N E W N A L

뉴날의 데이터 관리 구조

고객의 데이터를 보관하지 않고
개인화 서비스를 만드는 방법

본 문서는 뉴날의 데이터 관리 구조가 어떻게 개인 데이터를 보호하면서 동시에 활용할 수 있게 하는지를 설명합니다.

NEWNAL Inc. · 2026

목차

개요

지금까지의 디지털 서비스는 이용자의 데이터를 회사의 중앙 서버에 모아 두고, 외부 침입을 막는 방식으로 데이터를 보호해 왔습니다. 뉴날은 중앙 서버에 데이터를 모아 두는 방식을 '데이터 요새'라고 부릅니다. 데이터 요새는 외부 침입은 막지만, 열람 권한이 있는 내부 직원과 직원의 계정을 훔친 외부 공격자는 막지 못합니다. 데이터 요새 안의 데이터는 회사만 볼 수 있으므로, 이용자는 자기 데이터가 어떻게 쓰이는지 볼 수 없습니다. 그리고 회사가 데이터를 활용하려면 데이터를 자기 서버로 가져와야 하므로, 활용하는 순간 보관·유출·규제의 책임이 생깁니다.

뉴날은 보호의 방향을 바꾸었습니다. 개인을 식별하는 정보와 민감한 기록은 암호화해서 데이터의 주인인 고객만 자기 기기의 키로 열 수 있게 하고, 데이터가 사용된 기록은 공개 원장에 올려 누구나 확인할 수 있게 합니다. 뉴날은 사용 기록을 공개하는 방식을 '데이터 광장'이라고 부릅니다. 데이터 광장에서는 서비스가 데이터를 가져오지 않고 고객이 허락한 범위를 호출하므로, 회사는 책임 없이 데이터를 활용할 수 있습니다. 뉴날의 데이터 관리 구조는 보호를 위한 구조이면서 동시에 활용을 위한 구조입니다. 클라우드, AI 모델, 운영체제를 대체하지 않고 기존 인프라 위에 놓이는 층입니다(8장).

뉴날의 방식

회사가 고객 데이터를 모으지 않습니다. 고객 데이터는 고객 한 사람마다 하나씩 있는 **개인 데이터 노드**에 저장됩니다. 개인 데이터 노드는 클라우드에서 실행되지만, 노드를 여는 암호화 키는 고객의 기기에만 있습니다. 파트너 기업의 서비스는 고객이 허락한 범위 안에서 노드의 데이터를 호출해 사용합니다. 허락과 접근의 기록은 뉴날 밖의 공개 원장에 남으며, 뉴날도 바꿀 수 없습니다.

> **고객 데이터는 고객의 개인 데이터 노드에 저장됩니다. 파트너 기업의 서비스는 고객이 허락한 범위의 데이터만 사용합니다.**

보안과 활용이 동시에 되는 이유

고객 데이터가 안전한 이유	파트너 기업이 고객 데이터를 활용할 수 있는 이유
모든 고객의 데이터를 모은 데이터베이스가 없습니다. 해킹 한 번으로 얻을 수 있는 것은 한 사람의 데이터뿐이며, 얻은 데이터로도 사람을 식별하거나 연락할 수 없습니다.	데이터는 노드에 그대로 있고, 파트너 기업의 서비스가 허락된 범위를 호출해 사용합니다. 데이터를 옮기지 않으므로 책임이 생기지 않습니다.
노드를 여는 키는 고객의 기기에만 있습니다. 뉴날의 직원도 파트너 기업의 직원도 열 수 없습니다.	고객이 허락하면 노드 안에 파트너 기업의 데이터 영역이 생기고, 파트너 기업은 파트너 기업의 영역에 있는 데이터로 개인화 서비스를 만듭니다.
실명·전화번호 같은 식별 정보는 시스템에 없습니다. 훔친 데이터가 누구의 것인지 알 수 없습니다.	식별·연락·인증은 DID와 고객의 기기가 맡습니다. 로그인·알림·구독 확인은 식별 정보 없이 동작합니다.
모든 접근이 공개 원장에 기록되고 고객에게 통보됩니다.	고객은 기록을 확인하고 파트너 기업에게 데이터를 허락합니다. 보호가 확실할수록 허락하는 범위가 넓어집니다.

