



ZBD PRIVACY POLICY v1.1

Last updated: July 17th, 2025

This Privacy Policy is designed to help you understand how ZEBEDEE, LLC and ZEBEDEE EUROPE B.V. (“**ZBD**,” “**we**,” “**us**,” or “**our**”) collects, uses, processes, and shares your personal information, and to help you understand and exercise your privacy rights.

Depending on your location, the ZBD Services will be delivered to you by one of the following ZBD entities which will also be responsible for processing your personal data and act as a controller:

1. If you are located in the Netherlands, the ZBD contracting party is ZEBEDEE EUROPE B.V. (“**ZBD EU**”), a limited liability company incorporated under the laws of the Netherlands, having its registered office Vijzelstraat 68, 1017 HL Amsterdam, 1017 HL, the Netherlands, registered with the Commercial Register under registration number 90944127. ZBD EU is authorized by the Dutch Authority for the Financial Markets (“AFM”) and operates as a licensed crypto asset service provider (“CASP”) under the Markets in Crypto Assets Regulation (“MiCAR”), and Stichting Customer Assets ZEBEDEE, having its registered office Vijzelstraat 68, 1017 HL Amsterdam, 1017 HL, the Netherlands, registered with the Commercial Register under registration number 91032474. ZBD EU is authorized as a CASP engaged in exchange services between virtual currencies and fiat currencies, custodial wallet provider and to provide transfer services of crypto-asset on behalf of its customers from one distributed ledger wallet to another. Stichting Customer Assets ZEBEDEE is a party exclusively for the purpose of asset segregation and the custody of the customer assets and funds as included hereunder. This Privacy Policy also applies to the processing of personal data by Stichting Customer Assets ZEBEDEE as controller (as further explained in paragraph 7).
2. If you are located outside of the Netherlands, the ZBD contracting party is ZEBEDEE, LLC, a Delaware corporation with offices at 50 Harrison ST STE 472, Hoboken, NJ, 07030-6064 (“**ZBD US**”).

If you need to access this Policy in an alternative format due to having a disability, please contact support@zbdpay.com.

If you are a resident of the United States and have a ZBD consumer account or begin the process of creating a ZBD consumer account, please review our U.S. Consumer Financial Privacy Notice for a summary of our practices with respect to nonpublic personal information we collect about you.

Table of Contents

1. SCOPE AND UPDATES TO THIS PRIVACY POLICY
2. PERSONAL INFORMATION WE COLLECT
3. HOW WE USE YOUR PERSONAL INFORMATION
4. HOW WE DISCLOSE YOUR PERSONAL INFORMATION
5. YOUR PRIVACY CHOICES AND RIGHTS
6. INTERNATIONAL TRANSFERS OF PERSONAL INFORMATION
7. RETENTION OF PERSONAL INFORMATION
8. SUPPLEMENTAL NOTICE FOR NEVADA RESIDENTS
9. CHILDREN’S INFORMATION



10. OTHER PROVISIONS, INCLUDING FOR EU/UK CITIZENS

11. COMPLAINTS

12. CONTACT US

i.

1. SCOPE AND UPDATES TO THIS PRIVACY POLICY

This Privacy Policy applies to personal information processed by us, including on our website <https://zbd.gg> ("Site"), mobile application ("App"), ZBD Developer Dashboard ("ZBD Dashboard") and other online or offline offerings. To make this Privacy Policy easier to read, our websites, mobile applications, and other offerings are collectively called the "ZBD Services".

An Important Note Regarding Blockchain Technologies: If you use our Services relating to the creation, management, participation, or operation of a decentralized autonomous organization ("DAO") or with payment channels that may be used on a blockchain protocol network, smart contracts will be employed that necessarily collect information, such as your digital wallet address (which some legal jurisdictions may consider personal information), and that information will be stored on a public blockchain that we do not control. A smart contract is a computer code that automatically processes events when certain conditions are met; for example, when a transaction is conducted between two individuals where each sign off to close a payment channel (in other words, settle the accounts between individuals to be then broadcast to the blockchain), a smart contract would automatically execute the proposed action. In these situations, your personal information will be stored on that blockchain through the execution of a smart contract and may not be able to be modified or deleted due to the immutable nature of the blockchain.

Changes to our Privacy Policy. We may revise this Privacy Policy from time to time at our sole discretion. If there are any material changes to this Privacy Policy, we will notify you as required by applicable law by posting the updated Privacy Policy on the Site, to the App, the ZBD Dashboard and/or may also send other communications. You will need to accept the changes to the Privacy Policy when you next log in the ZBD App or ZBD Dashboard. It is important that you review the Privacy Policy whenever we update it or you use the ZBD Services. If you continue to use the ZBD Services after we have posted updated Privacy Policy, it means that you accept and agree to the changes.

2. PERSONAL INFORMATION WE COLLECT

The categories of personal information we collect depend on how you interact with us, our Services, and the requirements of applicable law. We collect information that you provide to us, information we obtain automatically when you use our Services, and information from other sources such as third-party services and organizations, as described below.

A. Personal Information You Provide to Us Directly. We may collect personal information that you provide to us.

- i. **Account Creation.** We may collect personal information when you create an account, such as name, email address, username, password, profile picture, etc. During the account creation, you will have the ability to create a Gamertag, which is an online handle/identifier for use with our Services that you may personalize to your own preferences and can change at any time. Under some jurisdictions, this Gamertag may be considered personal information that could identify you over the internet, and you should know that people may be able to identify with you this Gamertag.



- ii. **Identity and Residence Verification.** We may collect personal information and details to verify your identity or place of residence. This may include your name, address, documents/images such as your utility bill or comparable residential information, and images of your government-issued ID (e.g., passport, national ID card, or driver's license). We may ask for access to your mobile device's camera to have you take a selfie for identification purposes. We use third-party services with whom we have a written contract to ensure the security of your personal information to verify your identification using your government-issued identification and other information or images you may provide through the Services.
- iii. We may also use your mobile device's native biometrics applications (such as facial or fingerprint recognition) for user identification to create an account. In those instances, we do not have access to this biometrics information, nor do we receive it from your mobile device's developer (such as Apple or Google.) Please contact your mobile device's operating system developer for more information about their biometrics practices.
- iv. **Online Transactions.** We may collect personal information and details associated with your online bitcoin transactions, including crypto wallet addresses or bitcoin transactional information associated with your use of the ZBD Services. Any fiat payments or transactions made via the ZBD Services are processed by third-party processors. We may store the details of the information associated with your online bitcoin transactions and can process bitcoin transactions to other user's ZBD crypto currency wallets or third party provided cryptocurrency wallets.
- v. **Financial information.** Bank account information, transaction history, source of funds, source of wealth and / or tax identification number.
- vi. **Your Communications with Us.** We may collect personal information, such as email address, phone number, or mailing address when you request information about the ZBD Services, register for our newsletter, request customer or technical support, or otherwise communicate with us.
- vii. **Surveys.** We may contact you to participate in surveys. If you decide to participate, we may collect personal information from you in connection with the survey.
- viii. **Interactive Features.** We and others who use our Services may collect personal information that you submit or make available through our interactive features (e.g., messaging and chat features, commenting functionalities, forums, blogs, and social media pages). Any information you provide using the public sharing features of the Services will be considered "public," unless otherwise required by applicable law, and is not subject to the privacy protections referenced herein. Please exercise caution before revealing any information that may identify you in the real world to other users.
- ix. **Sweepstakes or Contests.** We may collect personal information you provide for any sweepstakes or contests that we offer. In some jurisdictions, we are required to publicly share information of sweepstakes and contest winners.
- x. **Conferences, Trade Shows, and Other Events.** We may collect personal information from individuals when we attend or host conferences, trade shows, and other events.
- xi. **Business Development and Strategic Partnerships.** We may collect personal information from individuals and third parties to assess and pursue potential business opportunities.



