Privacy Policy
Vatom Corp

The protection of personal data is important to us. Therefore, we process personal data on the basis of the applicable data protection laws. In this **Privacy Policy** we inform you about the types of personal data we collect, how this data is used, to whom it is transferred and what options and rights you have in connection with our data processing. In addition, we describe the measures we take to ensure data security and how you, as data subject, can contact us if you have any questions about our data protection practice.

I. Name and Address of the Controller

We, Vatom Corporation, a Delaware corporation, are a *controller* within the meaning of the EU General Data Protection Regulation (GDPR) and other data protection laws and regulations that determine the purposes and means of processing personal data. If you have any questions regarding the processing of your personal data, please do not hesitate to contact us at:

1113 Electric Ave
#13
Venice, CA 90291

Our data protection coordinator can be contacted at info@vatominc.com

II. General Information regarding the Processing of Personal Data

1. Scope of data processing

We only process your personal data if this is necessary to allow you to use the Vatom applications ("**Application**") and to guarantee the Application's functionality and stability. As far as the GDPR is applicable, we only process your personal data if this is required to perform a contract to which you are party according to art. 6 (1) (b) GDPR and to protect our legitimate interests according to art. 6 (1) (f) GDPR.

2. The erasure and storage of personal data

Your personal data will be erased or blocked as soon as it is no longer necessary in relation of the purpose of storage. Furthermore, personal data may be stored if this has been required by regulations, laws or other provisions to which we are subject. The personal data will also be blocked or deleted if a storage period prescribed by the aforementioned standards expires, unless there is a need for further storage of the data for the conclusion or performance of a contract.

III. Creation of Account

A. User Account

1. Collected Information

If you want to create a user account ("**User Account**") on the Application or on our website ("**Website**") we will ask you to provide the following personal information ("**Personal User Account Information**") about you which we will collect and store as described herein:

- First Name
- Last Name
- Date of Birth (optional)
- Email Address
- Telephone Number
- Avatar Image
- Preferred Language
- Password

2. Purpose and Legal Basis of Processing

The processing of the Personal User Account Information allows us to open an individual User Account with a unique user ID ("**User ID**") and an Ethereum wallet address which allows you to hold and control digital objects ("**Vatoms**") that have been created and issued by developers using the Vatom platform ("**Platform**"). The creation of a User Account and individual User ID allows us to know who you are and enables you to interact with other users of the Application. As far as the GDPR is applicable, all processing of your Personal User Account Information is required to perform a contract to which you are party according to art. 6 (1) (b) GDPR and covered by our legitimate interests according to art. 6 (1) (f) GDPR.

3. Storage and Disclosure

Your Personal User Account Information is stored on the Platform which is currently hosted by BlockV (as defined below) on Amazon Web Services (AWS) as well as on the log files of our systems. Your Personal User Account Information will be deleted promptly after you delete your User Account. While we retain your User ID, we will not anymore be able to create a connection between your Personal User Account Information and your User ID. Furthermore, we will not disclose the Personal User Account Information to anyone unless your user name (First Name, Last Name) and/or avatar image is set to "public". In this case, your user name and avatar image is visible to other users of the Application who have created a User Account.

4. Possibility of Objection and Erasure

The processing of your Personal User Account Information is absolutely necessary for the functionality of the Application and your User Account. While you have the right to object to

the processing or to request deletion of your Personal User Account Information, this will lead to the deletion of your User Account and make it impossible for you to use the Application.

B. Studio Account

1. Collected Information

If you want to create a Studio account ("**Studio Account**") on https://studio.vatominc.com, we will ask you to provide the following additional information ("**Personal Studio Account Information**") about you which we will collect and store as described herein:

- First Name
- Last Name
- Email Address
- Password
- Company Name
- Company Logo
- Company Domain
- Billing Credit Card Number, Country, Postal Code and CVC
- Billing Name
- Billing Address

All provisions in this Privacy Policy governing the processing of data relating to the User Account shall apply correspondingly.