파트너 기업에게 달라지는 점

파트너 기업은 고객이 허락한 데이터로 개인화 서비스를 만듭니다. 회원 DB를 만들지 않고 개인정보를 보관하지 않으므로 유출 책임을 지지 않습니다. 브랜드, 판매 수익, 구독 수익, 고객 관계는 파트너 기업이 가집니다.

> **파트너 기업의 기존 시스템은 바꾸지 않습니다.** 뉴날의 데이터 관리 구조는 뉴날 기기를 위한 별도의 구조입니다. 파트너 기업의 기존 회원 데이터베이스, 결제, 고객센터 시스템은 지금 그대로 운영합니다. 같은 고객이 기존 회원이면서 뉴날 기기 사용자인 경우, 고객이 기기에서 기존 계정으로 로그인하면 두 시스템이 연결됩니다. 연결 방식은 6.3에서 설명합니다.

검증

뉴날이 개발·운영한 백신 패스 COOV 사용자 4,300만 명, 하루 최대 검증 3,000만 건, 발급된 DID 2억 6천만 개, 등록·출원 특허 90여 건.

---

1. 기본 개념 — 데이터 요새와 데이터 광장

비교 항목	데이터 요새 (지금까지의 서비스)	데이터 광장 (뉴날)
식별 정보와 민감한 기록	회사 서버에 저장되고, 회사 직원이 열 수 있습니다.	암호화되어 고객의 개인 데이터 노드에 저장되고, 고객의 키로만 열립니다.
데이터가 사용된 기록	회사 내부에만 있습니다.	공개 원장에 기록됩니다. 고객과 외부 감사인이 볼 수 있습니다.
무단 사용이 일어났을 때	회사 안에서 감춰집니다.	기록되고 고객에게 통보되므로 즉시 드러납니다.
활용의 방법	회사가 데이터를 자기 서버로 가져옵니다.	서비스가 고객의 노드에서 허락된 범위를 호출합니다.
활용의 대가	보관·유출·규제의 책임이 생깁니다.	책임이 생기지 않습니다. 사용 기록만 남습니다.
보호와 활용의 관계	보호를 늘리면 활용이 줄고, 활용을 늘리면 보호가 약해집니다.	보호가 늘수록 고객의 허락이 늘고, 허락이 늘수록 활용이 늘어납니다.

데이터 광장에서 공개되는 것은 사용 기록입니다. 데이터의 내용은 공개되지 않고 암호화됩니다. 고객이 자기 데이터의 소유를 믿음이 아니라 기록으로 확인할 수 있으므로, 뉴날은 데이터 광장이 만드는 소유를 **검증 가능한 소유권**이라고 부릅니다.

로그인의 방향도 바뀝니다. 데이터 요새에서는 이용자가 서비스에 로그인해서 데이터를 넘깁니다. 데이터 광장에서는 서비스가 이용자의 노드에 접근을 요청하고, 이용자가 승인합니다. 뉴날은 서비스가 이용자에게 접근을 요청하는 방식을 **역로그인(Reverse Login)** 이라고 부릅니다.

뉴날의 데이터 관리 구조는 보호를 위해 활용을 포기하는 구조가 아니라, 보호의 방향을 바꾼 결과로 활용이 가능해지는 구조입니다. 나머지 장은 위 표의 오른쪽 열이 어떤 구조로 구현되어 있는지를 설명합니다.

2. 용어 정의

용어	뜻
DID (디지털 신원)	실명이나 회사 계정 대신 사람을 가리키는 식별자입니다. 고객의 기기가 만들고 공개 원장에 등록합니다. 소유권은 고객의 기기에 있는 암호화 키로 증명됩니다.
개인 데이터 노드	고객 한 사람마다 하나씩 있는 데이터 저장 단위입니다. 클라우드에서 실행되지만, 고객의 DID에 등기되어 있고, 고객의 키로만 열리며, 고객이 다른 클라우드로 옮길 수 있습니다. 3장에서 설명합니다.
데이터 스피어	개인 데이터 노드 안에서 서비스별로 나뉜 데이터 영역입니다. 파트너 기업마다 하나씩 있습니다. 고객이 허락하면 고객의 노드 안에 파트너 기업의 영역이 생기고, 파트너 기업은 파트너 기업의 영역만 봅니다.
에이전트 플레이스	파트너 기업의 서비스가 등록되어 동작하는 뉴날의 서비스 플랫폼입니다.
InfraBlockchain (공개 원장)	DID의 등기, 허락과 접근의 기록, 각 서비스가 읽고 쓸 수 있는 데이터 범위, 정산 장부가 오르는 퍼블릭 블록체인입니다. 가상화폐 발행 없이 작동하고, 데이터 원본은 저장하지 않으며, 뉴날도 기록을 바꿀 수 없습니다.