- xii. **Job Applications.** We may post job openings and opportunities on our Services. If you respond to one of these postings, we may collect your personal information, such as your application, CV, cover letter, and/or any other information you provide to us.

B. Personal Information Collected Automatically. We may collect personal information automatically when you use our Services.

- i. **Automatic Collection of Personal Information.** We may collect certain information automatically when you use our Services, such as your Internet protocol (IP) address, user settings, MAC address, cookie identifiers, mobile carrier, mobile advertising and other unique identifiers, browser or device information, location information (including approximate location derived from IP address), and Internet service provider. We may also automatically collect information regarding your use of our Services, such as pages that you visit before, during and after using our Services, information about the links you click, the types of content you interact with, the frequency and duration of your activities, and other information about how you use our Services.
- ii. **Cookie Policy (and Other Technologies).** We, as well as third parties that provide content, advertising, or other functionality on our Services, may use cookies, pixel tags, and other technologies (“Technologies”) to automatically collect information through your use of our Services.
 - a. **Cookies.** Cookies are small text files placed in device browsers that store preferences and facilitate and enhance your experience.
 - b. **Pixel Tags/Web Beacons.** A pixel tag (also known as a web beacon) is a piece of code embedded in our Services that collects information about engagement on our Services. The use of a pixel tag allows us to record, for example, that a user has visited a particular web page or clicked on a particular advertisement. We may also include web beacons in e-mails to understand whether messages have been opened, acted on, or forwarded.

C. Technology Use. Our uses of these Technologies fall into the following general categories:

- i. **Operationally Necessary.** This includes Technologies that allow you access to our Services, applications, and tools that are required to identify irregular website behavior, prevent fraudulent activity, improve security, or allow you to make use of our functionality;
- ii. **Performance-Related.** We may use Technologies to assess the performance of our Services, including as part of our analytic practices to help us understand how individuals use our Services (see Analytics below);
- iii. **Functionality-Related.** We may use Technologies that allow us to offer you enhanced functionality when accessing or using our Services. This may include identifying you when you sign into our Services or keeping track of your specified preferences, interests, or past items viewed;
- iv. **Advertising- or Targeting-Related.** We may use first party or third-party Technologies to deliver content, including ads relevant to your interests, on our Services or on third-party digital properties. See “5) Your Privacy Choices and Rights” below to understand your choices regarding these Technologies.



- v. **Analytics.** We may use Technologies and other third-party tools to process analytics information on our Services. These Technologies allow us to better understand how our digital Services are used and to continually improve and personalize our Services. Some of our analytics partners include the following non-exclusive list:
 - a. Google Analytics. For more information about how Google uses your personal information (including for its own purposes, e.g., for profiling or linking it to other data), please visit [Google Analytics' Privacy Policy](#). To learn more about how to opt-out of Google Analytics' use of your information, please [click here](#).
 - b. Playtime (adjoe) is a third-party feature that is integrated with our app. Playtime allows users to earn in-app currency by playing third-party games and collects devices' application usage from users. The processing of the data is necessary to recommend, via system messages, the installation of the app available in Playtime that matches users' interests and calculates the bonuses acquired as a result of users' use of the corresponding apps. For more information, please refer to Playtime (adjoe) [Data Privacy Statement](#).

D. Personal Information Collected from Other Sources

- i. **Third-Party Services and Sources.** We may obtain personal information about you from other sources, including through third-party services and organizations. For example, if you access our Services through a third-party application, such as an app store, a third-party login service, or a social networking site, we may collect personal information about you from that third-party application that you have made available via your privacy settings.
- ii. **Credit Bureaus and ID Verification Partners.** We may obtain personal information about you from credit bureaus and identity verification partners.
- iii. **Blockchain Information.** We may obtain personal information about you through our analysis of blockchain information.
- iv. **Referrals and Sharing Features.** Our Services may offer various tools and functionalities that allow you to provide personal information about your friends through our referral service. Our referral services may also allow you to forward or share certain content with a friend or colleague, such as an email inviting your friend to use our Services. Please only share with us contact information of people with whom you have a relationship (e.g., relative, friend, neighbor, or co-worker).
- v. **Public Databases:** We may obtain information from public databases such as the relevant Chamber of Commerce, the UBO / Beneficial Owners / Transparency (or similar) register, Google searches and other (reliable and independent) sources. We may also receive such public information via third party service providers.

E. Information generated by us

- i. **Risk and fraud related information:** risk profiles, risk categories, transaction profile information, transaction patterns information, behavioral pattern information and internal unusual or suspicious transaction reports or intelligence, derived from information about the transactions you make on the ZBD Services - such as the type of transaction (e.g. buy transaction and/or sell transaction), the amount, the type of virtual currency, the counterparty – and other personal data we have of you, such as related to Politically Exposed Persons (PEPs) and sanction lists – and/or notices to designated authorities including reports/notifications to FIU.



ii. Fraud and whistleblowing reports: We may receive your personal data if they have been necessarily included in whistleblowing reports from ZBD employees or in fraud reports from relevant payment institutions and payments service providers, law enforcement agencies and the Financial Intelligence Units (FIU). We may draw conclusions from such personal data regarding your risk classification and include such conclusions in our systems and records.

3. HOW WE USE YOUR PERSONAL INFORMATION

We use your personal information for a variety of business purposes, including to provide the ZBD Services, for administrative purposes, and to market our products and Services, as described below.

A. Comply with laws and regulations. Most of the ZBD Services are subject to laws and regulations requiring us to collect, use, and store your personal data in certain ways. For example, ZBD must identify and verify customers using the ZBD Services in order to comply with anti-money laundering laws. In order to verify your identity remotely, we match your photo with your identification.

B. Provide Our Services. We use your information to fulfill our contract with you and provide you with our Services, such as:

- i. Managing your information and accounts;
- ii. Verify your identity in accordance with applicable know-your-customer, money-laundering and other financial sector legislation or regulations;
- iii. Providing access to certain areas, functionalities, and features of our Services;
- iv. Answering requests for customer or technical support;
- v. Communicating with you about your account, activities on our Services, and policy changes;
- vi. Processing your financial information and other payment methods for products or Services purchased or used;
- vii. Processing applications if you apply for a job we post on our Services; and
- viii. Allowing you to register for events.

C. Administrative Purposes. We use your information for various administrative purposes, such as:

- i. Pursuing our legitimate business interests such as direct marketing, research and development (including marketing research), network and information security, and fraud prevention;
- ii. Detecting security incidents, protecting against malicious, deceptive, fraudulent or illegal activity, and prosecuting those responsible for that activity;
- iii. Measuring interest and engagement in our Services;
- iv. Improving, upgrading, or enhancing our Services;
- v. Developing new products and services;
- vi. Ensuring internal quality control and safety;



- vii. Authenticating and verifying individual identities, including requests to exercise your rights under this Privacy Policy;
- viii. Debugging to identify and repair errors with our Services;
- ix. Auditing relating to interactions, transactions, and other compliance activities;
- x. Sharing personal information with third parties as needed to provide the Services;
- xi. Enforcing our agreements and policies; and
- xii. Carrying out activities that are required to comply with our legal obligations.