2. Purpose and Legal Basis of Processing

The processing of the Personal Studio Account Information allows us to open a Studio Account with a unique User ID that is tied to a business. This account allows you to design, build and distribute Vatoms on the Platform. The creation of a Studio Account and individual User ID allows us to know who you are and enables you to interact with other users of the Application. As far as the GDPR is applicable, all processing of your Personal Studio Account Information is required to perform a contract to which you are party according to art. 6 (1) (b) GDPR and covered by our legitimate interests according to art. 6 (1) (f) GDPR.

3. Storage and Disclosure

Your Personal Studio Account Information is stored on the Studio Platform which is currently hosted by Amazon Web Services (AWS) and a third party: Auth0.com. Billing information such Name, Address, Credit Card Number, Country, Postal Code and CVC are stored by a third party: Stripe.com.

Your Personal Studio Account Information will be deleted promptly after you delete your User Account. While we retain your User ID, we will not anymore be able to create a connection between your Personal Studio Account Information and your User ID. Furthermore, we will not

disclose the Personal Studio Account Information to anyone with the exception of your Company Name, Logo and Domain that is displayed in the informational section of the Vatom.

IV. Verification of the User Account

1. Collected Information

If you want to verify your User Account, we do not need to collect additional information. However, we will need to process your phone number and email address which you have already provided in order to create a User Account ("**Verification Information**").

2. Purpose and Legal Basis of Processing

The verification of your User Account allows us to verify your identity and to restore your access to your User Account if you forget your password. As far as the GDPR is applicable, the processing of your Verification Information is required to perform a contract to which you are party according to art. 6 (1) (b) GDPR and covered by our legitimate interests according to art. 6 (1) (f) GDPR.

3. Storage and Disclosure

In order to verify your User Account, we use the services provided by BlockV AG, a cloud service Platform-as-a-Service (PaaS) company based in Zug, CH-6300, Switzerland ("**BlockV**") and the SMS gateway provider Twilio Inc., a cloud communications Platform-as-a-Service (PaaS) company based in San Francisco, CA 94105, California, USA ("**Twilio**"). Twilio allows us to use two factor authentication ("**2FA**") to guarantee a secure authentication process to and from the platform and to restore access to your User Account. In order for Twilio to carry out authentication by SMS, we will send your telephone number to Twilio. Twilio may process your telephone number outside the EEA but is certified under the EU-US Privacy Shield. The latest data protection information on Twilio and additional information can be found on this website: https://www.twilio.com/legal/privacy.

Alternatively, we use the services of Amazon Web Services EMEA Sàrl. based in L-2338 Luxembourg ("**Amazon**") that allows us to use two factor authentication (2FA). Amazon will use your email address to guarantee a secure authentication process to and from the platform and to restore access to your User Account. In order for Amazon to carry out authentication by Email, we will send your email address to Amazon. The latest data protection information on Amazon can be found on this website: https://aws.amazon.com/privacy.

In order to verify your Studio Account, we use the services provided by Auth0 Inc., a cloud security platform as a service (PaaS) company based in Bellevue, Washington. Auth0 stores your email address and password and will send an email to your email address with a reset link if needed.

4. Possibility of Objection and Erasure

The processing of your Verification Information is absolutely necessary for restoring access to your User Account. While you have the right to object to the processing of the Verification Information or to request deletion of your Personal User Account Information, this will render it impossible to restore access to your User Account if you ever forget your password.

V. Creation of Transaction Data

1. Collected Information

When you create a User Account and use the Application, we collect all transaction data that is related to your User ID ("**Personal Transaction Data**"). This Personal Transaction Data includes, but is not limited to, all transfer of Vatoms from your User Account to another user account, including the redemption of a Vatom, the pick-up or drop-off of a Vatom, or the acquisition of a Vatom.

2. Purpose and Legal Basis of Processing

The collection of Personal Transaction Data is essential in order to verify the location and ownership information regarding all Vatoms that are part of the Vatom ecosystem. Furthermore, some Vatoms have a built-in functionality that are only triggered based on certain transaction patterns. This means that we have to keep track of your Personal Transaction Data to ensure that these functionalities are triggered correctly. As far as the GDPR is applicable, all processing of your Personal Transaction Data is required to perform a contract to which you are party according to art. 6 (1) (b) GDPR and covered by our legitimate interests according to art. 6 (1) (f) GDPR.