3. 개인 데이터 노드

"고객이 데이터를 소유한다"는 설명에 파트너 기업은 두 가지를 묻습니다. "고객의 디바이스에 저장한다는 뜻인가?" "클라우드에 저장한다면 결국 서버 저장 아닌가?"

디바이스에 저장하지 않습니다. 개인 데이터 노드는 클라우드에서 실행되는 프로그램과 저장소입니다. 디바이스에는 노드를 여는 암호화 키와 소량의 비공개 저장소만 있습니다. 디바이스가 꺼져 있어도 노드는 동작합니다.

클라우드에 있지만 회사 서버 저장과 다릅니다. 저장 위치는 같고, 다음 다섯 가지가 다릅니다.

비교 항목	회사 서버의 데이터베이스	개인 데이터 노드
데이터의 단위	모든 고객의 데이터가 하나의 데이터베이스에 담깁니다.	고객 한 사람마다 노드가 하나씩 있습니다.
누구의 것으로 등기되는가	회사의 계정 체계에 속하며, 회사의 자산입니다.	고객의 DID에 등기됩니다. 등기 기록은 공개 원장에 있습니다.
누가 열 수 있는가	데이터베이스 권한을 가진 회사 직원이 엽니다.	고객의 기기에 있는 암호화 키로만 열립니다. 클라우드 운영자도 뉴날도 열 수 없습니다.

비교 항목	회사 서버의 데이터베이스	개인 데이터 노드
실행 환경	일반 서버입니다. 서버 관리자가 내용을 볼 수 있습니다.	메모리까지 암호화되는 기밀 실행 환경입니다. 클라우드 관리자도 소프트웨어 접근으로는 내용을 볼 수 없습니다. 실행 중인 코드가 공개된 코드와 같은지 외부에서 검증할 수 있습니다.
옮길 수 있는가	회사가 정한 서버에 있습니다.	고객이 노드를 다른 클라우드로 옮길 수 있습니다.

본 문서에서 "고객이 데이터를 소유한다"는 세 조건을 뜻합니다. 데이터가 고객의 DID에 **등기**되어 있고, 여는 **키**가 고객의 기기에만 있으며, 고객이 노드를 **옮길** 수 있습니다. 저장 위치는 소유의 기준이 아닙니다.

---

4. 보안 — 외부 해킹과 내부자 부정에 대한 대응

4.1 식별·연락·인증의 수단

회사에 필요한 기능	지금까지의 수단	뉴날의 수단
식별 — 같은 고객을 다음에도 알아본다	실명, 주민번호, 계정 ID	DID
연락 — 고객에게 메시지를 보낸다	전화번호, 이메일, 앱 푸시	DID 기반의 폐쇄망 통신. 고객이 허락한 상대만 연결됩니다.
인증 — 고객이 본인임을 확인한다	전화번호 인증, 이메일 인증, 비밀번호	고객의 기기와 기기 안의 암호화 키

회사가 실명과 전화번호를 수집해 온 이유는 식별·연락·인증을 할 다른 수단이 없었기 때문입니다. 문제는 저장 방식에 있습니다. 지금까지의 서비스는 실명, 전화번호, 계정, 민감한 기록을 하나의 테이블에 함께 저장하고, 수백만 명의 테이블을 하나의 서버에 둡니다. 한 번의 유출이 대규모 사고가 되는 이유입니다. 뉴날은 세 기능의 수단을 바꾸고, 남는 기록을 고객 한 사람마다 하나의 노드에 따로 저장합니다.