D. Marketing and Advertising our Products and Services. We may use personal information to tailor and provide you with content and advertisements. We may provide you with these materials as permitted by applicable law. Some of the ways we market to you include email campaigns, custom audiences advertising, and “interest-based” or “personalized advertising,” including through cross-device tracking. If you have any questions about our marketing practices or if you would like to opt out of the use of your personal information for marketing purposes, you may contact us at any time as set forth in “[Contact Us](#)” below.

E. Other Purposes We also use your personal information for other purposes as requested by you or as permitted by applicable law.

- i. **To prevent fraud, misuse of the ZBD services, or money laundering.** ZBD processes personal data that are not strictly required by law, but nevertheless are necessary to protect the legitimate interest to (i) guarantee the safety and integrity of the financial sector, (ii) to prevent and actively combat (attempts to commit) criminal offenses and (iii) to assist in combating fraud and other types of abuse.
- ii. **With Your Consent.** We may use personal information for other purposes that are clearly disclosed to you at the time you provide personal information or with your consent.
- iii. **Automated Decision Making.** We may engage in automated decision making. For example, we may engage in automated decision making for purposes of fraud prevention. Our processing of your personal information will not result in a decision based solely on automated processing that significantly affects you unless such a decision is necessary as part of a contract we have with you, we have your consent, or we are permitted by law to engage in such automated decision making. If you have questions about our automated decision making, you may contact us as set forth in “[Contact Us](#)” below.
- iv. **De-identified and Aggregated Information.** We may use personal information to create de-identified and/or aggregated information, such as demographic information, information about the device from which you access our Services, or other analyses we create.

4. HOW WE DISCLOSE YOUR PERSONAL INFORMATION

We disclose your personal information to third parties for a variety of business purposes, including to provide the ZBD Services, to protect us or others, or in the event of a major business transaction such as a merger, sale, or asset transfer, as described below. Your personal data may also be shared after requesting and obtaining your (explicit) consent.



ZBD has instructed third parties to process personal data on our behalf if such is necessary for third parties to perform their tasks and duties. Such third parties qualify as Data Processors. ZBD signs appropriate data processing agreements with all Data Processors. Through these data processing agreements, the Data Processors provide at least the same level of security as provided ZBD and guarantee the confidentiality of your personal data. ZBD nevertheless remains fully responsible for these processing operations and will therefore take all reasonable technical and organizational measures to protect your personal data against accidental or unlawful destruction, loss, alteration and unauthorised disclosure or access.

A. Disclosures to Provide our Services The categories of third parties with whom we may share your personal information are described below.

- i. If you are a customer of ZBD EU, Stichting Customer Assets ZEBEDEE (in the Netherlands) functions as a bankruptcy remote vehicle for safeguarding funds and assets of customers of the ZBD Services. For this purpose, your name and bank account number is shared with and processed by Stichting Customer Assets ZEBEDEE.
- ii. **Service Providers.** We may share your personal information with our third-party service providers and vendors that assist us with the provision of our Services. This includes service providers and vendors that provide us with IT support, hosting, payment processing, customer service, and related services.
- iii. **Verification Partners.** We may provide an opportunity through our Services for you to share your personal information, such as your selfie photos or government identification, with our verification partners to verify your identity to use portions of our Services. In these instances, we will notify you when you are going to provide personal information to our Verification Partners for this purpose, and your sharing of this information will be subject to our Verification Partners' Privacy Policies and Terms of Service.
- iv. **Third-Party Services.** Certain features and functionalities of the Services may link to or allow you to interface, interact, or share information with, access and/or use third-party websites, services, products, and technology (collectively, "Third-Party Services"). For example, you may use the Services to interact with Third-Party Services such as financial institutions and cryptocurrency exchanges and vice versa. Any information disclosed to or otherwise collected by a Third-Party Service may be subject to the Third-Party Service's privacy policy. We do not provide or control any aspect of the Third-Party Services and are not responsible for any compatibility issues, errors or bugs in the Services or Third-Party Services caused in whole or in part by the Third-Party Services or any update or upgrade thereto. We encourage our users to read the privacy policies of each Third-Party Service with which they interact. We do not endorse, screen or approve, and are not responsible for such Third-Party Services. Providing information to or interacting with Third-Party Services is at your own risk.
- v. **Business Partners.** We may share your personal information with business partners to provide you with a product or service you have requested. We may also share your personal information with business partners with whom we jointly offer products or services.
- vi. **Affiliates.** We may share your personal information with our company affiliates.
- vii. **Other Users or Third Parties You Share or Interact With.** As described above in "Personal Information We Collect," our Services may allow you to share personal information or interact with other users and third parties (including individuals and third parties who do not use our Services and the general public).



- viii. **Advertising Partners.** We may share your personal information with third-party advertising partners. These third-party advertising partners may set Technologies and other tracking tools on our Services to collect information regarding your activities and your device (e.g., your IP address, cookie identifiers, page(s) visited, location, time of day). These advertising partners may use this information (and similar information collected from other services) for purposes of delivering personalized advertisements to you when you visit digital properties within their networks. This practice is commonly referred to as “interest-based advertising” or “personalized advertising.”
- ix. **APIs/SDKs.** We may use third-party application program interfaces (“APIs”) and software development kits (“SDKs”) as part of the functionality of our Services. For more information about our use of APIs and SDKs, please contact us as set forth in “[Contact Us](#)” below.

B. Disclosures to Protect Us or Others

We may access, preserve, and disclose any information we store associated with you to external parties if we, in good faith, believe doing so is required or appropriate to: comply with law enforcement or national security requests and legal process, such as a court order or subpoena; protect your, our, or others’ rights, property, or safety; enforce our policies or contracts; collect amounts owed to us; or assist with an investigation or prosecution of suspected or actual illegal activity.

C. Competent Authorities and other institutions

- i. ZBD shares your personal data if and to the extent this is required to be able to fulfill applicable (European, Dutch or international) rules and regulations, including assisting Financial Intelligence Units (FIU) or (other) competent supervisory authorities, law enforcement authorities or if necessary to assist in combating fraud and other types of abuse to the extent permitted by law.
- ii. We are legally obliged to include (some of) your personal data in our financial administration, which has to be shared with the national tax authorities. The tax authorities will process these personal data in accordance with its own privacy policies.

D. Disclosure in the Event of Merger, Sale, or Other Asset Transfers

If we are involved in a merger, acquisition, financing due diligence, reorganization, bankruptcy, receivership, purchase or sale of assets, or transition of service to another provider, your information may be sold or transferred as part of such a transaction, as permitted by law and/or contract.

5. YOUR PRIVACY CHOICES AND RIGHTS

A. Your Privacy Choices. The privacy choices you may have about your personal information are determined by applicable law and are described below.

- i. **Email Communications.** If you receive an unwanted email from us, you can use the unsubscribe link found at the bottom of the email to opt out of receiving future emails. Note that you will continue to receive transaction-related emails regarding products or Services you have requested. We may also send you certain non-promotional communications regarding us and our Services, and you will not be able to opt out of those communications (e.g., communications regarding our Services or updates to our Terms or this Privacy Policy).
- ii. **Mobile Devices.** We may send you push notifications through our mobile application. You may opt out from receiving these push notifications by changing the settings on your mobile device.



