IDBlock Privacy Policy

Article 1 (General Provisions)

Crosshub Co., Ltd. (hereinafter referred to as the “Company”) operates the decentralized digital identification service, IDBlock, and is committed to actively protecting user information. In compliance with the Personal Information Protection Act and other relevant privacy laws, this Privacy Policy is established to inform users of how their personal information is collected and used. IDBlock's Privacy Policy may change according to relevant laws, guidelines, or internal policies, and any changes will be notified to users as stipulated in relevant laws and the IDBlock Terms of Service.

Article 2 (Purpose of Collecting and Using Personal Information and Collected Information Items)

1. Purpose of Collection and Use

(1) Establishment of service contracts for IDBlock (for identity verification and confirmation of user intent)

(2) Fulfillment of IDBlock services (service history inquiries, processing, and notifications)

(3) Fulfillment of "Adult Verification" services (verification of adult status)

(4) Usage of services provided by the Company and affiliated or partner companies

2. Personal Information Items

(1) Information collected at the time of membership registration

- Passport information (all required fields): passport number, passport name, date of birth, nationality, gender, passport type, issuance and expiration dates, passport status (verification of passport authenticity and visa status), a scanned copy of the physical passport, and user’s photograph from the physical passport

(2) Personal photo (required): facial recognition information

Article 3 (Method and Verification of Personal Information Collection)

1. The Company collects personal information through the following methods:

(1) App, email, etc.

(2) Data collection through log analysis programs

2. Verification of Passport Authenticity and Foreign Residency Information

(1) If the user registers their passport, the passport information is verified for authenticity and foreign residency through the following methods:

- Ministry of Justice’s HiKorea (www.hikorea.go.kr), Ministry of Foreign Affairs (Minwon24) (www.passport.go.kr), and Korea Customs Service’s Tax Refund Network

Article 4 (Retention and Use Period of Personal Information, and Disposal of Personal Information)

1. Retention and Use Period

(1) Personal information will be retained until the purpose of collection is achieved or until one year after membership termination. (If necessary for compliance with legal obligations or

based on prior consent, retention may be extended according to applicable periods.)

(2) Retention and use periods according to relevant laws:

- Records on contracts or withdrawal of subscription: 5 years (in accordance with the Consumer Protection Act in Electronic Commerce)
- Records on consumer complaints or dispute resolution: 3 years (in accordance with the Consumer Protection Act in Electronic Commerce)
- Records on labeling and advertising: 6 months (in accordance with the Consumer Protection Act in Electronic Commerce)

(3) Inactive Accounts: For users inactive for one year, personal information will be promptly deleted or separately stored and managed.

2. Procedure and Method for Disposal of Personal Information

(1) Disposal Procedure: Users' personal information will be deleted immediately after service termination or one year post-membership withdrawal. Users will be notified by email of the disposal date, expired data, and deleted information items, after which the information will be disposed of.

(2) Disposal Method:

- For physical documents: shredding or incineration
- For electronic files: technical methods to prevent recovery or reproduction

Article 5 (Use of Personal Information for Purposes Other Than Its Original Purpose and Provision to Third Parties)

1. The Company provides personal information to third parties only if valid consent has been obtained from the user in accordance with the Personal Information Protection Act, or if required by law. Other than this, personal information is not used for purposes other than those specified nor provided to third parties.

2. Exceptions:

(1) When required by law or necessary to fulfill statutory obligations

(2) When necessary for the performance of public duties as prescribed by law (e.g., upon request by the Ministry of Culture, Sports and Tourism for certification of an excellent product)

(3) When necessary for billing purposes related to the provision of telecommunication services

(4) In cases where other laws specifically require it

3. Right to Refuse Consent

- Users have the right to refuse consent for the provision of personal information to third parties. However, refusal to consent may result in difficulties in reserving services provided by third-party service providers.

Article 6 (Delegation of Personal Information Processing)

1. The Company entrusts tasks related to the processing of personal information as follows:

(1) Service Development and Operation

- Entrusted Party: ButterSoft Co., Ltd., IPXHOP Co., Ltd.

