Privacy Policy

Superblock Co., Ltd. (hereinafter referred to as the "Company") complies with the relevant legal provisions that information service providers must adhere to, including the Personal Information Protection Act, the Act on Promotion of Information and Communications Network Utilization and Information Protection, and the Communication Secrets Protection Act. The Company strives to protect the rights and interests of users by establishing a privacy policy based on applicable laws and regulations concerning the processing of personal information related to the services provided by the Company. This privacy policy applies to the use of services provided by the Company and includes the following contents.

Article 1 (Status of Personal Information Collection and Use)

① The Company processes user's personal information for smooth service provision as follows.

Classification (task name)	purpose of processing	Information to be collected and used	Retention/use period
Membership Registration	• Verification and Authentication of the User's Identity • Delivery of Various Notices and Notifications • Prevention of Unauthorized Membership Registration and Misuse of the Service	Mandatory Information: Email address corresponding to the ID, nickname, email address of the inviter	Until the user withdraws membership. ※ If an investigation or inquiry is being conducted due to a violation of relevant laws, it will be retained until the conclusion of the investigation or inquiry, in accordance with internal regulations or relevant laws.
Information Generated and Collected during Service Usage	• Smooth Operation and Improvement of the Service • Prevention of Unauthorized Use of the Service	Mandatory Information: Country, visit date and time, service usage records, device information (OS, screen size, device type, location information, device identifier, advertising ID), device token	Same as above
Identity Verification (KYC)	• Provision of Identity Verification (KYC) Service	Mandatory Information: Name, CI (Customer Identifier), DI (Device Identifier), mobile phone number, date of birth, gender, telecommunications company, information about domestic/foreign status, and other information required for identity verification (KYC)	Until the user withdraws membership or revokes consent. ※ If an investigation or inquiry is being conducted due to a violation of relevant laws, it will be retained until the conclusion of the investigation or inquiry, in accordance with internal regulations or relevant laws.

② User's personal information is collected during the process of user registration and service usage when the user agrees to the collection of personal information and provides information directly during service usage.

③ The Company processes and retains personal information within the period specified in the related laws or within the period agreed upon by the information subject at the time of collecting personal information. However, in the following cases, personal information is processed and retained until the end of the respective reasons:

1) In case of ongoing investigations or inquiries due to violations of relevant laws, until the end of the investigation or inquiry.
2) In case of the existence of creditor-debtor relationships resulting from website usage, until the settlement of the relevant creditor-debtor relationship.
3) In case of the obligation to retain according to relevant laws, until the end of the specified retention period:

- Communication Secrets Protection Act: Website visit records (3 months).

- Act on Promotion of Information and Communications Network Utilization and Information Protection: Records of personal identification (6 months).

Article 2 (Handling of Personal Information of Children Under 14 Years of Age)

The Company does not collect or use information about individuals under the age of 14 who require the consent of their legal representatives, such as parents or guardians, or individuals of the age for which parental consent is required according to the user's country.

Article 3: Matters Concerning Outsourcing of Personal Information Processing

The Company outsources personal information processing tasks for smooth personal information management and supervises whether the entrusted party processes personal information safely.

Outsourced Parties (Data Processors)	Outsourced Tasks
Google Cloud Platform (Google Inc.)	• Storage and Analysis of Information
Amazon Web Services, Inc.	• Storage of Information
AppsFlyer	• Storage and Analysis of Information

Article 4: Matters Concerning Overseas Transfer of Personal Information

The Company entrusts the personal information of users to overseas cloud services for data analysis and data loss prevention.

Company Name	**Purpose of Transfer**	**Contact**	**Data Transferred to**	**Information Transferred**	**When and How**	**Duration of retention and use**
Google Cloud Platform	Data storage on Google Cloud Storage and data analysis via Google BigQuery	080-822-1422	United States	All collected personal information	Personal information is stored in the Google Cloud Computing environment within minutes after data collection.	Until user withdrawal or termination of the outsourcing contract
Amazon Web Services, Inc	Data storage using Simple Storage Service	02-1544-8667	United States	All collected personal information	Personal information is stored in the Amazon Cloud Computing environment within minutes after data collection.	Until user withdrawal or termination of the outsourcing contract
AppsFlyer	Data storage and data analysis by queries	globalops@appsflyer.com	United States	All collected personal information	Personal information is stored in a cloud computing environment within minutes after data collection.	Until user withdrawal or termination of the outsourcing contract

Article 5: Personal Information Disposal Procedure

① When personal information becomes unnecessary due to the expiration of the retention period or achievement of the processing purpose, the Company promptly disposes of such personal information. However, in cases where there is a specified retention period within the Company's internal policies or relevant laws, the personal information is stored and managed separately for a certain period before disposal.