- iii. **“Do Not Track.”** Do Not Track (“DNT”) is a privacy preference that users can set in certain web browsers. Please note that we do not respond to or honor DNT signals or similar mechanisms transmitted by web browsers.
- iv. **Cookies and Personalized Advertising.** You may stop or restrict the placement of Technologies on your device or remove them by adjusting your preferences as your browser or device permits. However, if you adjust your preferences, our Services may not work properly. Please note that cookie-based opt-outs are not effective on mobile applications. However, you may opt-out of personalized advertisements on some mobile applications by following the instructions for [Android](#), [iOS](#), and [others](#).
 - a. The online advertising industry also provides websites from which you may opt out of receiving targeted ads from data partners and other advertising partners that participate in self-regulatory programs. You can access these and learn more about targeted advertising and consumer choice and privacy by visiting the [Network Advertising Initiative](#), the [Digital Advertising Alliance](#), the [European Digital Advertising Alliance](#), and the [Digital Advertising Alliance of Canada](#). Please note you must separately opt out in each browser and on each device.

B. Your Privacy Rights. In accordance with applicable law, you may have the right to:

- ii. **Confirm Whether We Are Processing Your Personal Information** (the right to know);
- iii. **Access to and Portability of Your Personal Information**, including: (i) obtaining access to or a copy of your personal information; and (ii) receiving an electronic copy of personal information that you have provided to us, or asking us to send that information to another company in a structured, commonly used, and machine readable format (also known as the “right of data portability”);
- iv. **Request Correction** of your personal information where it is inaccurate or incomplete. In some cases, we may provide self-service tools that enable you to update your personal information;
- v. **Request Deletion** of your personal information;
- vi. **Request Restriction of or Object** to our processing of your personal information;
- vii. **Withdraw Your Consent** to our processing of your personal information. Please note that your withdrawal will only take effect for future processing, and will not affect the lawfulness of processing before the withdrawal; and
- viii. **Appeal Our Decision** to decline to process your request.

If you would like to exercise any of these rights, please contact us as set forth in “[Contact Us](#)” below. We will process such requests in accordance with applicable laws.

If applicable laws grant you an appeal right and you would like to appeal our decision with respect to your request, you may do so by informing us of this and providing us with information supporting your appeal.

6. INTERNATIONAL TRANSFERS OF PERSONAL INFORMATION

All information processed by us may be transferred, processed, and stored anywhere in the world, including, but not limited to, the United States or other countries, which may have data protection laws



that are different from the laws where you live. We endeavor to safeguard your personal information consistent with the requirements of applicable laws.

If we transfer personal information which originates in the European Economic Area, Switzerland, and/or the United Kingdom to a country that has not been found to provide an adequate level of protection under applicable data protection laws, one of the safeguards we may use to support such transfer is the [EU Standard Contractual Clauses](#).

For more information about the safeguards we use for international transfers of your personal information, please “[Contact Us](#)” as set forth below.

7. RETENTION OF PERSONAL INFORMATION

We store the personal information we collect as described in this Privacy Policy for as long as you use our Services and up to five years after the account is closed, or as necessary to fulfill the purpose(s) for which it was collected, provide our Services, resolve disputes, establish legal defenses, conduct audits, pursue legitimate business purposes, enforce our agreements, and comply with applicable laws.

To determine the appropriate retention period for personal information, we may consider applicable legal requirements, the amount, nature, and sensitivity of the personal information, certain risk factors, the purposes for which we process your personal information, and whether we can achieve those purposes through other means.

8. SUPPLEMENTAL NOTICE FOR NEVADA RESIDENTS

If you are a resident of Nevada, you have the right to opt-out of the sale of certain personal information to third parties who intend to license or sell that personal information. Please note that we do not currently sell your personal information as sales are defined in Nevada Revised Statutes Chapter 603A. If you have any questions, please contact us as set forth in “[Contact Us](#)” below.

9. CHILDREN’S INFORMATION

The Services are not directed to children under 18 (or other age as required by local law), and we do not knowingly collect personal information from children.

If you are a parent or guardian and believe your child has uploaded personal information to our site without your consent and wish to review information collected from your child or have that information modified or deleted, you may contact us as described in “[Contact Us](#)” below. If we become aware that a child has provided us with personal information in violation of applicable law, we will delete any personal information we have collected, unless we have a legal obligation to keep it, and terminate the child’s account, if applicable.

10. OTHER PROVISIONS, INCLUDING FOR EU/UK CITIZENS

Sensitive Personal Information. We do not generally require you to disclose any sensitive personal information (for example, details of race, religious belief, sexual orientation, or membership of a trade union) to us. If you do provide us with sensitive personal information for any reason, you consent to us collecting that information and then using and disclosing that information for the purpose for which you disclosed it to us.

Third-Party Websites/Applications/Services. The Services may contain links to other websites/applications and other websites/applications may reference or link to our Services or the Services may allow you to interact with Third-Party Services. These third-party services are not



controlled by us. We encourage our users to read the privacy policies of each website and application with which they interact. We do not endorse, screen, or approve, and are not responsible for the third party's actions or omissions, including but not limited to their privacy practices, content of such other websites or applications, and errors or bugs in their software. Providing personal information to third-party websites or applications is at your own risk.

Our Lawful Basis for Processing Personal Information. If your personal information is subject to the EU General Data Protection Regulation or other related legislation, our processing of your personal information is supported by the following lawful bases:

	Lawful Basis: Performance of a Contract (i.e., to Provide Our Services to You)	Lawful Basis: Legitimate Interest	Lawful Basis: Consent	Lawful Basis: For Compliance with Legal Obligations
Comply with laws and regulations		✓		✓
To Provide the Services or Information Requested	✓	✓		✓
To Measure Performance and Carry Out Research	✓	✓		
For Customer Support	✓	✓	✓	✓
For Advertising Purposes		✓	✓	
For Administrative or Legal Purposes	✓	✓		✓

If you provided ZBD your consent for any processing of your personal data, you always have the right to withdraw your consent at any moment by emailing us at: support@zbdpay.com. Please note withdrawal of your consent does not affect the lawfulness of the processing of your personal data before such withdrawal.

11. COMPLAINTS

If you believe that ZBD has processed your personal data unlawfully or if you are not satisfied with ZBD's response to your request, you can send your complaint to support@zbdpay.com. ZBD will respond to your complaint as quickly as possible. You may also directly contact our Data Protection Officer via eu-dpo@zbdpay.com.

Supervisory Authority. If your personal information is subject to the applicable data protection laws of Brazil, the European Economic Area, Switzerland, or the United Kingdom, you have the right to lodge a complaint with the competent supervisory authority if you believe our processing of your personal information violates applicable law.

- [Autoridade Nacional de Proteção de Dados \(ANPD\)](#)



- [EEA Data Protection Authorities \(DPAs\)](#)
- [Swiss Federal Data Protection and Information Commissioner \(FDPIC\)](#)
- [UK Information Commissioner's Office \(ICO\)](#)
- [The Dutch Data Protection Authority \(AP\)](#)

12. CONTACT US

ZBD is the controller of the personal information we process under this Privacy Policy. If you have any questions about our privacy practices or this Privacy Policy, or to exercise your rights as detailed in this Privacy Policy, please contact us at:

ZEBEDEE, LLC
Attn: Compliance Department
50 Harrison St STE 472,
Hoboken, NJ 07030
support@zbdpay.com
+1 888 817 8682

ZEBEDEE EUROPE B.V.
Vijzelstraat 68, 1017 HL
Amsterdam, Netherlands
support@zbdpay.com



ZBD PRIVACY POLICY v1.2

Last updated: December 19th, 2025

This Privacy Policy is designed to help you understand how ZEBEDEE, LLC and ZEBEDEE EUROPE B.V. (collectively “**ZBD**,” “**we**,” “**us**,” or “**our**”) collects, uses, processes, and shares your personal information, and to help you understand and exercise your privacy rights.

