

개인정보처리방침

1. 개인정보 처리 목적 : (주)NADP는 다음의 목적을 위하여 개인정보를 처리하고 있으며 목적 이외의 용도로는 이용하지 않습니다.

- 고객 가입의사 확인, 고객에 대한 서비스 제공에 따른 본인 식별·인증, 회원자격 유지·관리 등

2. 개인정보의 처리 및 보유 기간

① (주)NADP는 정보주체로부터 개인정보를 수집할 때 동의 받은 개인정보 보유·이용 기간 또는 법령에 따른 개인정보 보유·이용 기간 내에서 개인정보를 처리 보유합니다.

② 구체적인 개인정보 처리 및 보유 기간은 다음과 같습니다.

☞ 아래 예시를 참고하여 개인정보 처리업무와 개인정보 처리업무에 대한 보유기간 및 관련 법령, 근거 등을 기재합니다.

(예시) 고객 가입 및 관리 : 서비스 이용계약 또는 회원가입 해지시까지

3. 정보주체와 법정대리인의 권리·의무 및 그 행사방법 이용자는 개인정보주체로서 다음과 같은 권리를 행사할 수 있습니다.

① 정보주체는 (주)NADP에 대해 언제든지 다음 각 호의 개인정보 보호 관련 권리를 행사할 수 있습니다.

(1) 오류 개인정보 열람요구

(2) 오류 등이 있을 경우 정정 요구

(3) 삭제요구

(4) 처리정지 요구

4. 처리하는 개인정보의 항목 작성 : (주)NADP는 다음의 개인정보 항목을 처리하고 있습니다.

① 필수항목 : 휴대전화번호, 이름(닉네임)

② 선택항목 : 해당사항 없음

5. 개인정보의 파기는 원칙적으로 개인정보 처리목적이 달성된 경우에는 지체없이 해당 개인정보를 파기합니다. 파기의 절차, 기한 및 방법은 다음과 같습니다.

① 파기절차 : 이용자가 입력한 정보는 목적 달성 후 별도의 DB로 옮겨지지 않으며 내부 방침 및 기타 관련 법령에 따라 일정기간 혹은 즉시 파기됩니다. 이때, 다른 목적으로 이용하지 않습니다.

② 파기기한 : 이용자의 개인정보는 개인정보의 보유기간이 경과된 경우에는 보유기간의 종료일로부터 7일 이내에, 개인정보의 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 개인정보의 처리가 불필요한 것으로 인정되는 날로부터 7일 이내에 그 개인정보를 파기합니다.

6. 개인정보 자동 수집 장치의 설치·운영 및 거부에 관한 사항 : (주)NADP는 정보주체의 이용정보를 저장하고 수시로 불러오는 '쿠키'를 사용하지 않습니다.

7. 개인정보 보호책임자 작성

① (주)NADP는 개인정보 처리에 관한 업무를 총괄해서 책임지고, 개인정보 처리와 관련한 정보주체의 불만처리 및 피해구제 등을 위하여 아래와 같이 개인정보 보호책임자를 지정하고 있습니다.

▶ 개인정보 보호 책임자 : 담당자 연락처 010-8542-5384, nadpghost@gmail.com

② 정보주체께서는 (주)NADP는 서비스(또는 사업)를 이용하면서 발생한 모든 개인정보 보호 관련 문의, 불만처리, 피해구제 등에 관한 사항을 개인정보 보호 책임자에게 문의하실 수 있습니다. (주)NADP는 정보주체의 문의에 대해 지체 없이 답변 및 처리해드릴 것입니다.

8. 개인정보 처리방침 변경 : 이 개인정보처리방침은 시행일로부터 적용되며, 법령 및 방침에 따른 변경내용의 추가, 삭제 및 정정이 있는 경우에는 변경사항의 시행 7일 전부터 공지사항을 통하여 고지할 것입니다.

9. 개인정보의 안전성 확보 조치는 개인정보보호법 제29조에 따라 다음과 같이 안전성 확보에 필요한 기술적, 관리적 및 물리적 조치를 하고 있습니다.

① 정기적인 자체 감사 실시 : 개인정보 취급 관련 안정성 확보를 위해 정기적(분기 1회)으로 자체 감사를 실시하고 있습니다.

② 개인정보 취급 직원의 최소화 및 교육 : 개인정보를 취급하는 직원을 지정하고 담당자에 한정시켜 최소화하여 개인정보를 관리하는 대책을 시행하고 있습니다.

③ 내부관리계획의 수립 및 시행 : 개인정보의 안전한 처리를 위하여 내부관리 계획을 수립, 시행하고 있습니다.

④ 해킹 등에 대비한 기술적 대책 : (주)NADP의 DP(Data Protection) Messenger는 30년 특허 보안기술 노하우가 적용되어 해킹이나 컴퓨터 바이러스 등에 의한 개인정보 유출을 원천적으로 차단, 해킹이 불가능하도록 설계되어 안전합니다.

⑤ 개인정보의 암호화 : 이용자의 개인정보는 서버 및 엔드포인트까지 자동 암호화 저장되며 (주)NADP 에서도 자료를 복호화 할 수 없습니다.