② Personal information printed on paper is shredded or incinerated, and electronically stored records are deleted using technical methods that prevent reproduction.

Article 6: Measures for Inactive Users

The Company disposes of information of users who have not used the service for one year. However, the personal information of such users can be kept separate from that of other users until the expiration of the retention period specified in other laws.

Article 7: Rights, Obligations, and Exercise Methods of Information Subjects and Legal Representatives

① Information subjects can inquire about or modify personal information, request the withdrawal of consent for collection/use, or request termination of membership.

② The exercise of the above rights can be made through the personal information protection officer by sending an email or other means according to Article 41(1) of the Enforcement Decree of the Personal Information Protection Act.

③ The exercise of rights can also be done through the legal representative or a proxy with delegated authority. In this case, the person making the request must submit a power of attorney according to the format in Annex 11 of the Enforcement Rule of the Personal Information Protection Act.

④ The right to access and request processing suspension of personal information may be limited according to Article 35(4) and Article 37(2) of the Personal Information Protection Act.

⑤ The request for correction and deletion of personal information cannot be made in cases where the relevant personal information is specified as a collection target under other laws.

⑥ The Company confirms whether the requester of access, correction, deletion, or suspension of personal information is the information subject or a legitimate representative.

Article 8: Matters Concerning the Security of Personal Information

The Company establishes and operates the necessary technical, administrative, and physical protection measures for security in accordance with Article 29 of the 「Personal Information Protection Act」, including:

- Technical countermeasures against hacking, etc
  - Installation and regular updates of security programs to prevent personal information leakage and damage caused by hacking, computer viruses, and similar threats.
  - Implementation of systems in restricted access areas with both technical and physical monitoring and blocking measures to prevent unauthorized access from external sources.
  - Monitoring and detection of network traffic to identify attempts of illegal information alteration and other unauthorized activities.
- Preservation and Prevention of Tampering Access Records
  - Retention and management of access records (web logs, summary information, etc.) to the personal information processing system for a minimum of 2 years.
  - Implementation of security features to ensure the integrity and protection of access records against tampering, theft, or loss.
- Access Control to Personal Information
  - Establishment and operation of procedures for granting, modifying, and revoking access permissions to the systems processing personal information.
  - Utilization of intrusion detection systems to control unauthorized access attempts from external sources.

Article 9: Installation, Operation, and Rejection of Automatic Personal Information Collection Devices

① The Company uses "cookies" for the following purposes. A cookie is a small amount of information that the server (http) used to operate the website sends to the user's computer browser or mobile application, and is stored on the user's computer's internal hard disk or mobile device.

1) Purpose of cookie use: To provide convenient service functions

2) Disadvantages of refusing to store cookies: There may be difficulties in using customized services.

3) Installation/Operation and Rejection of Cookies: Depending on the type of browser or app, you can refuse to save cookies in the following ways.

- How to set cookies if you use Google Chrome look
- How to set cookies if you use Microsoft Edge look
- How to set cookies if you use Safari look
- How to set cookies if you use the Safari App look
- How to set cookies if you use Chrome App look
- How to set cookies when using the Naver App: Settings > Browsing History > Delete Cookies
- Android: Settings > Applications > Select Services > Storage > Clear Cache
- iOS: Settings > Privacy > Tracking > Select Disable Service App

② In order to provide users with a better experience, the Company uses a "web log analysis tool" that automatically collects and analyzes behavioral information such as visit records and access methods when accessing the homepage/app. In some cases, the Company outsources web log analysis to a third party, and the information collected in the process may be transferred overseas.

Article 10: Matters Concerning the Personal Information Protection Officer

The Company designates a personal information protection officer who is responsible for the overall management of personal information processing and handles complaints and damage relief related to personal information processing. Please contact the responsible department for quick and sufficient responses to user inquiries.

division	manager	contact
Personal Information Protection Officer	Title/Position: VP Manager Name: Joong-ho Lee	privacy@over.network

Article 11: Methods for Remedying Information Subject's Rights Infringement

① The Company ensures the information subject's right to self-determination regarding personal information and makes efforts to provide counseling and remedies for damages caused by personal information infringements. If necessary, please contact the relevant department for reporting or consultation.