Depending on your location, the ZBD Services will be delivered to you by one of the following ZBD entities which will also be responsible for processing your personal data and act as a controller:

1. If you are located in the Netherlands, the ZBD contracting party is ZEBEDEE EUROPE B.V. (“**ZBD EU**”), a limited liability company incorporated under the laws of the Netherlands, having its registered office Vijzelstraat 68, 1017 HL, Amsterdam, the Netherlands, registered with the Commercial Register under registration number 90944127. ZBD EU is authorized by the Dutch Authority for the Financial Markets (“AFM”) and operates as a licensed crypto asset service provider (“CASP”) under the Markets in Crypto Assets Regulation (“MiCAR”), and Stichting Customer Assets ZEBEDEE, having its registered office Vijzelstraat 68, 1017 HL, Amsterdam, the Netherlands, registered with the Commercial Register under registration number 91032474. ZBD EU is authorized as a CASP engaged in exchange services between virtual currencies and fiat currencies, custodial wallet provider and to provide transfer services of crypto-asset on behalf of its customers from one distributed ledger wallet to another. Stichting Customer Assets ZEBEDEE is a party exclusively for the purpose of asset segregation and the custody of the customer assets and funds as included hereunder. This Privacy Policy also applies to the processing of personal data by Stichting Customer Assets ZEBEDEE as controller (as further explained in paragraph 7).
2. If you are located outside of the Netherlands, the ZBD contracting party is ZEBEDEE, LLC, a Delaware corporation with offices at 50 Harrison St STE 472, Hoboken, NJ, 07030-6064 (“**ZBD US**”).

If you need to access this Policy in an alternative format due to having a disability, please contact support@zbdpay.com.

If you are a resident of the United States and have a ZBD consumer account or begin the process of creating a ZBD consumer account, please review our [U.S. Consumer Financial Privacy Notice](#) for a summary of our practices with respect to nonpublic personal information we collect about you.



Table of Contents

- [1. SCOPE AND UPDATES TO THIS PRIVACY POLICY](#)
- [2. PERSONAL INFORMATION WE COLLECT](#)
- [3. INFORMATION GENERATED BY US](#)
- [4. HOW WE USE YOUR PERSONAL INFORMATION](#)
- [5. HOW WE DISCLOSE YOUR PERSONAL INFORMATION](#)
- [6. YOUR PRIVACY CHOICES AND RIGHTS](#)
- [7. INTERNATIONAL TRANSFERS OF PERSONAL INFORMATION](#)
- [8. RETENTION OF PERSONAL INFORMATION](#)
- [9. SUPPLEMENTAL NOTICE FOR NEVADA RESIDENTS](#)
- [10. CHILDREN'S INFORMATION](#)
- [11. OTHER PROVISIONS, INCLUDING FOR EU/UK CITIZENS](#)
- [12. COMPLAINTS](#)
- [13. CONTACT US](#)
- [14. COOKIES AND OTHER TECHNOLOGIES](#)



1. SCOPE AND UPDATES TO THIS PRIVACY POLICY

This Privacy Policy applies to personal information processed by us, including on our website <https://zbd.gg> ("Site"), mobile application ("App"), ZBD Developer Dashboard ("ZBD Dashboard") and other online or offline offerings. To make this Privacy Policy easier to read, our websites, mobile applications, and other offerings are collectively called the "ZBD Services".

An Important Note Regarding Blockchain Technologies: If you use our Services relating to the creation, management, participation, or operation of a decentralized autonomous organization ("DAO") or with payment channels that may be used on a blockchain protocol network, smart contracts will be employed that necessarily collect information, such as your digital wallet address (which some legal jurisdictions may consider personal information), and that information will be stored on a public blockchain that we do not control. A smart contract is a computer code that automatically processes events when certain conditions are met; for example, when a transaction is conducted between two individuals where each sign off to close a payment channel (in other words, settle the accounts between individuals to be then broadcast to the blockchain), a smart contract would automatically execute the proposed action. In these situations, your personal information will be stored on that blockchain through the execution of a smart contract and may not be able to be modified or deleted due to the immutable nature of the blockchain.

Changes to our Privacy Policy. We may revise this Privacy Policy from time to time at our sole discretion. If there are any material changes to this Privacy Policy, we will notify you as required by applicable law by posting the updated Privacy Policy on the Site, to the App, the ZBD Dashboard and/or may also send other communications. You will need to accept the changes to the Privacy Policy when you next log in the ZBD App or ZBD Dashboard. It is important that you review the Privacy Policy whenever we update it or you use the ZBD Services. If you continue to use the ZBD Services after we have posted updated Privacy Policy, it means that you accept and agree to the changes.

2. PERSONAL INFORMATION WE COLLECT

The categories of personal information we collect depend on how you interact with us, our Services, and the requirements of applicable law. We collect information that you provide to us, information we obtain automatically when you use our Services, and information from other sources such as third-party services and organizations, as described below.

A. Personal Information You Provide to Us Directly. We may collect personal information that you provide to us.

We collect information you provide when you:

- Create your account
- Perform customer due diligence (e.g. identity verification checks)
- Perform online bitcoin transactions
- Provide financial information as part of your use of our services
- Reach out to us (e.g. request information about the ZBD Services, register for our marketing promotions, request customer or technical support)
- Register for communications (e.g. newsletter)
- Participate in surveys
- Engage with interactive features (e.g. messaging and chat features, commenting on social media posts)
- Participate in Sweepstakes or Contests



- Participate in ZBD activities or engage with ZBD at Conferences, Trade Shows, and Other Events.
- Share contact and other information in relation to Business Development and Strategic Partnerships
- Apply for a job at ZBD

When provided to us as part of your use of our services or other engagement with us, we will collect the following information about you:

- Name, residential address, date of birth
- Email address, phone number, or mailing address
- Username, gamertag, password, profile picture,
- Documents/images such as your utility bill or comparable residential information
- Images of your government-issued ID (e.g. passport, national ID card, or driver's license)
- Information related to online bitcoin transactions made via the ZBD services, including crypto wallet addresses, lightning network addresses or bitcoin transactional information
- Transaction history, source of funds, source of wealth
- Tax information including your tax residency country and tax identification number
- Job application, CV, cover letter, and/or any other personal information provided as part of a job application (including for a background check)

Please also note that in relation to data collected from you:

- We may ask for access to your mobile device's camera to have you take a selfie for identification purposes.
- We may also use your mobile device's native biometrics applications (such as facial or fingerprint recognition) for user identification to create an account. In those instances, we do not have access to this biometrics information, nor do we receive it from your mobile device's developer (such as Apple or Google.) Please contact your mobile device's operating system developer for more information about their biometrics practices.
- Where you engage with ZBD's interactive features, any information you provide using the public sharing features of the Services will be considered "public," unless otherwise required by applicable law. Public information is not subject to the privacy protections referenced herein. Please exercise caution before revealing any information that may identify you in the real world to other users.
- In some jurisdictions, we are required to publicly share information of sweepstakes and contest winners.

B. Personal Information Collected Automatically. We may collect personal information automatically when you use our Services.



