify which country you are located in. When we rely on your IP address, we cannot apply the terms of this section to any individual that masks or otherwise hides their location information from us so as not to appear located in the Designated Countries. If any terms in this section conflict with other terms contained in this Policy, the terms in this section shall apply to individuals in the Designated Countries.

i. Our Relationship to You. TokenSoft is a data controller with regard to any personal information collected from individuals accessing or using its Service. A “data controller” is an entity that determines the purposes for which and the manner in which any personal information is processed. Any third parties that handle your personal information in accordance with our instructions are our service providers and are “data processors.”

You are a “User.” Users are individuals providing personal information to us via our Services, such as by sending us an inquiry form, signing up for our newsletter(s), or otherwise accessing or using our Services.

ii. Legal Bases for Processing Personal Information. Below is a chart indicating the legal bases we rely in processing personal information.

[REMAINDER OF THE PAGE INTENTIONALLY LEFT BLANK.]

Section	Purposes of Processing	Legal Basis for Processing
6(i)	Provide the Services	Processing is based on our contract obligations or to take steps at the request of the individual prior to entering into a contract.
6(ii)	Provide Service-related Communications	
6(iii)	Enforce our Terms, Agreements or Policies	
6(iv)	Provide Customer Support	
6(v)	Secure our Services	
7(i)	Affiliated Businesses	
7(ii)	Our Service Providers, Business Partners and Others	

6(vi)	Conduct Research and Product Development	Processing is based on our legitimate interest to better understand you, to maintain and improve the accuracy of the information we store about you, and to better promote or optimize our Services.
7(v)	Change of Control	
6(viii)	Maintain Legal or Regulatory Compliance	Processing is necessary for compliance with our legal obligations, the public interest, or in your vital interests.
7(vi)	Safety and Legal Compliance	

iii. Marketing. We will only contact you if you are located in the Designated Countries by electronic means (including email or SMS) based on our legitimate interests, as permitted by applicable law, or your consent. When we rely on legitimate interest, we will only send you information about our Services that are similar to those which were the subject of a previous sale or negotiations of a sale to you.

If you do not want us to use your personal information in this way, or to disclose your personal information to third parties for marketing purposes, please click an unsubscribe link in your emails or contact us at [privacy@tokensoft.io](mailto:privacy@tokensoft.io). You can object to direct marketing at any time and free of charge.

iv. Individual Rights. We provide you with the rights described below when you use our Services. We may limit your individual rights requests (a) where denial of access is required or authorized by law; (b) when granting access would have a negative impact on other's privacy; (c) to protect our rights and properties; or (4) where the request is frivolous or burdensome.

If you would like to exercise your rights under applicable law, please contact us at [privacy@tokensoft.io](mailto:privacy@tokensoft.io). We may seek to verify your identity when we receive an individual rights request from you to ensure the security of your personal information.

a. Right to withdraw consent. For any consent-based processing of your personal information, you have the right to withdraw your consent at any time. A withdrawal of consent will not affect the lawfulness of our processing or the processing of any third parties based on consent before your withdrawal.

b. Right of access. Upon your request, we will provide you with a copy of your personal information in our files without undue delay and free of charge, unless we permitted by law to charge a fee. Your access may limited to the extent it would adversely affect the rights and freedoms of other individuals.

c. Right to rectification (or “correction”). You may request to correct or update any of your personal information in our files. We may provide you with the ability to update some or all of your personal information directly via the Services.

d. Right to erasure (or the “Right to be Forgotten”). Upon your request, we will erase any of your personal information in our files that: is no longer necessary in relation to the purposes for which it was collected or otherwise processed; was collected in relation to processing that you previously consented to, but later withdrew such consent; or was collected in relation to processing activities to which you object, and there are no overriding legitimate grounds for our processing.

e. Right to restriction. You have the right to restrict our processing of your personal information where one of the following conditions applies:

- 1) You contest the accuracy of your personal information that we processed. If you restrict processing based on this condition, you may experience an interruption of some or all of the Services during the period necessary for us to verify the accuracy of your personal information;
- 2) The processing is unlawful and you oppose the erasure of your personal information and request the restriction of its use instead;
- 3) We no longer need your personal information for the purposes of the processing, but it is required by you to establish, exercise or defense of legal claims; or
- 4) You have objected to processing, pending the verification whether the legitimate grounds of our processing override your rights.