4.2 유출 경로별 비교

실제 유출 사고는 대부분 세 경로로 일어납니다. 열람 권한이 있는 내부 직원이 데이터를 유출하거나, 외부 공격자가 직원의 계정을 훔쳐 접근하거나, 외부 공격자가 서버에 침입해 데이터베이스를 복사합니다. 세 경로의 전제는 모든 고객의 데이터가 한곳에 있고 열람 권한이 회사 안에 있다는 것입니다. 뉴날의 데이터 관리 구조에는 두 전제가 없습니다.

공격 경로	회사 서버 방식	뉴날 데이터 관리 구조
내부 직원이 권한으로 데이터를 유출	정당한 권한으로 전체 고객 데이터를 조회하므로 보안 시스템이 막지 못합니다.	고객 데이터를 열 수 있는 직원이 없습니다. 뉴날의 관리자 권한은 노드를 운영하는 권한이지 읽는 권한이 아닙니다.
외부 공격자가 직원 계정을 탈취	탈취한 계정의 권한으로 데이터베이스에 접근합니다.	탈취할 계정에 열람 권한이 없습니다.
외부 공격자가 서버에 침입	수백만 명의 데이터가 한 번에 복사되고, 복사된 데이터에 실명·연락처가 함께 들어 있습니다.	노드 하나에 한 사람의 데이터만 있고, 암호화되어 있으며, 실명·연락처가 없습니다.
서버 관리자가 서버 내부를 봄	일반 서버에서는 최고 권한을 가진 관리자가 메모리와 디스크를 볼 수 있습니다.	노드는 클라우드 사업자가 제공하는 기밀 컴퓨팅 환경에서 동작합니다. 최고 권한을 가진 관리자도 소프트웨어 접근으로는 볼 수 없습니다. 물리적 공격이 남지만 노드 하나에는 한 사람뿐입니다.
뉴날이 몰래 코드를 바꿈	외부에서 알 수 없습니다.	기밀 실행 환경이 "실행 중인 코드가 공개된 코드와 같다"는 증거를 외부에 제출합니다(원격 증명).
파트너 기업 서비스가 허락 범위 밖에 접근	허락 범위는 회사의 약속으로만 지켜집니다.	각 서비스의 접근 범위가 공개 원장에 등록되어 있고, 범위 밖의 호출은 실행되지 않습니다. 범위 안의 접근도 기록되어 고객에게 통보됩니다.
고객의 기기를 공격	해당 없음.	한 사람의 데이터만 노출되고, 노출된 데이터로도 사람을 식별하거나 연락할 수 없습니다. 키는 기기의 하드웨어 보안 영역에 있습니다.

4.3 해킹이 소용없는 이유

회사 서버 방식에서는 서버 한 대를 한 번 침입하면 수백만 명의 데이터를 얻고, 데이터에 실명과 연락처가 함께 들어 있으므로 바로 범죄에 쓸 수 있습니다. 대규모 유출 사고가 반복되는 이유입니다.

뉴날의 데이터 관리 구조에서는 해킹이 두 단계에서 소용없어집니다.

첫째, 대규모 해킹이 성립하지 않습니다. 모든 고객의 데이터를 모은 서버가 없습니다. 개인 데이터 노드 하나에는 한 사람의 데이터만 있고, 노드를 열려면 그 사람의 기기를 따로 공격해야 합니다. 수만 명의 데이터를 얻으려면 같은 공격을 수만 번 반복해야 합니다.

둘째, 한 사람의 데이터를 얻어도 쓸 수 없습니다. 공격자가 큰 비용을 들여 한 사람의 노드를 열었다고 해도, 얻은 데이터에는 실명·주민번호·전화번호·이메일·주소가 없습니다. 공격자는 데이터가 누구의 것인지 알 수 없고, 데이터의 주인에게 연락할 수도 없습니다. 유출이 사고가 되려면 민감한 기록, 누구의 것인지 알려 주는 정보, 그 사람에게 닿는 수단이 함께 있어야 하는데, 뉴날의 구조에는 뒤의 둘이 없습니다.

