*Last updated on 10.10.2025*

# Privacy Policy

This Privacy Policy (hereinafter – "Policy") explains how **STOCKENN LLC**, a limited liability company incorporated under the laws of Wyoming, USA with its registered office at 30 N Gould St #47571, Sheridan, WY 82801 ("**Company**", "**we**", "**us**", or "**our**"), collects, uses, stores, and protects your personal data when you access and use our web-based platform available at **https://stockenn.com** (the "**Platform**").

We are committed to protecting your privacy and handling your personal data in a lawful, fair, and transparent manner. This Policy is drafted in accordance with the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and applicable ePrivacy rules.

This Policy applies to all Users of the Platform, including those who register an account, undergo CDD and Enhanced EDD checks, participate in activities, submit entry fees/payments, claim rewards, or otherwise interact with the Platform. It also applies to visitors who browse the Platform without registering.

*If you do not agree with any provision of this Policy, please refrain from using the Platform. For any questions, contact **legal@stockenn.com**.*

## 1. Definitions

**"Platform"**: the website operated by the Company (available at https://stockenn.com) that enables Users to register, access services and participate in activities.

**"User"**: any natural person who visits, accesses, registers on, or otherwise interacts with the Platform.

**"Personal Data"**: any information relating to an identified or identifiable natural person (GDPR Art. 4(1)).

**"Processing"**: any operation performed on Personal Data (GDPR Art. 4(2)).

**"Controller"**: the natural or legal person which determines the purposes and means of the processing of Personal Data (GDPR Art. 4(7)).

**"Processor"**: a natural or legal person which processes Personal Data on behalf of the Controller (GDPR Art. 4(8)).

**"Applicable Law"**: GDPR, national data protection laws, ePrivacy rules, AML/CTF laws, consumer protection, and other relevant laws.

**"Services"**: all features, functions, content and technologies made available through the Platform.

**"KYC/CDD":** Know Your Customer / Customer Due Diligence checks performed to verify identity and eligibility in accordance with Applicable Law and the Company's onboarding policy.

**“Enhanced KYC/EDD”**: Enhanced Due Diligence requiring additional documents (e.g., source of funds/wealth) in higher-risk cases.

## 2. Scope and applicability

This Policy covers processing of Personal Data of Users and visitors of the Platform, including data collected via forms, payments, support requests, cookies and analytics. This Policy forms an integral part of the **Terms of Use** [link]; capitalised terms not defined here have the meanings given there.

We only process Personal Data where a valid legal basis exists under GDPR (see Section 4). Where consent is required (e.g., non-essential cookies or direct marketing), we obtain your explicit consent (GDPR Art. 6(1)(a), Art. 7).

By ticking the applicable checkbox indicating your acceptance during registration or onboarding, you confirm that you have read, understood, and expressly agree to this Policy. If you do not provide such explicit consent, you will not be able to use the Platform or its Services. For any questions, contact **legal@stockenn.com**.

## 3. Principles of processing

We process Personal Data in line with the core principles set out in the GDPR:

| Principle | Description |
|---|---|
| Lawfulness, fairness, transparency | All processing is based on a valid legal basis under Art. 6 GDPR. We provide clear, accessible information to Users on how their data is used, ensuring transparency at the point of collection. |
| Purpose limitation | Data is collected only for specified, explicit, and legitimate purposes and is not further processed in ways incompatible with those purposes (Art. 5(1)(b)). |
| Data minimisation | We ensure that Personal Data is adequate, relevant, and limited to what is necessary for the purposes pursued (Art. 5(1)(c)). |
| Accuracy | We take reasonable steps to keep Personal Data accurate and up to date. Users may request rectification of inaccurate data (Art. 5(1)(d)). |
| Storage limitation | Data is kept no longer than necessary for the purposes for which it was collected, subject to statutory retention obligations (Art. 5(1)(e)). |
| Integrity and confidentiality | We secure data with appropriate technical and organisational measures to protect against unauthorised or unlawful processing, accidental loss, destruction, or damage (Art. 5(1)(f); Art. 32). |

| | |
|---|---|
| Accountability | We are responsible for, and can demonstrate compliance with, all GDPR principles (Art. 5(2)). This includes maintaining records of processing activities (Art. 30), conducting Data Protection Impact Assessments (Art. 35) where necessary, and implementing data protection by design and by default (Art. 25). |

We also ensure that any third-party Processors we engage provide sufficient guarantees to implement appropriate technical and organisational measures (Art. 28), and that such processing is governed by a binding Data Processing Agreement. Internal staff are trained and subject to confidentiality obligations, and we regularly review compliance with these principles.