② Information subjects can apply for dispute resolution or consultation related to damages caused by personal information infringement to the Personal Information Dispute Mediation Committee, KISA Privacy Infringement Report Center, and other institutions in order to receive relief from personal information infringement. For other reports or consultations regarding personal information infringements, please contact the following institutions:

- Personal Information Dispute Mediation Committee: 1833-6972 (**www.kopico.go.kr**)
- KISA Privacy Infringement Report Center: 118 (privacy.kisa.or.kr)
- Supreme Prosecutors' Office: 1301 (**www.spo.go.kr**)
- National Police Agency: 182 (ecrm.cyber.go.kr)

③ According to the provisions of Article 35 (right to access personal information), Article 36 (right to correction or deletion of personal information), and Article 37 (right to request suspension of personal information processing) of the Personal

Information Protection Act, those who have suffered infringement of rights or interests due to decisions or actions of public authorities can request administrative adjudication in accordance with the Administrative Adjudication Act.

- Central Administrative Appeals Commission: (without an area code) 110 (**www.simpan.go.kr**)

Supplementary Provisions

This policy will be effective from July 31, 2023.

주식회사 슈퍼블록(이하 "회사")은 개인정보보호법, 정보통신망 이용촉진 및 정보보호에 관한 법률, 통신비밀보호법 등 정보통신서비스제공자가 준수하여야 할 관련 법령상의 규정을 준수하며, 관련 법령에 의거한 개인정보 처리방침을 정하여 이용자의 권익 보호에 최선을 다하고 있습니다. 본 개인정보 처리방침은 회사가 제공하는 서비스 이용에 적용되고 다음과 같은 내용을 담고 있습니다.

제1조 개인정보의 수집 및 이용 현황

① 회사가 원활한 서비스 제공을 위하여 다음과 같이 사용자의 개인정보를 처리합니다.

구분(업무명)	처리 목적	처리 항목	보유 및 이용기간
회원 가입	• 본인 식별·인증 • 각종 고지·통지사항 전달 • 서비스 부정 가입 및 부정 이용 방지	필수 : 아이디에 해당하는 이메일 주소, 닉네임, 추천인 이메일 주소	회원탈퇴시까지 ※ 단, 관계 법령 위반에 따른 수사, 조사 등이 진행중인 경우에는 해당 수사, 조사 종료 시 까지 보관 하며 내부규정 혹은 관련법령에 따라 일정기간 보관됨.
서비스 이용 시 생성되어 수집되는 정보	• 서비스의 원활한 이용 및 개선 • 서비스 부정 이용 방지	필수: 국가, 방문 일시, 서비스 이용기록, 단말기 정보(OS, 화면사이즈, 디바이스 종류, 위치정보, 기기식별값, 광고ID) 디바이스 토큰	상동
본인인증(KYC)	본인인증(KYC) 서비스 제공	필수: 이름, CI, DI, 휴대폰번호, 생년월일, 성별, 통신사, 내/외국인 정보 등 본인인증(KYC)를 위하여 필요한 정보	회원탈퇴시 혹은 동의 철회시 까지 ※ 단, 관계 법령 위반에 따른 수사, 조사 등이 진행중인 경우에는 해당 수사, 조사 종료 시 까지 보관 하며 내부규정 혹은 관련법령에 따라 일정기간 보관됨.

② 사용자가 회원가입 및 서비스 이용 과정에서 이용자가 개인정보 수집에 대해 동의하고 직접 정보를 입력하는 경우, 서비스를 이용하는 과정에서 사용자로부터 수집하는 경우 등을 통하여 사용자의 개인정보가 수집됩니다.

③ 회사는 법령에 따른 개인정보 보유·이용기간 또는 정보주체로부터 개인정보를 수집 시에 동의 받은 개인정보 보유·이용기간 내에서 개인정보를 처리·보유합니다. 다만, 다음의 사유에 해당하는 경우에는 해당 사유 종료시까지 처리·보유합니다.

1) 관계 법령 위반에 따른 수사·조사 등이 진행 중인 경우에는 해당 수사·조사 종료 시까지
2) 홈페이지 이용에 따른 채권·채무관계 잔존 시에는 해당 채권·채무관계 정산 시까지
3) 관련 법령에 따른 의무 보유기간에 해당 시에는 해당 기간 종료 시까지

- 통신비밀보호법 : 웹사이트 방문 기록(3개월)
- 정보통신망법 : 본인확인에 관한 기록(6개월)

제2조 만 14세 미만 아동의 개인정보 처리

회사는 법정대리인의 동의가 필요한 만 14세 미만의 아동이거나, 사용자의 국가에서 부모 등 법정대리인의 동의를 요하는 연령에 해당하는 자에 대한 정보를 수집 및 이용하지 않습니다.

제3조 개인정보 처리의 위탁에 관한 사항

회사는 원활한 개인정보 업무처리를 위하여 다음과 같이 개인정보 처리업무를 위탁하며, 수탁자가 개인정보를 안전하게 처리하는지를 관리·감독합니다.

