Privacy Policy

Bizblocks Inc. ("Company") considers the individual user's personal information very important and makes efforts to protect the personal information that the user provides company to use the company's service (crypto wallet service). Accordingly, the company is in compliance with laws and regulations related to the protection of personal information such as "Act on Promotion of Information and Communication Network Utilization and Information Protection" and "Personal Information Protection Act".

The company makes it easy for users to check the Privacy Policy at any time within service. This Privacy Policy may be changed according to the related legislation and the company's internal policies. If it changes, the revision can be checked through Kaiser PayBanC app.

Article 1 (Personal Information Collection)

The personal information items collected by the company are as follows.

1.Personal information items to join the membership or to use the service

① Membership: Kaiser PayBanC account(email, contact, nickname, other information for KYC authentication), nickname

② Mobile phone number verification: mobile phone number

③ Self-verification: name, mobile phone number, date of birth, gender, resident/foreigner information, using mobile phone company, self-verification information(CI, DI)(In case of self-verification, separate consent procedure is carried out by the verification agency).

④ Advertising/marketing (optional): mobile phone number, email address(Receiving advertising/marketing information can optionally be determined whether you agree or not).

2.Information collected automatically in service

Information can be generated or collected automatically during the course of using the service for the purpose of securing service stability, providing safe services and limiting violations of law and service terms and conditions.

① Service use history, access log, transaction record, IP information, cookies, bad and fraudulent use history, mobile device information(model name, mobile phone company information, OS information, screen size, language and country information, advertisement ID, device identification and etc)

② Illegal and negative access to service and service application and related records, records of attempts to access to service and necessary information to check the safe operating circumstances

3. Additional information collected for the customer consultation

① Common: mobile phone number, Kaiser PayBanC account

② Mobile phone number change: data to verify mobile phone company

4. How to collect the personal information

① Collection through mobile app, email, customer service, phone and etc

② Collection from other service through consent provided by third parties

③ Collection through automatic collecting device

Article 2 (Purpose of personal information processing)

The company processes the user's personal information for the following purposes. Personal information being processed shall not be used for any other purpose than the following and if the purpose of use is changed, the company will implement the necessary measures such as obtaining separate approval in accordance with Article 18 of the Personal Information Protection

Act.

1.Users Information Management

① User identification, user information management and various notices passing

② Develop new service d, provide various service

③User consultation and public complain processing and compensation for customer damage

④Account closing process through non-facing self-verification, personal information change and transfer password initialization and etc

2.Provide service

① Confirm oneself and transfer history of cryptocurrency.

② Overall service management such as cryptocurrency transfer in and out.

③ When interworking with the exchange and other wallets, settlement and reconciliation by transaction.

3.Instruct event information

① Provide various information about event and advertisement.

② Provide new service and customized service.

Article 3 (Retain the personal information and period of using)

The company retains the personal information according to law and proceeds it within the period which the user has assented when collecting the personal information. Respective period of holding and using is as follows.

1. Retention and use period of personal information

Classification	Reason to retain	Period of use
Join membership	Member management Consulting with users Resolve public complaint	When withdrawing
Additional verification	Member withdrawal processing	5 years after withdrawing
Cryptocurrency deposit/withdrawal	· Verification the identity by the use of the service provided by the company · Information management of the withdrawal processing in the case of transferring cryptocurrency · Determination of the transaction relation	5 years after withdrawing

However, if investigation and examination are in progress due to violation of relevant law and regulation, it will be retained and used until the end of investigation and examination.

2. Retain by laws according to the service provided

① In principle, the personal information of the user is destroyed without delay when the purpose of collecting and using information is achieved. However, according to the internal policy to prevent disputes due to fraudulent use of the service, fraudulent use records can be retained for one year.

② The company separately stores, manages and destroys the personal information of members who have not used the service for one year in accordance with the laws and regulation of 'Personal information valid period'. The personal information stored separately shall be stored for four years and destroyed without delay. If law imposes an obligation to keep information for a certain period of time, it will keep the personal information safely during that period.

Classification	Related laws	Period of use
Record on contract or	Law related to consumer	5 years

withdrawal	protection in e-commerce	
Records of consumer complaints or disputes		3 years
Records of display and advertisement		6 months
Records of wrong deposit		5 years
Records of self-verification	Act on Information Network Promotion and Information Protection	6 months
Records of login	Act on Communication Confidentiality Protection	3months

Article 4 (How to exercise the rights and duties of users and legal representatives)

1. Users can exercise their rights their rights to view, correct, delete and request to stop processing of the personal information to the company at any time. However, the exercise of rights such as review, correction, delete, request to stop processing of personal information may be restricted in accordance with the Personal Information Protection Act Article 35 (4), Article 36(1), Article 37(2), etc.