	회사 서버 방식	뉴날 데이터 관리 구조
해킹 한 번으로 얻는 것	수백만 명의 데이터	한 사람의 데이터
얻은 데이터로 사람을 식별할 수 있는가	있습니다. 실명·주민번호가 함께 있습니다.	없습니다. 식별 정보가 없습니다.
얻은 데이터로 사람에게 연락할 수 있는가	있습니다. 전화번호·이메일이 함께 있습니다.	없습니다. 연락처가 없습니다.

뉴날이 유출 사고를 막는 방법은 침입을 완전히 차단하는 것이 아니라, 침입해도 대규모로 얻을 수 없고 얻어도 쓸 수 없게 만드는 것입니다.

4.4 키의 보관과 관리

노드를 여는 키는 고객 기기의 하드웨어 보안 영역에 있습니다. 뉴날의 서버에는 키가 없습니다. 고객이 원하면 뉴날의 키 관리 서비스를 쓸 수 있습니다. 키 관리 서비스는 키 정보를 고객 단위로 따로 저장하고, 본인 인증을 통과한 고객에게만 키를 제공합니다. 본인 인증은 고객이 등록 시점에 설정한 복구 수단으로 하며, 수단의 종류는 기술 문서에 있습니다. 관리자 권한으로는 키를 조회할 수 없으므로, 한 번의 침입으로 여러 고객의 키를 얻는 방법이 없습니다.

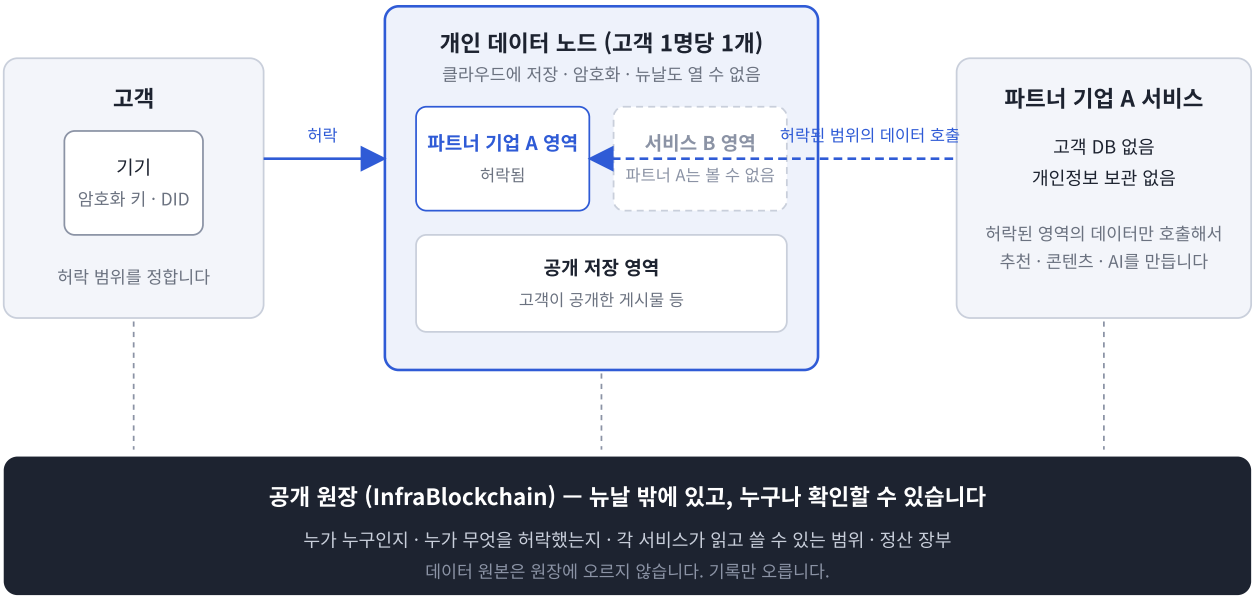
4.5 남는 위험

한 사람의 기기를 표적으로 공격하면 한 사람의 데이터가 노출될 수 있습니다. 노출된 데이터에도 식별 정보와 연락처는 없습니다. 고객이 사연이나 후기에 스스로 적는 이름은 시스템이 막을 수 없으며, 이름이 적힌 기록에도 전화번호와 주소는 없습니다. 결제 대행사와 판매 채널에 남는 결제 정보는 뉴날의 구조 밖에 있으며, 해당 사업자의 책임입니다.