위탁받는 자(수탁자)	위탁업무
Google Cloud Platform (Google Inc.)	정보 보관 및 분석
Amazon Web Services, Inc.	정보 보관
AppsFlyer	정보 보관 및 분석

제4조 개인정보의 국외 이전에 관한 사항

회사는 데이터 분석과 데이터 유실에 대비한 분산 저장을 위해 사용자의 개인정보를 해외 클라우드 서비스에 위탁하고 있습니다.

회사명	이전 목적	연락처	개인정보 이전국가	이전되는 항목	이전 일시 및 방법	보유 및 이용기간
Google Cloud Platform	Google Cloud Storage에 데이터 저장 및 Google BigQuery를 통한 데이터 분석	080-822-1422	미국	수집하는 모든 개인정보	데이터 수집 후 수분 이내 Google 클라우드 컴퓨팅 환경에 개인정보 보관	회원탈퇴 또는 위탁계약 종료시
Amazon Web Services, Inc	Simple Storage Service를 이용한 데이터 저장	02-1544-8667	미국	수집하는 모든 개인정보	데이터 수집 후 수분 이내 Amazon 클라우드 컴퓨팅 환경에 개인정보 보관	회원탈퇴 또는 위탁계약 종료시
AppsFlyer	데이터 저장 및 Query를 통한 데이터 분석	globalops@appsflyer.com	미국	수집하는 모든 개인정보	데이터 수집 후 수분 이내 AppsFlyer 클라우드 컴퓨팅 환경에 개인정보 보관	회원탈퇴 또는 위탁계약 종료시

제5조 개인정보의 파기 절차

① 회사는 개인정보 보유기간의 경과, 처리 목적 달성 등 개인정보가 불필요하게 되었을 때에는 지체 없이 해당 개인정보를 파기합니다. 다만, 회사 내부 방침 또는 관계 법령에서 정한 보관기간이 있을 경우 일정 기간동안 보관 후 파기 됩니다.

② 종이에 출력된 개인정보는 분쇄기로 분쇄하거나 소각하여 파기하고, 전자적 파일 형태로 저장된 기록은 재생할 수 없는 기술적 방법을 사용하여 삭제합니다.

제6조 장기 미사용자에 대한 조치

① 회사는 1년간 서비스를 이용하지 않은 사용자의 정보를 파기하고 있습니다. 다만, 다른 법령에서 정한 보존기간이 경과할 때까지 다른 이용자의 개인정보와 분리하여 별도로 저장·관리할 수 있습니다.

제7조 정보주체와 법정대리인의 권리·의무 및 행사방법

① 정보주체는 언제든지 개인정보를 조회하거나 수정할 수 있고 수집/이용에 대한 동의 철회 또는 가입 해지를 요청 할 수 있습니다.

② 위 권리 행사는 「개인정보 보호법」 시행령 제41조 제1항에 따라 개인정보보호책임자의 전자우편 등을 통하여 하실 수 있습니다.

③ 권리 행사는 정보주체의 법정대리인이나 위임을 받은 자 등 대리인을 통하여 하실 수도 있습니다. 이 경우 "개인정보 처리 방법에 관한 고시" 별지 제11호 서식에 따른 위임장을 제출하셔야 합니다.

④ 개인정보 열람 및 처리정지 요구는 「개인정보 보호법」 제35조 제4항, 제37조 제2항에 의하여 정보주체의 권리가 제한될 수 있습니다.

⑤ 개인정보의 정정 및 삭제 요구는 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없습니다.

⑥ 회사는 정보주체 권리에 따른 열람의 요구, 정정·삭제의 요구, 처리 정지의 요구 시 열람 등 요구를 한 자가 본인이거나 정당한 대리인인지를 확인합니다.

제8조 개인정보의 안전성 확보조치에 관한 사항

회사는 「개인정보 보호법」 제29조에 따라 다음과 같이 안전성 확보에 필요한 기술적, 관리적, 물리적 보호대책 등을 수립하여 운영합니다.