The following personal information will be collected:

- Your Internet protocol (IP) address, user settings, MAC address, cookie identifiers,
- Mobile carrier, mobile advertising and other unique identifiers, browser or device information, Internet service provider
- Location information (including approximate location derived from IP address)
- Information surrounding your use of our Services (e.g. pages that you visit before, during and after using our Services, the links you click, the types of content you interact with, the frequency and duration of your activities)

C. Personal Information Collected from Other Sources

We may collect personal information about you from the following sources:

- **Third-Party Services and Sources.** For example, if you access our Services through a third-party application, such as an app store, a third-party login service, or a social networking site, we may collect personal information about you from that third-party application that you have made available via your privacy settings.
- **Credit Bureaus and ID Verification Partners.**
- **Blockchain Information.**
- **Referrals and Sharing Features.** Our Services may offer various tools and functionalities that allow you to provide personal information about your friends through our referral service. Our referral services may also allow you to forward or share certain content with a friend or colleague, such as an email inviting your friend to use our Services. Please only share with us contact information of people with whom you have a relationship (e.g., relative, friend, neighbor, or co-worker) and have their consent to share their information.
- **Public Databases:** We may obtain information from public databases such as the relevant Chamber of Commerce, the UBO / Beneficial Owners / Transparency (or similar) register, Google searches and other (reliable and independent) sources. Publicly available information is not provided the same protections as personal information unless otherwise required by law.

3. INFORMATION GENERATED BY US

- **Risk and fraud related information:** risk profiles, risk categories, transaction profile information, transaction patterns information, behavioral pattern information and internal unusual or suspicious transaction reports or intelligence, derived from information about the transactions you make on the ZBD Services - such as the type of transaction (e.g. buy transaction and/or sell transaction), the amount, the type of virtual currency, the counterparty – and other personal data we have of you, such as related to Politically Exposed Persons (PEPs) and sanction lists – and/or notices to designated authorities including reports/notifications to FIU.
- **Fraud and whistleblowing reports:** We may receive your personal data if they have been necessarily included in whistleblowing reports from ZBD employees or in fraud reports from relevant payment institutions and payments service providers, law enforcement agencies and the Financial Intelligence Units (FIU). We may draw conclusions from such personal data regarding your risk classification and include such conclusions in our systems and records.



4. OUR LEGAL BASIS FOR HOW WE USE YOUR PERSONAL INFORMATION

We ensure that your personal information is processed lawfully, applying the following principles:

- You have provided consent;
- Processing is necessary for us to perform a contract;
- Processing is necessary for us to comply with a legal obligation; and
- Processing is necessary for the purposes of our legitimate interests, balanced against your interests and fundamental rights and freedoms.

Your data is used for a variety of business purposes, using relevant legal bases as described below.

A. Comply with laws and regulations. Most of the ZBD Services are subject to laws and regulations requiring us to collect, use, and store your personal data in certain ways. For example, ZBD must identify and verify customers using the ZBD Services in order to comply with anti-money laundering laws. In order to verify your identity remotely, we match your photo with your identification. ZBD is also required to report to regulators and authorities and such reporting may contain personal information.

Legal basis: legal obligations

B. Provide Our Services. We use your information to fulfill our contract with you and provide you with our Services, such as:

- i. Managing your information and accounts;
- ii. Verify your identity in accordance with applicable know-your-customer, money-laundering and other financial sector legislation or regulations;
- iii. Providing access to certain areas, functionalities, and features of our Services;
- iv. Answering requests for customer or technical support;
- v. Communicating with you about your account, activities on our Services, and policy changes;
- vi. Processing your financial information and other payment methods for products or Services purchased or used;
- vii. Processing applications if you apply for a job we post on our Services; and
- viii. Allowing you to register for events.

Legal basis: performance of a contract, legal obligations, legitimate interests, your consent.

C. Administrative Purposes. We use your information for various administrative purposes, such as:

- i. Pursuing our legitimate business interests such as direct marketing, research and development (including marketing research), network and information security, and fraud prevention;
- ii. Detecting security incidents, protecting against malicious, deceptive, fraudulent or illegal activity, and prosecuting those responsible for that activity;
- iii. Measuring interest and engagement in our Services;



- iv. Improving, upgrading, or enhancing our Services;
- v. Developing new products and services;
- vi. Ensuring internal quality control and safety;
- vii. Authenticating and verifying individual identities, including requests to exercise your rights under this Privacy Policy;
- viii. Debugging to identify and repair errors with our Services;
- ix. Auditing relating to interactions, transactions, and other compliance activities;
- x. Sharing personal information with third parties as needed to provide the Services;
- xi. Enforcing our agreements and policies; and
- xii. Carrying out activities that are required to comply with our legal obligations.

Legal basis: performance of a contract, legitimate interests, your consent.

D. Marketing and Advertising our Products and Services. We may use personal information to tailor and provide you with content and advertisements. We may provide you with these materials as permitted by applicable law. Some of the ways we market to you include email campaigns, custom audiences advertising, and “interest-based” or “personalized advertising,” including through cross-device tracking. If you have any questions about our marketing practices or if you would like to opt out of the use of your personal information for marketing purposes, you may contact us at any time as set forth in “[Contact Us](#)” below.

Legal basis: legitimate interests, your consent.

E. Other Purposes We also use your personal information for other purposes as requested by you or as permitted by applicable law.

- i. **To prevent fraud, misuse of the ZBD services, or money laundering.** ZBD processes personal data that are not strictly required by law, but nevertheless are necessary to protect the legitimate interest to (i) guarantee the safety and integrity of the financial sector, (ii) to prevent and actively combat (attempts to commit) criminal offenses and (iii) to assist in combating fraud and other types of abuse.
- ii. **Automated Decision Making.** We may engage in automated decision making. For example, we may engage in automated decision making for purposes of fraud prevention. Our processing of your personal information will not result in a decision based solely on automated processing that significantly affects you unless such a decision is necessary as part of a contract we have with you, we have your consent, or we are permitted by law to engage in such automated decision making. If you have questions about our automated decision making, you may contact us as set forth in “[Contact Us](#)” below.
- iii. **De-identified and Aggregated Information.** We may use personal information to create de-identified and/or aggregated information, such as demographic information, information about the device from which you access our Services, or other analyses we create.

Legal basis: legitimate interests, legal obligation, your consent.



5. HOW WE DISCLOSE YOUR PERSONAL INFORMATION

We disclose your personal information to third parties for a variety of business purposes, including to provide the ZBD Services, to protect us or others, or in the event of a major business transaction such as a merger, sale, or asset transfer, as described below. Your personal data may also be shared after requesting and obtaining your (explicit) consent.

ZBD has instructed third parties to process personal data on our behalf if such is necessary for third parties to perform their tasks and duties. Such third parties qualify as Data Processors. ZBD ensures that these third parties are contractually obliged to provide the same level of protection (i.e. security and confidentiality) that ZBD provides you in relation to any data shared, for example by signing appropriate data processing agreements with the Data Processor. ZBD nevertheless remains fully responsible for these processing operations and will therefore take all reasonable technical and organizational measures to protect your personal data against accidental or unlawful destruction, loss, alteration and unauthorised disclosure or access.

A. Disclosures to Provide our Services The categories of third parties with whom we may share your personal information are described below.