---

5. 구조의 원칙

1. **고객 한 사람마다 개인 데이터 노드가 하나씩 있습니다.** 노드는 고객의 DID에 등기되어 있고, 고객의 키로만 열리며, 고객이 옮길 수 있습니다.
2. **시스템은 이름·전화번호·주민번호를 저장하지 않습니다.** 식별·연락·인증은 DID와 고객의 기기가 맡습니다.
3. **파트너 기업의 서비스는 허락된 데이터 영역만 봅니다.** 같은 고객의 다른 서비스 영역은 보이지 않습니다. 고객이 허락을 철회하면 접근은 즉시 중단됩니다.
4. **모든 접근은 기록되고 고객에게 통보됩니다.** 외부 감사인이 기록을 검증할 수 있습니다.
5. **소유·허락·접근의 기록은 뉴날 밖의 공개 원장에 있습니다.** 공개 원장에는 기록만 오르고 데이터 원본은 오르지 않습니다.



6. 파트너 기업의 역할과 책임

파트너 기업이 하는 일	파트너 기업이 하지 않는 일	파트너 기업이 얻는 것
서비스 기획과 운영	회원 데이터베이스 구축	고객이 허락한 데이터로 만드는 개인화 서비스
브랜드, 판매, 가격, 상품 구성	개인정보 보관	판매 수익, 구독 수익, 고객 관계
다룰 데이터 항목과 API 계약의 등록 (뉴날이 함께 합니다)	로그인·본인 확인 시스템 구축	보관·유출 책임 없음
고객에게 허락을 요청하는 화면과 문구	알림 발송 인프라 구축	DID 단위의 자동 정산
콘텐츠, 추천, AI 응답의 설계	유출 대응 체계 운영	서비스 시작 전에 고객 데이터를 확보할 필요 없음
결제 (지금 쓰는 결제 채널 그대로)	데이터 보안 인력 확보	

6.1 서비스 시작 절차

1. 등록	2. 허락	3. 활용	4. 정산
파트너 기업이 다룰 데이터의 서식과 API 계약을 공개 원장에 등록합니다.	파트너 기업의 서비스가 고객의 노드에 접근을 요청하고(역로그인), 고객이 승인하면 노드 안에 파트너 기업의 영역이 생깁니다.	파트너 기업의 서비스가 허락된 범위의 데이터를 호출해 추천·콘텐츠·AI 응답을 만듭니다.	DID 단위의 정산 장부가 사용료와 수익을 자동으로 집행합니다.

6.2 계정 기능의 대체

기능	지금까지의 방법	뉴날의 방법
로그인 · 본인 확인	아이디, 비밀번호, 전화번호 인증	DID와 기기가 증명합니다.
연락 · 알림	전화번호, 이메일, 앱 푸시	DID 기반의 폐쇄망 통신입니다. 고객이 허락한 상대만 연결됩니다.
구독 · 자격 확인	계정에 결제 이력을 연결	"해당 기기의 구독은 유효하다"는 자격증명만 검증합니다.
결제 · 환불 · CS	계정 조회	지금 쓰는 판매 채널과 결제 대행사가 그대로 맡습니다.
개인화 · 추천	서버의 이용자 프로필과 결합	고객의 노드 안에서 고객의 키로 결합합니다.
분실 · 복구	주민번호, 전화번호로 본인 확인	고객 본인이 주도하는 복구 절차입니다. 미성년 고객은 보호자가 참여합니다.

6.3 기존 시스템과의 연동

뉴날의 데이터 관리 구조는 파트너 기업의 기존 시스템과 병행합니다. 기존 회원 데이터베이스, 결제, 고객센터, 콘텐츠 시스템은 아무것도 바꾸지 않고 지금 그대로 운영합니다. 뉴날 기기의 서비스는 개인 데이터 노드와 에이전트 플레이스에서 동작하며, 기존 시스템과 데이터를 공유하지 않습니다.

같은 고객이 기존 회원이면서 뉴날 기기 사용자인 경우, 연결은 다음 절차로 이루어집니다.