## 4. Legal bases for processing

Depending on context, we rely on one or more of the following legal bases:

*Performance of a contract* (GDPR Art. 6(1)(b)): account registration and management; providing Platform features; processing fees/payments; calculating rankings/scores; disbursing rewards; customer support.

*Compliance with legal obligations* (GDPR Art. 6(1)(c)): AML/CTF obligations; identity verification (KYC/CDD/Enhanced KYC/EDD); responding to lawful requests from authorities.

*Legitimate interests* (GDPR Art. 6(1)(f)): platform security; fraud and abuse prevention; product analytics and improvement; defending legal claims. We balance these interests against your rights (Art. 6(1)(f)).

*Consent* (GDPR Art. 6(1)(a)): non-essential cookies/analytics; direct marketing; optional features. You may withdraw consent at any time (Art. 7(3)).

Special categories (if applicable): We do not seek to process special categories (GDPR Art. 9). If certain KYC vendors process biometric data for liveness/ID matching, we will rely on explicit consent (GDPR Art. 9(2)(a)) or, where supported by national AML law, substantial public interest with safeguards (GDPR Art. 9(2)(g)). Where used, you will be clearly informed and provided with an alternative where feasible.

*California residents / U.S. privacy (CCPA/CPRA):*

The Company does not provide services to residents of the United States and access to the Platform from within the U.S. is restricted. However, if you are a resident of California and access the Platform (for example, using a VPN) and provide Personal Data such as an email address for marketing, we will treat your data in line with the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA).

You will not be able to proceed with onboarding or access Services, but any limited processing of your data (e.g., marketing communications) will respect all

rights granted by CCPA/CPRA, including the right to know, delete, opt-out of sale/sharing, and non-discrimination.

To exercise these rights, please contact **legal@stockenn.com** with the subject line "CCPA Request." We may need to verify your identity before fulfilling the request.

## 5. Types of Personal Data we collect

### 5.1 Data you provide directly

These are Personal Data that you voluntarily provide to us when registering, completing onboarding, interacting with the Platform or contacting us.

| Category | Examples |
|---|---|
| Identification data | First name, last name, date of birth, nationality/country of residence, username/nickname. |
| Contact details | Email address, phone number. |
| Account data | Settings, preferences, communications. |
| Payments | Transaction identifiers, payment method, wallet address (if applicable), payout details. We do not store payment card credentials, banking login details, or any sensitive authentication data; such information is processed exclusively by our regulated payment service providers. |
| KYC/CDD | Government-issued ID, proof of address, selfie/liveness checks, sanctions/PEP screening results. These documents and biometric data are not stored by the Company; they are processed and stored by our authorised verification providers. The Company only receives and processes the results/outcomes of such checks. |
| Enhanced KYC/EDD | Source of funds/wealth documents, profession/employer, purpose and expected nature of relationship. |

### 5.2 Data collected automatically

| Category | Examples |
|---|---|
| Technical data | IP address, device/OS, browser type/version, language/time zone, access times, referring URLs |
| Usage data | Session data, feature interactions, activity logs, error/crash logs |
| Cookies/trackers | Data collected via cookies, pixel tags or similar technologies (see Cookies Policy) |

### 5.3 Data from third parties

| Source | Examples |
|---|---|
| Payment processors | Payment confirmations, fraud risk indicators. |
| KYC/AML vendors | Verification outcomes, sanctions/PEP hits, document authenticity check. |
| Affiliates/partners | Referral and attribution data. Currently not collected; may be introduced in the future if affiliate or partnership programmes are launched, in which case Users will be duly informed in advance. |

### 5.4. Categories of Personal Data we do not collect

The Company applies a strict policy to avoid processing certain sensitive categories of Personal Data. In particular, we do not intentionally collect or use the following types of data:

*Data of minors*: We do not knowingly collect data from individuals under the age of 18. When we become aware that a minor has submitted information without verified parental or guardian consent, such data will be securely deleted and access to the Platform restricted.

*Special categories of data*: We do not process sensitive information such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for unique identification, health information, or data relating to sex life or sexual orientation, unless expressly required by law with adequate safeguards.

*Criminal records*: We do not handle data relating to criminal convictions or offences unless processing is explicitly mandated by Applicable Law for compliance, background checks, or due diligence purposes.

*Illegitimately obtained data*: We will not process Personal Data acquired through unlawful, non-transparent, or unauthorised sources. Any processing of such data will occur only if the User has been properly informed and there is a valid legal basis under GDPR (e.g., performance of a contract, legal obligation, or legitimate interest).