During the time which restriction of processing applies, we will only process your restricted personal information with your consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest. We will inform you if or when the restriction is lifted.

f. Right to object to processing. You may object to our processing at any time and as permitted by applicable law if we process your personal information on the legal bases of: consent; contract; or legitimate interests. We may continue to process your personal information if it is necessary for the defense of legal claims, or for any other exceptions permitted by applicable law.

g. Right to data portability. If we process your personal information based in a contract with you or based on your consent, or the processing is carried out by automated means, you may request to receive your personal information in a structured, commonly used and machine-readable format, and to have us transfer your personal information directly to another “controller,” where technically feasible, unless exercise of this right adversely affects the rights and freedoms of

others. Your right to data portability only applies to personal information provided by you to us.

h. Notification to third parties. When we fulfill your individual rights requests for correct (or rectification), erasure or restriction of processing, we will notify third parties also handling the relevant personal information unless this proves impossible or involves disproportionate effort. Upon your request, we will identify such third parties.

i. Member representative. If you have questions, you may reach our member representative at DPR Group by sending an email to DPR Group at [datainquiry@dpr.eu.com](mailto:datainquiry@dpr.eu.com) quoting <Tokensoft Inc.> in the subject line; submitting an inquiry online through their webform at [www.dpr.eu.com/datarequest](http://www.dpr.eu.com/datarequest); or mailing your inquiry to 1-2 Marino Mart, Fairview, Dublin 3, Ireland.

j. Transfer of your personal information. We transfer your personal information subject to appropriate safeguards as permitted under the Data Protection Laws. Specifically, when your personal information is transferred out of the Designated Countries, we have the required contractual provisions for transferring personal information in place with the third-parties to which your information is transferred. For such transfers, we rely on legal transfer mechanisms such as Standard Contractual Clauses or we work with U.S. based third parties that are certified under the EU-U.S. and Swiss-U.S. Privacy Shield Framework.

Tokensoft also participates in and has certified its compliance with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks (“Privacy Shield”) as set forth by the U.S. Department of Commerce regarding the processing of personal information transferred the European Union (“EU”) member countries, European Economic Area (“EEA”), and Switzerland to the United States. Tokensoft has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about Privacy Shield, and to view our certification, visit the <https://www.privacyshield.gov>.

Under Privacy Shield, we are responsible for the processing of personal information we receive and any subsequent transfer of personal information to third parties acting for or on our behalf. We will remain responsible if a third party processes your personal information in a manner inconsistent with our Privacy Shield commitments or this Privacy Policy, unless Tokensoft is not responsible for the violation. Pursuant to the Privacy Shield Principles, Tokensoft will use personal information only in ways that are compatible with the purposes for which the information was collected or subsequently authorized by you.

Tokensoft commits to resolve complaints about the processing of EU, EEA, or Swiss personal information in compliance with the Privacy Shield Principles. Individuals with inquiries or complaints regarding this Privacy Policy should first contact Tokensoft at [privacy@tokensoft.io](mailto:privacy@tokensoft.io).

If you have an unresolved complaint or dispute arising under the requirements of Privacy Shield, we agree to refer your complaint under the Framework to an independent dispute resolution mechanism. Our independent dispute resolution mechanism is the International Centre for Dispute Resolution / American Arbitration Association (“ICDR/AAA”). For more information and to file a complaint, you may contact the ICDR/AAA by visiting the website at <http://go.adr.org/privacyshield.html>.

The U.S. Federal Trade Commission has regulatory enforcement authority over our processing activities of personal information transferred pursuant to Privacy Shield. Under certain conditions, described more fully on the Privacy Shield website, you may invoke binding arbitration option when other dispute resolution procedures have been exhausted. In certain situations, Tokensoft may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

k. Right to lodge complaint. If you believe we have infringed or violated your privacy rights, please contact us at [privacy@tokensoft.io](mailto:privacy@tokensoft.io) so that we may resolve your dispute directly. You also have a right to lodge a complaint with a competent supervisory authority situated in a Member State of your habitual residence, place of work, or place of alleged infringement.

## HOW TO CONTACT US

If you have any questions about this Privacy Policy or our Services, please contact us at [privacy@tokensoft.io](mailto:privacy@tokensoft.io) or 44 Montgomery St., #3865, San Francisco, CA 94104.