단계	내용
1. 로그인	고객이 뉴날 기기에서 파트너 기업의 기존 계정으로 로그인합니다. 인증은 파트너 기업의 기존 시스템이 지금 하던 방식 그대로 처리합니다.
2. 자격증명 발급	인증이 끝나면 파트너 기업은 "해당 기기의 사용자는 우리 회원이다"라는 자격증명을 발급합니다. 자격증명에는 회원 등급, 구독 상태처럼 서비스에 필요한 항목만 담깁니다.

단계	내용
3. 저장	자격증명은 고객의 기기와 개인 데이터 노드에 저장됩니다.
4. 검증	파트너 기업의 서비스는 고객이 기존 회원인지 알아야 할 때 자격증명만 검증합니다. 기존 데이터베이스를 조회하지 않습니다.

연결 정보는 고객의 기기에만 있습니다. 파트너 기업의 데이터베이스에는 고객의 DID가 저장되지 않고, 고객의 노드에는 실명과 연락처가 저장되지 않습니다. 기존 데이터베이스가 유출되어도 노드의 데이터와 연결되지 않고, 노드가 노출되어도 기존 데이터베이스의 회원과 연결되지 않습니다. 결제(6.2 표)와 구독 확인이 자격증명으로 동작하는 것과 같은 방식입니다.

파트너 기업이 새로 하는 일은 자격증명 발급 하나입니다. 기존 시스템의 데이터 구조, 저장 위치, 운영 절차는 바뀌지 않습니다.

---

7. 검증 근거

국가 규모 운영. 뉴날이 개발·운영한 백신 패스 COOV를 대한민국 4,300만 명이 매일 사용했고, 하루 최대 3,000만 건 이상의 검증이 처리되었으며, 2억 6천만 개 이상의 DID가 발급되었습니다. 다룬 데이터는 의료 기록, 실명, 주민번호, 여권번호였습니다. 원본은 발급 기관의 서버에 남았고, 개인의 기기에는 자격증명만 담겼습니다. COOV가 국가 규모로 검증한 것은 DID, 자격증명, 공개 원장입니다. 개인 데이터 노드는 COOV 이후에 더해진 구성 요소이며, 현재 뉴날 aios에서 운영 중입니다.

공개 원장. 소유·허락·접근의 기록은 공개 원장에 있습니다. 파트너 기업의 감사인이나 외부 기관은 뉴날을 거치지 않고 확인할 수 있습니다.

원격 증명. 기밀 실행 환경은 "실행 중인 코드가 공개된 코드와 같다"는 증거를 외부에 제출합니다. 하드웨어 제조사의 증명 체계를 사용하는 제3자가 검증하며, 뉴날은 검증에 관여하지 않습니다.

가상화폐 없는 퍼블릭 블록체인. InfraBlockchain은 가상화폐 발행 없이 작동합니다. 합의 알고리즘은 미국·국제·한국에 등록된 특허이며, 수수료가 안정적입니다.

---

8. 기존 인프라와의 관계

뉴날의 데이터 관리 구조는 클라우드, AI 모델, 운영체제를 대체하지 않습니다. 기존 인프라 위에 놓이는 층이며, 기존 인프라가 하는 일은 그대로 두고 개인 데이터를 다루는 방식만 더합니다.

기존 인프라	기존 인프라가 하는 일	뉴날의 구조가 더하는 것
클라우드	개인 데이터 노드를 실행합니다. 노드가 동작하는 기밀 컴퓨팅 환경은 클라우드 사업자가 제공하는 기술입니다.	고객 한 사람마다 노드가 하나씩 생기므로, 사용자가 늘수록 클라우드 사용량이 늘어납니다.

기존 인프라	기존 인프라가 하는 일	뉴날의 구조가 더하는 것
AI 모델	고객이 허락한 데이터를 맥락으로 받아 개인화된 응답을 만듭니다.	모델 회사는 개인 데이터를 보관하지 않고도 개인의 맥락을 사용할 수 있습니다. 보관·유출·규제의 책임 없이 개인화가 가능합니다.
운영체제와 기기	로그인·알림·결제를 처리합니다.	뉴날 aios는 기존 안드로이드 기기에는 보안 계층으로 탑재되고, 전용 기기에는 독립 운영체제로 탑재됩니다. 기존 기기와 앱 생태계는 그대로 유지됩니다.
기존 서비스	회원 데이터베이스, 결제, 고객센터를 운영합니다.	바꾸지 않습니다. 같은 고객은 자격증명으로 연결됩니다(6.3).