⑥ 접속기록의 보관 및 위·변조 방지 : 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관, 관리하고 있으며 접속 기록이 위·변조 및 도난, 분실되지 않도록 보안기능을 사용하고 있습니다.

⑦ 개인정보에 대한 접근 제한 : 개인정보를 처리하는 데이터베이스 시스템에 대한 접근권한의 부여, 변경, 말소를 통하여 개인정보에 대한 접근통제를 위하여 필요한 조치를 하고 있으며 침입차단시스템을 이용하여 외부로부터의 무단 접근을 통제하고 있습니다.

⑧ 문서보안을 위한 잠금장치 사용 : 개인정보가 포함된 서류, 보조저장매체 등을 별도로 사용하지 않습니다.

⑨ 비인가자에 대한 출입 통제 : 개인정보를 물리적 보관하는 장소를 별도로 운영하지 않습니다.

Privacy Policy

1. Purpose of processing personal information: NADP Co., Ltd processes personal information for the following purposes and does not use it for purposes other than the purpose.

- Confirmation of the customer's subscription, identification and authentication of the person in accordance with the service provided to the customer, maintenance and management of membership, etc.

2. Period of processing and retention of personal information

(1) NADP Co., Ltd processes and retains personal information within the period of retention and use of personal information agreed to when collecting personal information from the information subject, or the period of retention and use of personal information in accordance with laws and regulations.

(2) The specific personal information processing and retention period is as follows.

☞ the following example, we will list the retention period, related laws, and grounds for the processing of personal information and the processing of personal information.

(e.g.) Customer subscription and management: Until the service use contract or termination of membership

3. Rights and obligations of information owners and legal representatives and how to exercise them Users may exercise the following rights as personal information owners:

- The information subject may exercise the following privacy-related rights for NADP Co., Ltd at any time.

(1) Request to view error personal information

(2) Request correction in the case of errors, etc.

(3) Deletion

(4) Request to be processed

4. Creation of items of personal information to be processed: NADP Co., Ltd handles the following items of personal information:

(1) Required items: mobile phone number, name (nickname)

(2) Optional items: Not available

5. In principle, the destruction of personal information destroys the personal information without delay if the purpose of processing the personal information is achieved. The procedure, deadline and method of destruction are as follows:

(1) Destruction procedure: The information entered by the user will not be transferred to a separate DB after achieving the purpose and will be destroyed for a certain period of time

or immediately in accordance with the internal policy and other relevant laws and regulations. At this time, it will not be used for other purposes.

(2) Destruction period: If the retention period of personal information has elapsed, the user's personal information will be destroyed within 7 days from the end of the retention period, within 7 days from the date on which the processing of personal information is recognized as unnecessary when the personal information becomes unnecessary, such as achieving the purpose of processing the personal information, abolishing the service, or terminating the business.

6. Matters related to the installation, operation and refusal of automatic collection of personal information devices: NADP Co., Ltd does not store information about the use of information subjects and use 'cookies' that are collected from time to time.

7. Create a personal information protection officer

(1) NADP Co., Ltd is responsible for the processing of personal information as a general responsibility and assigns the personal information protection officer as follows to handle complaints and remedy damages of information owners related to the processing of personal information.

► Privacy Officer: Contact +82-10-8542-5384, nadpghost@gmail.com

(2) The information subject may contact the Personal Information Protection Officer regarding all personal information protection inquiries, complaint handling, damage protection, etc. that occurred while using NADP Co., Ltd services (or business). NADP Co., Ltd will respond to and process inquiries from the information subject without delay.

8. Changes to the Personal Information Processing Policy: This Privacy Policy shall apply from the effective date, and if there is any addition, deletion or correction of changes in accordance with laws and policies, the Company will notify the changes through a notice 7 days prior to implementation.

9. Measures to ensure the safety of personal information are taken in accordance with Article 29 of the Personal Information Protection Act, and technical, administrative and physical measures necessary to ensure safety as follows:

(1) Conduct regular self-audits: We conduct our own audits on a regular day (once a quarter) to ensure stability related to the handling of personal information.

(2) Minimization and training of employees handling personal information: We have designated employees who handle personal information and implement measures to manage personal information by minimizing it by limiting it to persons in charge.

(3) Establishment and implementation of internal management plan: We establish and implement internal management plan for safe processing of personal information.

(4) Technical measures against hacking, etc.: NADP Co., Ltd DP(Data Protection) Messenger has been under patent security technology know-how for 30 years, which is designed to prevent and prevent the leak of personal information by hacking or computer viruses, etc., and make it safe to hack.

(5) Encryption of personal information: The user's personal information is automatically encrypted to the server and endpoint, and the data cannot be decrypted even in NADP Co., Ltd.

(6) Storage of access records and prevention of tampering: Records accessed to personal information processing system are stored and managed for at least 6 months, and security functions are used to prevent access records from being altered, stolen, or lost.

(7) Restrictions on access to personal information: We take necessary measures to control access to personal information through granting, changing, and de-addressing access rights to the database system that processes personal information, and we use an intrusion control system to control unauthorized access from outside.

(8) Use of lock for document security: Documents containing personal information, auxiliary storage media, etc. are not used separately.

(9) Access control for unauthorized persons: We do not operate separately where personal information is physically stored.