2. The user's right can be exercised through written email or FAX in accordance with Article 41, Paragraph 1 of Enforcement Ordinance of Protection of Personal Information and the company will take action without delay.

3. The exercise of the rights under Paragraph 1 may be done through the legal representative of the user or the authorized person. In this case, the power of attorney according to Form11 of the Annexed Paper of the Enforcement Regulation of the Personal Information Protection must be submitted.

4. When requesting correction or deletion of personal information, if other statute specifies that personal information is the object of collection, it cannot be requested to be deleted.

5. If the user requests to view, correction and stop processing, the company confirms whether the person who has done is the right person or his/her legitimate agent.

Article 5 (Shredding of Personal Information)

1. When personal information becomes unnecessary such as the expiration of the period of personal information holding and the achievement of the purpose of processing, the company destroys the personal information without delay.

2. The way to destroy the personal information is as follows

① Destroy permanently personal information stored in electronic file format so that the record cannot be played

② Shred with shredding machine or burn up the personal information recorded and stored in paper document

Article 6 (Technical and administrative protection measures of personal information)

The company provides the following technical and administrative measures to ensure the safety of personal information so that it is not lost stolen, leaked, altered or damaged while it is processing the user's personal information.

1. Establish an internal management plan

The company established and implements an internal management plan for the safe management of personal information processed by the company.

2. Encryption of the user's personal information

The company stores and manages personal information such as user's password and bank account using a secure password algorithm.

3. Countermeasures against hacking and etc

The company is making efforts to protect personal information of users from being leaked or damaged by hacking or computer viruses. The company is backing up frequently in order to protect personal information damage and use the latest vaccine program to prevent personal

information or data from being leaked or damaged and makes personal information on the network through encrypted communication be transmitted safely.

4. Minimization and training of personal information handlers

The company restricts the personal information handler to the minimum necessary for the performance of its business operation and makes the importance of protecting personal information through administrative measures such as training of personal information handlers be recognized.

Article 7 (Matters concerning the installation, operation and rejection of automatic personal information collection device)

The company stores cookies that store and retrieve the information frequently in order to provide the users with convenience in service. Cookies are a small amount of information that website sends to a customer's computer browser (such as Internet Explorer).

1. Purpose of using cookies

Cookies are used to store setting that users prefer and support much faster web environment and improve the service for convenient use. This makes it easier for users to use the service.

Article 8 (Person in charge of personal information protection and responsible department)

1. The company has designated the related department and the person in charge of personal information in order to protect the personal information of user and to deal with complaint related to personal information as follows.

(Person in charge of personal information)

-Name: KwangSoon Han

-Title: Person in charge of personal information protection

-Phone number: +82-42-825-1370

-Email: cs@bizblocks.io

2. You can contact to the person in charge of personal information protection and the department responsible for the protection of all personal information about public complaints that are generated by the users using the company's services. The company will answer and process to the inquiries of users.

Article 9 (Method of saving the infringement of the rights)

If you need help related to save from damage, consultation about infringement of personal information, you can contact to the following organizations

Personal Information Infringement Reporting Center(run by Korea Internet Promotion Agency)

-Hompage : privacy.kisa.or.kr

-Phone number: 118

Personal Information Dispute Coordinating Committee

-Homepage: www.kopico.go.kr

-Phone number: 1833-6972

Supreme Prosecutor Office Cyber-crime Investigation Unit

-Homepage: www.spo.go.kr

-Phone number: 02-3480-3573

National Police Cyber Security Agency

-Homepage: cyberbureau.police.go.kr

-Phone number: 182

Article 10 (Responsibility for link site)

The company can provide link connected to other outside sites to users. In this case, the company cannot guarantee the usefulness, authenticity and legality of services or materials provided by users from outside sites because the company has no control over external sites and the privacy policy of the linked external sites is independent of the company, so make sure to check the policies of the external sites.

Article 11(Personal information processing policy change)

If the current privacy policy is added, deleted or modified, the information will be notified by 'Notice' at least seven days before the revision. However, if there are significant changes in user's right such as the collection and use of personal information and the provision of personal information to third parties, the company shall notify them at least 30 days in advance.