If you believe that your data has been collected in contravention of these rules, please contact us at **[legal@stockenn.com]**. We will review the situation promptly and take appropriate corrective measures, including secure deletion where necessary.

Should exceptional circumstances require us to process any of the above categories, we will only do so with your explicit, informed consent and in strict compliance with GDPR and other Applicable Laws.

## 6. Purposes of use and legal bases

| Purpose | Examples | Legal basis |
|---|---|---|
| Account creation & management | register account, authenticate, manage preferences | GDPR Art. 6(1)(b) |
| Providing core features | enable activities calculate results, distribute rewards | GDPR Art. 6(1)(b) |
| Payments | process entry fees/payouts; bookkeeping | GDPR Art. 6(1)(b)/(c) |
| KYC/CDD/EDD | identify/verify; screen PEP/sanctions; risk assessment; source of funds | GDPR Art. 6(1)(c); Art. 9(2)(a)/(g) if biometrics |
| Security & fraud prevention | monitor abuse/bots; protect integrity | GDPR Art. 6(1)(f) |
| Customer support & disputes | handle requests/complaints; exercise rights | GDPR Art. 6(1)(b)/(c) |
| Analytics & improvement | usage analytics, A/B tests | GDPR Art. 6(1)(f) (with cookie consent) |
| Marketing | newsletters, promotions | GDPR Art. 6(1)9a) (consent) ; opt-out anytime |

## 7. Data sharing and disclosure

We do not sell, rent, or otherwise commercially exploit your Personal Data under any circumstances.

However, in order to operate the Platform lawfully and provide you with Services, we may share your Personal Data with carefully selected third parties strictly on a need-to-know basis and in accordance with the GDPR.

Such disclosures are limited to the following categories:

*Service providers acting on our behalf*, including cloud hosting and infrastructure providers (to securely host and operate the Platform), communication service providers (to send you essential notifications and updates), analytics partners (to understand user behaviour and improve Platform functionality), and vendors providing fraud detection or technical support. These providers are bound by strict contractual and confidentiality obligations and act solely under our instructions. They are not permitted to use your data for their own purposes.

*Regulated third-party providers*, including payment institutions, e-money providers, banks, and identity verification/compliance vendors (to process deposits, withdrawals, fees, prize disbursements, and perform AML/KYC/EDD checks). These parties operate under their own regulatory regimes, but we only engage providers

that demonstrate sufficient guarantees of data protection in line with GDPR standards.

*Legal disclosures*, where we are required to disclose Personal Data by law, regulation, subpoena, or court order; in response to legitimate requests from government authorities, regulators, or law enforcement bodies; or where disclosure is necessary to exercise, establish, or defend our legal rights, or to protect the safety of our Users and the integrity of the Platform.

*In the event of a restructuring* of the Company or transfer of the Platform's operation to another legal entity (for example, a successor DAO operator), your Personal Data may be transferred to that entity, provided equivalent privacy protections are ensured.

Any such disclosures will be made only for the same or directly related purpose for which the data was initially collected; where the class of recipient has been disclosed to you in advance; and with your consent, where required by law.

We ensure that all such data sharing complies with GDPR requirements, and we maintain records of all disclosures as required under Art. 30 GDPR.

## 8. International transfers

Your Personal Data may be transferred to and processed in countries outside the European Economic Area (EEA), particularly where our service providers, infrastructure providers, or compliance partners are located. Such transfers will always be carried out in strict compliance with Chapter V of the GDPR and only where an appropriate safeguard is in place to ensure your data remains adequately protected.

We rely primarily on the following mechanisms: adequacy decisions of the European Commission (Art. 45 GDPR), Standard Contractual Clauses approved by the Commission or competent authority together with transfer impact assessments and supplementary security measures (Art. 46 GDPR), or, in limited and exceptional cases, derogations such as your explicit, informed consent (Art. 49 GDPR).

Whenever an international transfer occurs, we take steps to ensure that the level of protection afforded to your Personal Data is not undermined. This includes contractual, technical, and organisational measures such as encryption, restricted access, and ongoing monitoring of local legal frameworks.

Further details of the specific safeguards used in connection with any international transfers, including a copy of the Standard Contractual Clauses where applicable, are available on request by contacting us at **[ legal@stockenn.com ]**.

## 9. Retention

We retain your Personal Data only for as long as it is necessary to achieve the purposes for which it was collected or as required by Applicable Law. This approach is consistent with the storage limitation principle under Art. 5(1)(e) GDPR, which

obliges controllers not to keep personal data longer than necessary, and the accountability principle under Art. 5(2) GDPR, which requires us to demonstrate compliance.