3. Storage and Disclosure

Your Personal Transaction Data is stored on the Platform and/or on the blockchain, depending on whether the Vatoms you are using are blockchain-enabled. If you delete your User Account, we will delete your name, telephone number and email as well as any other personal information from your profile. While we retain your User ID, we will not anymore be able to create a connection between your Personal Transaction Data and your Personal Information. We will only disclose your Personal Transaction Data in anonymized form and only to the publishers of the respective Vatoms.

4. Possibility of Objection and Erasure

The processing of your Personal Transaction Data is absolutely necessary for the use of the Application. This means that your Personal Transaction Data cannot be deleted without jeopardizing the functionality and stability of the Application. Your User ID will always remain connected to your Personal Transaction Data. However, when you decide to delete your User Account, we will delete your Personal User Account Information from your User ID. This means that we will not anymore be able to create a connection between you and your Personal Transaction Data. As a result, the Personal Transaction Data does not anymore qualify as personal data within the meaning of the applicable data protection regulation.

VI. Contact Possibility

1. Collected Information

If you want to contact us, you can do so by using the feedback button in the Application or on the Website which will trigger your email application to open a new e-mail pre-addressed to us. If you send the e-mail to us, we will collect your e-mail address as well as your feedback sent within this e-mail. We recommend you to additionally share with us the following information about the device you are using ("**Device Information**") which the new e-mail provides for by default:

- User ID
- Device Type
- Version of Operating System
- Version of Application
- Disk Space
- Memory

2. Purpose and Legal Basis of Processing

The collection of the Device Information as well as of the e-mail address / feedback allows us to provide a better customer service and to better understand the reasons why you are contacting us. As far as the GDPR is applicable, all processing of your email address and Device Information as described above is required to perform a contract to which you are party according to art. 6 (1) (b) GDPR and covered by our legitimate interests according to art. 6 (1) (f) GDPR.

3. Storage and Disclosure

Your Device Information is stored on the Vatom support platform and will be deleted as soon as it is no longer necessary to achieve the above-mentioned purpose. We will neither disclose the Device Information nor your e-mail address to anyone, unless explicitly stated otherwise herein.

4. Possibility of Objection and Erasure

You are free to decide whether you want to share your Device Information with us. If you do not want to share your Device Information with us, you can delete it manually from the email before you press the send button.

VII. Rights of the Data Subjects

We would like to inform you that, subject to the limitations mentioned herein, you have the right to:

- withdraw your consent at any time as set forth in art. 7 GDPR

- request information about the processing of your data as set forth in art. 15 GDPR;
- rectification and erasure of your data as set forth in art. 16 GDPR;
- restriction of processing of your data as set forth in art. 18 GDPR;
- object to processing data as set forth in art. 21 GDPR;
- data portability as set forth in art. 20 GDPR; and
- lodge a complaint with a supervisory authority.

VIII. Cookie Policy

We use cookies, pixels, and other similar technologies (collectively, "**cookies**") to recognize your browser or device, learn more about your interests, provide you with essential features and services, and for additional purposes, including:

- Monitoring and load-balancing of the application
- Preventing fraudulent activity
- Improving security
- Conducting research and diagnostics to improve our offerings
- Reporting: this allows us to measure and analyze the performance of our offerings.

If you block or otherwise reject our cookies, you will not be able to use the Application.

Approved third parties may also set cookies when you interact with our offerings. Third parties include providers of measurement and analytics services, and security companies.

You can manage browser cookies through your browser settings. The 'Help' feature on most browsers will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie, how to disable cookies, and when cookies will expire. If you disable all cookies on your browser, neither we nor third parties will transfer cookies to your browser. If you do this, however, you may have to manually adjust some preferences every time you visit a site and some features and services may not work.

IX. California Disclosures and Policies

This Section VIII is adopted to comply with the California Consumer Privacy Act of 2018 ("**CCPA**"). Any terms defined in the CCPA have the same meaning when used in this section.