- i. If you are a customer of ZBD EU, Stichting Customer Assets ZEBEDEE (in the Netherlands) functions as a bankruptcy remote vehicle for safeguarding funds and assets of customers of the ZBD Services. For this purpose, your name and bank account number is shared with and processed by Stichting Customer Assets ZEBEDEE.
- ii. **Service Providers.** We may share your personal information with our third-party service providers and vendors that assist us with the provision of our Services. This includes service providers and vendors that provide us with IT support, hosting, payment processing, customer service, and related services.
- iii. **Verification Partners.** We may provide an opportunity through our Services for you to share your personal information, such as your selfie photos or government identification, with our verification partners to verify your identity to use portions of our Services. In these instances, we will notify you when you are going to provide personal information to our Verification Partners for this purpose, and your sharing of this information will be subject to our Verification Partners' Privacy Policies and Terms of Service.
- iv. **Third-Party Services.** Certain features and functionalities of the Services may link to or allow you to interface, interact, or share information with, access and/or use third-party websites, services, products, and technology (collectively, "Third-Party Services"). For example, you may use the Services to interact with Third-Party Services such as financial institutions and cryptocurrency exchanges and vice versa. Any information disclosed to or otherwise collected by a Third-Party Service may be subject to the Third-Party Service's privacy policy. We do not provide or control any aspect of the Third-Party Services and are not responsible for any compatibility issues, errors or bugs in the Services or Third-Party Services caused in whole or in part by the Third-Party Services or any update or upgrade thereto. We encourage our users to read the privacy policies of each Third-Party Service with which they interact. We do not endorse, screen or approve, and are not responsible for such Third-Party Services. Providing information to or interacting with Third-Party Services is at your own risk.
- v. **Business Partners.** We may share your personal information with business partners to provide you with a product or service you have requested. We may also share your personal information with business partners with whom we jointly offer products or services.



- vi. **Affiliates.** We may share your personal information with our company affiliates.
- vii. **Other Users or Third Parties You Share or Interact With.** As described above in “Personal Information We Collect,” our Services may allow you to share personal information or interact with other users and third parties (including individuals and third parties who do not use our Services and the general public).
- viii. **Advertising Partners and Analytics Providers.** We may share your personal information with third-party advertising partners. These third-party advertising partners may set Technologies and other tracking tools on our Services to collect information regarding your activities and your device (e.g., your IP address, cookie identifiers, page(s) visited, location, time of day). These advertising partners may use this information (and similar information collected from other services) for purposes of delivering personalized advertisements to you when you visit digital properties within their networks. This practice is commonly referred to as “interest-based advertising” or “personalized advertising.”
- ix. **APIs/SDKs.** We may use third-party application program interfaces (“APIs”) and software development kits (“SDKs”) as part of the functionality of our Services. For more information about our use of APIs and SDKs, please contact us as set forth in [“Contact Us”](#) below.

B. Disclosures to Protect Us or Others

We may access, preserve, and disclose any information we store associated with you to external parties if we, in good faith, believe doing so is required or appropriate to: comply with law enforcement or national security requests and legal process, such as a court order or subpoena; protect your, our, or others’ rights, property, or safety; enforce our policies or contracts; collect amounts owed to us; or assist with an investigation or prosecution of suspected or actual illegal activity.

C. Competent Authorities and other institutions

- i. ZBD shares your personal data if and to the extent this is required to be able to fulfill applicable (European, Dutch or international) rules and regulations, including assisting Financial Intelligence Units (FIU) or (other) competent supervisory authorities, law enforcement authorities or if necessary to assist in combating fraud and other types of abuse to the extent permitted by law.
- ii. We are legally obliged to include (some of) your personal data in our financial administration, which has to be shared with the national tax authorities. The tax authorities will process these personal data in accordance with its own privacy policies.

D. Disclosure in the Event of Merger, Sale, or Other Asset Transfers

If we are involved in a merger, acquisition, financing due diligence, reorganization, bankruptcy, receivership, purchase or sale of assets, or transition of service to another provider, your information may be sold or transferred as part of such a transaction, as permitted by law and/or contract.

6. YOUR PRIVACY CHOICES AND RIGHTS

A. Your Privacy Choices. The privacy choices you may have about your personal information are determined by applicable law and are described below.

- i. **Email Communications.** If you receive an unwanted email from us, you can use the unsubscribe link found at the bottom of the email to opt out of receiving future emails. Note that you will continue to receive transaction-related emails regarding products or Services you have requested.



We may also send you certain non-promotional communications regarding us and our Services, and you will not be able to opt out of those communications (e.g., communications regarding our Services or updates to our Terms or this Privacy Policy).

- ii. **Mobile Devices.** We may send you push notifications through our mobile application. You may opt out of receiving these push notifications by changing the settings on your mobile device.
- iii. **“Do Not Track.”** Do Not Track (“DNT”) is a privacy preference that users can set in certain web browsers. Please note that we do not respond to or honor DNT signals or similar mechanisms transmitted by web browsers.
- iv. **Cookies and Personalized Advertising.** You may stop or restrict the placement of Technologies on your device or remove them by adjusting your preferences as your browser or device permits. However, if you adjust your preferences, our Services may not work properly. Please note that cookie-based opt-outs are not effective on mobile applications. However, you may opt-out of personalized advertisements on some mobile applications by following the instructions for [Android](#), [iOS](#), and [others](#).
 - a. The online advertising industry also provides websites from which you may opt out of receiving targeted ads from data partners and other advertising partners that participate in self-regulatory programs. You can access these and learn more about targeted advertising and consumer choice and privacy by visiting the [Network Advertising Initiative](#), the [Digital Advertising Alliance](#), the [European Digital Advertising Alliance](#), and the [Digital Advertising Alliance of Canada](#). Please note you must separately opt out in each browser and on each device.

B. Your Privacy Rights. In accordance with applicable law, you may have the right to:

- i. **Confirm Whether We Are Processing Your Personal Information** (the right to know);
- ii. **Access to and Portability of Your Personal Information**, including: (i) obtaining access to or a copy of your personal information; and (ii) receiving an electronic copy of personal information that you have provided to us, or asking us to send that information to another company in a structured, commonly used, and machine readable format (also known as the “right of data portability”);
- iii. **Request Correction** of your personal information where it is inaccurate or incomplete. In some cases, we may provide self-service tools that enable you to update your personal information;
- iv. **Request Deletion** of your personal information. Note that if you request deletion of your personal data (for the nature of ZBD EU's services, this means that you need to terminate your account), your data is deleted from production data bases within 30 days and data that ZBD EU is obliged to retain by law is maintained in a secure, deep storage. The data retained in deep storage is automatically deleted after 5 years (unless there is a legal or regulatory reason to retain it for a longer period);
- v. **Request Restriction of or Object** to our processing of your personal information;
Withdraw Your Consent to our processing of your personal information. Please note that your withdrawal will only take effect for future processing, and will not affect the lawfulness of processing before the withdrawal;
- vi. **Request human review of an automated decision** made about you; and



vii. **Appeal Our Decision** to decline to process your request.

If you would like to exercise any of these rights, please contact us as set forth in “[Contact Us](#)” below. We will process such requests in accordance with applicable laws. For some requests, for example where you wish to access personal data held about you, we may need to verify your identity. Note that your ability to exercise these rights will depend on various factors. We may decline your request, for example if there is a legitimate reason for not doing so.

If applicable laws grant you an appeal right and you would like to appeal our decision with respect to your request, you may do so by informing us of this and providing us with information supporting your appeal.

7. INTERNATIONAL TRANSFERS OF PERSONAL INFORMATION

All information processed by us may be transferred, processed, and stored anywhere in the world, including, but not limited to, the United States or other countries, which may have data protection laws that are different from the laws where you live. We endeavor to safeguard your personal information consistent with the requirements of applicable laws.