Retention periods differ depending on the category of data and the applicable legal basis:

*Account and profile data*: Retained for the duration of the contractual relationship (Art. 6(1)(b) GDPR – performance of contract) and for 12 months after account closure or prolonged inactivity. After this period, data is deleted or irreversibly anonymised unless further retention is required by law (e.g., fraud prevention, pending disputes).

*Transaction and payment records*: Retained for 5 years to comply with statutory accounting and tax obligations (Art. 6(1)(c) GDPR – legal obligation), in line with national commercial and tax legislation.

*KYC/CDD/EDD and AML-related records*: Retained for a minimum of 5 years from the termination of the business relationship or the date of the last transaction, whichever is later, as required by AML/CTF regulations. In some jurisdictions, this period may be extended up to 10 years (Art. 6(1)(c) GDPR – legal obligation; Recital 39, 65 GDPR).

*Security, audit and analytics logs*: Retained for up to 6 months, unless longer retention is necessary due to an ongoing investigation, fraud detection, or platform abuse (Art. 6(1)(f) GDPR – legitimate interest in ensuring security and integrity of the Platform).

Where immediate deletion is not technically possible (for example, because the data is stored in encrypted backups), we ensure that such data is securely isolated, access-restricted, and removed at the next available deletion cycle.

Once the retention period expires, we either securely erase the Personal Data, anonymise it for statistical purposes (where lawful), or retain it only in aggregate form that no longer identifies individual Users.

Users retain the right to request erasure of their Personal Data under Art. 17 GDPR (Right to erasure), subject to exceptions (e.g., compliance with legal obligations or the establishment, exercise or defence of legal claims).

## 10. Your rights

As a data subject, you benefit from a comprehensive set of rights under the GDPR. These rights empower you to maintain control over your Personal Data and ensure that it is processed lawfully, fairly, and transparently. Each right is subject to certain conditions, exceptions, or limitations as set out in the Regulation.

You may exercise any of the rights described below at any time by contacting us at **legal@stockenn.com**]. We may request reasonable information to verify your identity before acting on your request (Art. 12(2) GDPR). We will respond without

undue delay and in any event within one month, extendable by two further months for complex requests (Art. 12(3) GDPR).

Your rights include:

- *Right to be informed (Art. 13–14 GDPR)*

You have the right to receive clear and transparent information about how we collect and process your Personal Data, including the purposes of processing, categories of data, recipients, retention periods, and your rights. This Privacy Policy and any notices provided at the point of data collection fulfil this obligation.

- *Right of access (Art. 15 GDPR)*

You may request confirmation as to whether we process your Personal Data and, if so, obtain access to it, together with details on the categories of data held, purposes of processing, recipients, retention periods, and safeguards for international transfers. We will provide a copy of the data in a commonly used electronic format unless this adversely affects the rights of others.

- *Right to rectification (Art. 16 GDPR)*

You may request correction of inaccurate or incomplete Personal Data. Where feasible, we will integrate updates provided by you without undue delay.

- *Right to erasure ("right to be forgotten") (Art. 17 GDPR)*

You may request the deletion of your Personal Data where:

- the data is no longer necessary for the purposes for which it was collected;
- you withdraw consent and no other lawful basis exists;
- you successfully object to processing (see below);
- the processing is unlawful;
- erasure is required to comply with a legal obligation.

Exceptions apply where processing is necessary, for example, to comply with legal retention duties (e.g., AML/CTF), to exercise or defend legal claims, or for reasons of public interest.

- *Right to restriction of processing (Art. 18 GDPR)*

You may request that we restrict processing of your Personal Data in the following cases:

- you contest its accuracy (pending verification);
- processing is unlawful but you oppose erasure;
- we no longer need the data but you require it for legal claims;
- you have objected to processing (pending verification of legitimate grounds).

Where processing is restricted, your data will be stored but not further processed, except with your consent or for legal claims.

- *Right to data portability (Art. 20 GDPR)*

Where processing is based on consent (Art. 6(1)(a)) or contract (Art. 6(1)(b)) and carried out by automated means, you may request to receive your Personal Data

in a structured, commonly used, machine-readable format, and have it transmitted directly to another controller where technically feasible.

- *Right to object (Art. 21 GDPR)*

You may object, on grounds relating to your particular situation, to the processing of your Personal Data carried out on the basis of our legitimate interests (Art. 6(1)(f)). We will stop processing unless we can demonstrate compelling legitimate grounds that override your interests, rights, and freedoms, or unless processing is necessary for legal claims.

You have an unconditional right to object to the processing of your Personal Data for direct marketing, including profiling to the extent related to direct marketing.