Our App collects information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device ("**personal information**"). In particular, our App has collected the following categories of personal information from its consumers within the last twelve (12) months:

Category	**Examples**	**Collected**

A. Identifiers.	A real name, alias, unique personal identifier, online identifier, Internet Protocol address, email address, account name or other similar identifiers.	YES
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, telephone number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	YES
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	NO
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	YES
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	NO
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	YES
G. Geolocation data.	Physical location or movements.	YES
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	YES
I. Professional or employment-related information.	Current or past job history or performance evaluations.	NO
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	NO

K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	NO

Personal information does not include:

- Publicly available information from government records.
- Deidentified or aggregated consumer information.
- Information excluded from the CCPA's scope.

We obtain the categories of personal information listed above from the following categories of sources:

- Directly from you. For example, from forms you complete or products and services you use.
- Indirectly from you. For example, from observing your actions on the App.

Use of Personal Information

We may use or disclose the personal information we collect for one or more of the following purposes:

- To fulfill or meet the reason you provided the information. For example, if you share your name and contact information to ask a question about our products or services, we will use that personal information to respond to your inquiry.
- To provide, support, personalize, and develop our App, products, and services.
- To create, maintain, customize, and secure your account with us.
- To process your requests, purchases, transactions, and payments and prevent transactional fraud.
- To provide you with support and to respond to your inquiries, including to investigate and address your concerns and monitor and improve our responses.
- To personalize your App experience and to deliver content and product and service offerings relevant to your interests, including targeted offers and ads through our App, third-party sites, and via email or text message (with your consent, where required by law).
- To help maintain the safety, security, and integrity of our App, products and services, databases and other technology assets, and business.
- For testing, research, analysis, and product development, including to develop and improve our App, products, and services.

- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- As described to you when collecting your personal information or as otherwise set forth in the CCPA.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of the Company's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by the Company about our App users is among the assets transferred.

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Sharing Personal Information

We may disclose your personal information to a third party for a business purpose. When we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract. We share your personal information with the following categories of third parties: service providers.

Disclosures of Personal Information for a Business Purpose

In the preceding twelve (12) months, Company has disclosed the following categories of personal information for a business purpose:

Category A: Identifiers.

We store Studio Account email address and password with Auth0.com on a continuous basis to provide authentication services.

We store Studio Account billing Name, Address, Credit Card Number, Country, Postal Code and CVC with Stripe.com on a continuous basis to provide invoicing and credit card processing services.

User Account Information (see above) is disclosed to BlockV on a continuous basis to provide authentication and authorization services.

Category B: California Customer Records personal information categories.

Category D: Commercial information.

Category F: Internet or other similar network activity.

Category G: Geolocation data.

Category H: Sensory data.

We disclose your personal information for a business purpose to the following categories of third parties: service providers.

Your Rights and Choices

The CCPA provides consumers (California residents) with specific rights regarding their personal information. This section describes your CCPA rights and explains how to exercise those rights.

Access to Specific Information and Data Portability Rights

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request (see Exercising Access, Data Portability, and Deletion Rights), we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting or selling that personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you (also called a data portability request).
- If we sold or disclosed your personal information for a business purpose, two separate lists disclosing:
    - sales, identifying the personal information categories that each category of recipient purchased; and
    - disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.

Deletion Request Rights

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request (see Exercising Access, Data Portability, and Deletion Rights), we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

1. Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.

3. Debug products to identify and repair errors that impair existing intended functionality.

4. Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.

5. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 *et. seq.*).

6. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.

7. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.

8. Comply with a legal obligation.

9. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

Exercising Access, Data Portability, and Deletion Rights

To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request to info@vatominc.com.

Only you, or someone legally authorized to act on your behalf, may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.

- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you.

Making a verifiable consumer request does not require you to create an account with us. However, we do consider requests made through your password protected account sufficiently verified when the request relates to personal information associated with that specific account.

We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Response Timing and Format

We endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing.

If you have an account with us, we will deliver our written response to that account. If you do not have an account with us, we will deliver our written response electronically.

Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

X. Changes

We reserve our right to change or adapt this Privacy Policy at any time in compliance with the applicable data protection regulations. We will tell you about any changes by posting an updated Privacy Policy on our website. Any change we make applies from the date we post it on the website. If you have any questions about our Privacy Policy, please email us at info@vtom-inc.com.

This Privacy Policy was updated on [04/24/2020]