- 해킹 등에 대비한 기술적 대책
  - 해킹이나 컴퓨터 바이러스 등에 의한 개인정보 유출 및 훼손을 막기 위하여 보안프로그램을 설치하고 주기적인 갱신·점검
  - 외부로부터 접근이 통제된 구역에 시스템을 설치하고 기술적/물리적으로 감시 및 차단
  - 네트워크 트래픽의 통제(Monitoring)는 물론 불법적으로 정보를 변경하는 등의 시도를 탐지
- 접속기록의 보관 및 위변조 방지
  - 개인정보처리시스템에 접속한 기록(웹 로그, 요약정보 등)을 최소 2년 이상 보관 및 관리
  - 접속 기록이 위변조 및 도난, 분실되지 않도록 보안기능 사용
- 개인정보에 대한 접근 제한
  - 개인정보를 처리하는 시스템에 대한 접근권한의 부여, 변경, 말소 절차 수립 및 운영
  - 침입탐지시스템을 이용하여 외부로부터의 무단 접근 통제

제9조 개인정보 자동 수집 장치의 설치·운영 및 거부에 관한 사항

① 회사는 아래의 목적으로 "쿠키(cookie)"를 사용합니다. 쿠키는 웹사이트를 운영하는데 이용되는 서버(http)가 이용자의 컴퓨터 브라우저 또는 모바일 어플리케이션에게 보내는 소량의 정보로, 이용자의 컴퓨터 내부 하드디스크 또는 모바일 기기에 저장됩니다.

1) 쿠키의 사용 목적 : 서비스 편의기능 제공

2) 쿠키 저장 거부 시 불이익 : 맞춤형 서비스 이용에 어려움이 있을 수 있습니다.

3) 쿠키의 설치·운영 및 거부 : 브라우저나 앱의 종류에 따라 아래의 방법으로 쿠키의 저장을 거부할 수 있습니다.

- Chrome을 사용하는 경우 쿠키 설정 방법 보기
- Microsoft Edge를 사용하는 경우 쿠키 설정 방법 보기
- Safari를 사용하는 경우 쿠키 설정 방법 보기
- Safari App을 사용하는 경우 쿠키 설정 방법 보기
- Chrome App을 사용하는 경우 쿠키 설정 방법 보기
- Naver App을 사용하는 경우 쿠키 설정 방법: 설정 > 인터넷 사용 기록 > 쿠키 삭제
- Android : 설정 > 애플리케이션 > 서비스 선택 > 저장공간 > 캐시 삭제
- iOS: 설정 > 개인 정보 보호 > 추적 > 서비스 앱 비활성화 선택

② 회사는 이용자에게 더 나은 이용 경험을 제공하기 위하여, 모바일 앱 접속 시 자동으로 방문기록과 접속 수단에 관한 정보 등 행태정보를 수집하여 분석하는 "웹 로그 분석 도구"를 사용합니다. 경우에 따라 회사는 웹 로그 분석 업무를 타사에 위탁하며, 그 과정에서 수집된 정보가 국외로 이전될 수 있습니다.

제10조 개인정보 보호책임자에 관한 사항

회사는 개인정보 처리에 관한 업무를 총괄해서 책임지고, 개인정보 처리와 관련한 정보주체의 불만 처리 및 피해 구제 등을 위하여 아래와 같이 개인정보 보호책임자를 지정하고 있으니, 해당 사항은 담당자에게 연락 주시기 바랍니다. 회사는 사용자 문의에 대하여 신속하고 충분한 답변을 드릴 수 있도록 하겠습니다.

구분	담당자	연락처
개인정보 보호책임자	직책/직위 : VP 담당자 성명 : 이중호	privacy@over.network

제11조 정보주체의 권익침해 구제 방법

① 회사는 정보주체의 개인정보 자기 결정권을 보장하고, 개인정보 침해로 인한 상담 및 피해 구제를 위해 노력하고 있으며, 신고나 상담이 필요한 경우 담당부서로 연락해 주시기 바랍니다.

② 정보주체는 개인정보 침해로 인한 구제를 받기 위하여 개인정보 분쟁조정위원회, 한국인터넷진흥원 개인정보 침해신고센터 등에 분쟁해결이나 상담 등을 신청할 수 있습니다. 이 밖에 기타 개인정보 침해의 신고, 상담에 대하여는 아래의 기관에 문의하시기 바랍니다.

- 개인정보분쟁조정위원회 : (국번없이) 1833-6972 (www.kopico.go.kr)
- 개인정보침해신고센터 : (국번없이) 118 (privacy.kisa.or.kr)
- 대검찰청 : (국번없이) 1301 (www.spo.go.kr)
- 경찰청 : (국번없이) 182 (ecrm.cyber.go.kr)

③ 「개인정보 보호법」 제35조(개인정보의 열람), 제36조(개인정보의 정정·삭제), 제37조(개인정보의 처리정지 등)의 규정에 의한 요구에 대하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 행정심판법이 정하는 바에 따라 행정심판을 청구할 수 있습니다.

- 중앙행정심판위원회 : (국번없이) 110 (www.simpan.go.kr)

부 칙

본 방침은 2023년 7월 31일부터 시행됩니다.