If we transfer personal information which originates in the European Economic Area, Switzerland, and/or the United Kingdom to a country that has not been found to provide an adequate level of protection under applicable data protection laws, one of the safeguards we may use to support such transfer is the [EU Standard Contractual Clauses](#).

For more information about the safeguards we use for international transfers of your personal information, please “[Contact Us](#)” as set forth below.

8. RETENTION OF PERSONAL INFORMATION

We store the personal information we collect as described in this Privacy Policy for as long as you use our Services and up to five years after the account is closed, or as necessary to fulfill the purpose(s) for which it was collected, provide our Services, resolve disputes, establish legal defenses, conduct audits, pursue legitimate business purposes, enforce our agreements, and comply with applicable laws.

To determine the appropriate retention period for personal information, we may consider applicable legal requirements, the amount, nature, and sensitivity of the personal information, certain risk factors, the purposes for which we process your personal information, and whether we can achieve those purposes through other means.

9. SUPPLEMENTAL NOTICE FOR NEVADA RESIDENTS

If you are a resident of Nevada, you have the right to opt-out of the sale of certain personal information to third parties who intend to license or sell that personal information. Please note that we do not currently sell your personal information as sales are defined in Nevada Revised Statutes Chapter 603A. If you have any questions, please contact us as set forth in “[Contact Us](#)” below.

10. CHILDREN’S INFORMATION

The Services are not directed to children under 18 (or other age as required by local law), and we do not knowingly collect personal information from children.

If you are a parent or guardian and believe your child has uploaded personal information to our site without your consent and wish to review information collected from your child or have that information modified or deleted, you may contact us as described in “[Contact Us](#)” below. If we become aware that a child has provided us with personal information in violation of applicable law, we will delete any personal



information we have collected, unless we have a legal obligation to keep it, and terminate the child's account, if applicable.

11. OTHER PROVISIONS, INCLUDING FOR EU/UK CITIZENS

Sensitive Personal Information. We do not generally require you to disclose any sensitive personal information (for example, details of race, religious belief, sexual orientation, or membership of a trade union) to us. If you do provide us with sensitive personal information for any reason, you consent to us collecting that information and then using and disclosing that information for the purpose for which you disclosed it to us.

Third-Party Websites/Applications/Services. The Services may contain links to other websites/applications and other websites/applications may reference or link to our Services or the Services may allow you to interact with Third-Party Services. These third-party services are not controlled by us. We encourage our users to read the privacy policies of each website and application with which they interact. We do not endorse, screen, or approve, and are not responsible for the third party's actions or omissions, including but not limited to their privacy practices, content of such other websites or applications, and errors or bugs in their software. Providing personal information to third-party websites or applications is at your own risk.

Our Lawful Basis for Processing Personal Information. If your personal information is subject to the EU General Data Protection Regulation or other related legislation, our processing of your personal information is supported by the following lawful bases:

	Lawful Basis: Performance of a Contract (i.e., to Provide Our Services to You)	Lawful Basis: Legitimate Interest	Lawful Basis: Consent	Lawful Basis: For Compliance with Legal Obligations
Comply with laws and regulations		✓		✓
To Provide the Services or Information Requested	✓	✓		✓
To Measure Performance and Carry Out Research	✓	✓		
For Customer Support	✓	✓	✓	✓
For Advertising Purposes		✓	✓	
For Administrative or Legal Purposes	✓	✓		✓

If you provided ZBD your consent for any processing of your personal data, you always have the right to withdraw your consent at any moment by emailing us at: support@zbdpay.com. Please note withdrawal of your consent does not affect the lawfulness of the processing of your personal data before such withdrawal.



12. COMPLAINTS

If you believe that ZBD has processed your personal data unlawfully or if you are not satisfied with ZBD's response to your request, you can send your complaint to support@zbdpay.com. ZBD will respond to your complaint as quickly as possible. ZBD EU Customers may also directly contact our Data Protection Officer via eu-dpo@zbdpay.com.

Supervisory Authority. If your personal information is subject to the applicable data protection laws of Brazil, the European Economic Area, Switzerland, or the United Kingdom, you have the right to lodge a complaint with the competent supervisory authority if you believe our processing of your personal information violates applicable law.

- [Autoridade Nacionalde Proteção de Dados \(ANPD\)](#)
- [EEA Data Protection Authorities \(DPAs\)](#)
- [Swiss Federal Data Protection and Information Commissioner \(FDPIC\)](#)
- [UK Information Commissioner's Office \(ICO\)](#)
- [The Dutch Data Protection Authority \(AP\)](#)

13. CONTACT US

ZBD is the controller of the personal information we process under this Privacy Policy. If you have any questions about our privacy practices or this Privacy Policy, or to exercise your rights as detailed in this Privacy Policy, please contact us at:

ZEBEDEE, LLC
Attn: Compliance Department
50 Harrison St STE 472,
Hoboken, NJ 07030
support@zbdpay.com
+1 888 817 8682

ZEBEDEE EUROPE B.V.
Vijzelstraat 68, 1017 HL
Amsterdam, Netherlands
support@zbdpay.com

14. COOKIES AND OTHER TECHNOLOGIES

We, as well as third parties that provide content, advertising, or other functionality on our Services, may use cookies, pixel tags, and other technologies ("Technologies") to automatically collect information through your use of our Services.

- Cookies.** Cookies are small text files placed in device browsers that store preferences and facilitate and enhance your experience.
- Pixel Tags/Web Beacons.** A pixel tag (also known as a web beacon) is a piece of code embedded in our Services that collects information about engagement on our Services. The use of a pixel tag



allows us to record, for example, that a user has visited a particular web page or clicked on a particular advertisement. We may also include web beacons in e-mails to understand whether messages have been opened, acted on, or forwarded.

c. **Technology Use.** Our uses of these Technologies fall into the following general categories:

- i. **Operationally Necessary.** This includes Technologies that allow you access to our Services, applications, and tools that are required to identify irregular website behavior, prevent fraudulent activity, improve security, or allow you to make use of our functionality;
- ii. **Performance-Related.** We may use Technologies to assess the performance of our Services, including as part of our analytic practices to help us understand how individuals use our Services (see Analytics below);
- iii. **Functionality-Related.** We may use Technologies that allow us to offer you enhanced functionality when accessing or using our Services. This may include identifying you when you sign into our Services or keeping track of your specified preferences, interests, or past items viewed;
- iv. **Advertising- or Targeting-Related.** We may use first party or third-party Technologies to deliver content, including ads relevant to your interests, on our Services or on third-party digital properties. See “5) Your Privacy Choices and Rights” below to understand your choices regarding these Technologies.
- v. **Analytics.** We may use Technologies and other third-party tools to process analytics information on our Services. These Technologies allow us to better understand how our digital Services are used and to continually improve and personalize our Services. Some of our analytics partners include the following non-exclusive list:
 - a. Google Analytics. For more information about how Google uses your personal information (including for its own purposes, e.g., for profiling or linking it to other data), please visit [Google Analytics’ Privacy Policy](#). To learn more about how to opt-out of Google Analytics’ use of your information, please [click here](#).
 - b. Playtime (adjoie) is a third-party feature that is integrated with our app. Playtime allows users to earn in-app currency by playing third-party games and collects devices' application usage from users. The processing of the data is necessary to recommend, via system messages, the installation of the app available in Playtime that matches users' interests and calculates the bonuses acquired as a result of users' use of the corresponding apps. For more information, please refer to Playtime (adjoie) [Data Privacy Statement](#).