- *Rights in relation to automated decision-making and profiling (Art. 22 GDPR)*

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or significantly affects you. Exceptions apply if the decision is:

- necessary for entering into or performing a contract;
- authorised by law with safeguards; or
- based on your explicit consent.

In such cases, you also have the right to obtain human intervention, express your point of view, and contest the decision.

- *Right to withdraw consent (Art. 7(3) GDPR)*

Where processing is based on your consent, you may withdraw that consent at any time without affecting the lawfulness of processing carried out before withdrawal. We will make withdrawing consent as easy as giving it.

- *Right to lodge a complaint (Art. 77 GDPR)*

If you believe that your rights under GDPR have been infringed, you may lodge a complaint with a supervisory authority in your place of habitual residence, place of work, or place of the alleged infringement. Without prejudice to this right, we encourage you to contact us first so that we can attempt to resolve the issue informally.

- *Right to judicial remedy (Arts. 78–79 GDPR)*

In addition to filing a complaint, you also have the right to an effective judicial remedy against a supervisory authority (Art. 78) or against a controller/processor (Art. 79) if you consider that your rights have been violated.

**Exercising your rights**

To exercise any of the above rights, please contact us at **[legal@stockenn.com]**. We will use reasonable measures to verify your identity before responding, which may include confirming account details, requesting proof of identity, or using secure verification procedures.

We commit to handling all requests in accordance with the GDPR and applicable national laws, documenting our responses, and providing clear

explanations if we are unable to fully comply with your request due to legal obligations or applicable exemptions.

## 11. Cookies and tracking technologies

We use cookies and similar technologies to run the Platform, remember preferences, analyse usage, and support marketing. For non-essential cookies, we request consent via our banner and provide granular controls (ePrivacy; GDPR Art. 6(1)(a)). See **Cookies Policy** [link] for details (types, purposes, lifetimes, vendors, opt-out).

## 12. Children's privacy

The Platform is not intended for individuals under the age of 18, and we do not knowingly collect or process their Personal Data. By using the Platform, you confirm that you are at least 18 years old or have reached the age of majority in your country of residence, whichever is higher.

We take the privacy of children very seriously. If we become aware that Personal Data has been collected from a User under 18 years of age without verified parental or guardian consent, we will take reasonable steps to:

- promptly delete such data from our records;
- close or restrict the related User Account;
- prevent any further access to the Platform by the minor; and
- where appropriate, notify the parent or legal guardian.

If you are a parent or legal guardian and believe that your child has provided us with Personal Data, please contact us immediately at **[legal@stockenn.com]** so that we can investigate and take appropriate remedial action.

## 13. Security measures

We are committed to ensuring the security, integrity, and confidentiality of your Personal Data. In line with Art. 32 GDPR, we apply appropriate technical and organisational measures proportionate to the risks associated with processing.

Our key security measures include:

- *Access controls:* restricting access to Personal Data only to authorised staff who require it for their job functions.
- *Encryption and secure storage:* protecting Personal Data in transit and at rest using industry-standard encryption where applicable.
- *Minimisation of data:* we collect and retain only the minimum necessary information. Sensitive documents (e.g., KYC/AML) are processed and stored by authorised third-party providers, not by us.
- *Confidentiality commitments:* ensuring that employees and contractors with access to Personal Data are bound by confidentiality obligations.

- *Third-party due diligence:* engaging only service providers that offer sufficient guarantees of data protection in line with GDPR.

*Personal Data breaches*

If a personal data breach occurs, we will notify the competent supervisory authority within 72 hours (where required by Art. 33 GDPR), and affected Users if the breach poses a high risk to their rights and freedoms (Art. 34 GDPR).

*User responsibility*

Users also share responsibility for safeguarding their data (e.g., by choosing strong passwords, protecting devices, and not disclosing credentials).

## 14. Amendments

We may update this Policy from time to time to reflect changes in our practices, services, legal requirements, or technological developments. All updates will be published in this section with an updated “Last updated” date. Where the changes are material or significantly affect your rights, we will provide additional notice (e.g., by email, in-app notification, or a prominent banner on the Platform) prior to the changes taking effect.

We encourage you to review this Policy periodically to stay informed about how we protect your Personal Data. Your continued use of the Platform after updates have been published will constitute your acceptance of the revised terms.

## 15. Contact information & regulatory details

If you have any questions, concerns, or complaints regarding this Privacy Policy or your Personal Data, or if you wish to exercise your data protection rights, please contact us:

Controller: STOCKENN LLC

Address of Controller: 30 N Gould St #47571, Sheridan, WY 82801

Email: **legal@stockenn.com**