- Task: Development of new services and provision of customized services

(2) KakaoTalk Notifications

- Entrusted Party: Kakao Co., Ltd.

- Task: Provision of KakaoTalk notification services for service alerts and event information

(3) Verification of Passport Information

- Entrusted Parties: Ministry of Justice, Ministry of Foreign Affairs

- Task: Verification of visa status, passport expiration date, real-name verification, and passport authenticity

The Company provides only the minimum necessary personal information for each task and, through contractual agreements, prohibits the entrusted parties from processing personal information for any purposes other than the intended purpose. The Company ensures the safety of personal information through technical and managerial safeguards, restriction on re-delegation, monitoring of entrusted parties, and liability measures, including damages, as stipulated in contracts or other documentation.

Article 7 (Rights of Users and Legal Representatives and How to Exercise Them)

1. Users or legal representatives (for users under the age of 14) may view or correct their registered personal information at any time via the mobile passport verification app. The Company will suspend the use of personal information until corrections are completed. Non-mobile app users may contact the head office for immediate assistance.

2. Users or legal representatives (for users under the age of 14) may withdraw consent for the collection, use, and provision of personal information or terminate membership at any time. Requests for withdrawal (membership termination) can be made through the IDBlock app, and the Company will promptly take the necessary actions.

Article 8 (Measures to Ensure the Security of Personal Information)

1. To ensure the security of personal information, the Company takes the following measures:

(1) Regular Self-Audit: Annual self-audits are conducted to ensure personal information handling security.

(2) Minimization and Training of Personnel Handling Personal Information: Designated personnel handle personal information, with access limited to responsible employees only.

(3) Establishment and Implementation of Internal Management Plans: Internal management plans are developed and implemented to securely process personal information.

(4) Technical Measures Against Hacking: Security programs are installed and updated regularly to prevent leaks and damage from hacking or viruses. Systems are installed in restricted areas and are monitored and blocked technically and physically.

(5) Encryption of Personal Information: Personal information, including passwords, is stored and managed in an encrypted format. Important data is encrypted or protected with file-locking features.

(6) Storage of Access Records and Prevention of Tampering: Records of access to personal information processing systems are stored and managed for at least one year. For systems

handling unique identification or sensitive information for 50,000 or more individuals, access records are maintained for at least two years, with safeguards in place to prevent tampering.

(7) Access Restrictions to Personal Information: Access rights to databases storing personal information are managed, including granting, changing, and deleting access permissions. Unauthorized access from outside is blocked by a firewall system.

(8) Use of Locking Devices for Document Security: Documents or storage media containing personal information are kept in secure locations with locking devices.

(9) Access Control for Physical Storage Locations: Separate physical storage areas are designated for personal information, and access control procedures are implemented and maintained.

Article 9 (Personal Information Protection Officers and Departments)

Personal Information Protection Officer

- Name: Jae-seol Kim
- Position: CEO
- Contact: +82-2-6975-9999

Personal Information Protection Manager

- Name: Jin-woo Lee
- Position: Manager
- Contact: +82-2-6975-9999

Article 10 (Remedies for Infringement of User Rights)

1. Users may seek dispute resolution or counseling regarding personal information infringement through the following institutions:

- Personal Information Dispute Mediation Committee: 1833-6972 (www.kopico.go.kr)
- Personal Information Infringement Report Center: 118 (privacy.kisa.or.kr)
- Supreme Prosecutors' Office Cyber Crime Investigation Division: +82-2-3480-3571 (cybercid@spo.go.kr)
- Cyber Safety Bureau of the National Police Agency: 1566-0112 (cyberbureau.police.go.kr)

Article 11 (Changes to the Privacy Policy)

1. In the event of additions, deletions, or modifications, users will be notified through announcements or similar methods.
2. The Company will not reduce the user rights described in this Privacy Policy without explicit consent from users and will retain previous versions of this Privacy Policy for user review.

Effective Date: November 29, 2024