뉴날의 구조 위에서 지능의 사용량이 늘수록 클라우드와 모델의 사용량도 함께 늘어납니다. 뉴날은 기존 인프라 회사의 경쟁자가 아니라 사용자입니다. 뉴날의 구조를 채택하는 회사는 자기 클라우드, 자기 모델, 자기 기기 위에서 같은 방식으로 개인 데이터를 다룰 수 있습니다.

---

9. 규제 대응

개인정보 규제는 데이터로 개인을 **식별할 수 있는가**와 회사가 데이터를 **수집했는가**를 기준으로 적용됩니다. 뉴날의 구조는 두 조건에 해당하는 범위를 최소로 줄이도록 설계되었습니다. 공개 원장의 허락·접근 기록은 DID 단위의 가명 기록이며, 규제에 따라 가명 기록도 개인정보로 볼 수 있습니다.

규제가 요구하는 것	회사 서버 방식의 대응	뉴날 구조의 대응
최소 수집 GDPR 제5조	회사가 수집 항목을 줄입니다.	식별자와 연락처를 수집하지 않습니다.
동의만큼 쉬운 철회 GDPR 제7조	회사가 동의 관리 시스템을 운영합니다.	철회하면 접근이 즉시 중단됩니다.
설계 단계의 프라이버시 GDPR 제25조	회사가 개발 절차에 심사를 추가합니다.	구조가 요구를 충족합니다.
삭제권 GDPR 제17조	회사가 흩어진 사본을 찾아 지웁니다.	회사가 사본을 가진 적이 없습니다.
이동권 GDPR 제20조	회사가 내보내기 기능을 구축합니다.	고객이 노드 전체를 다른 클라우드로 옮깁니다.
열람권 GDPR 제15조	회사가 요청을 접수하고 회신합니다.	모든 접근이 기록되고 본인에게 통보됩니다.
유출 통지 GDPR 제33·34조	회사가 72시간 안에 통지합니다.	유출되어도 누구의 데이터인지 식별할 수 없도록 설계되었습니다.

규제가 요구하는 것	회사 서버 방식의 대응	뉴날 구조의 대응
국외 이전 제한 GDPR 제5장	회사가 이전 심사와 표준계약을 체결합니다.	노드의 소재지를 관할별로 둘 수 있습니다.
아동 보호 GDPR 제8조 · COPPA	회사가 연령을 확인하고 보호자 동의를 받습니다.	아동의 식별자와 연락처를 수집하지 않으며, 결제와 동의의 주체는 보호자입니다.

> 위 표는 법적 판단을 대신하지 않습니다. 관할별 세부 적용은 파트너 기업의 법무 검토와 함께 확정하며, 뉴날은 필요한 기술 자료를 제공합니다.

---

10. 자주 묻는 질문

Q1. 파트너 기업의 기존 데이터베이스와 시스템은 어떻게 되는가? 그대로 운영합니다. 뉴날의 데이터 관리 구조는 뉴날 기기를 위한 별도의 구조이며, 기존 시스템을 바꾸거나 옮기지 않습니다. 같은 고객이 기존 회원이면 고객이 기기에서 기존 계정으로 로그인하고, 파트너 기업이 회원 자격증명을 발급합니다. 파트너 기업의 데이터베이스에는 DID가 남지 않고, 노드에는 실명이 남지 않습니다(6.3).

Q2. 회원 DB가 없으면 고객 수와 활성 고객을 어떻게 아는가? 파트너 기업의 스피어에 허락을 준 고객 전원이 파트너 기업의 고객입니다. 고객 수, 활성 여부, 구독 상태는 DID 단위로 집계됩니다. 실명·연락처 명단은 생기지 않습니다.

Q3. 파트너 기업의 서비스에서 만들어진 데이터는 누구의 것인가? 고객의 노드 안 파트너 기업 영역에 남습니다. 소유권은 고객에게 있고, 파트너 기업은 허락 범위 안에서 계속 쓸 수 있습니다. 파트너 기업의 콘텐츠와 추천 로직은 파트너 기업의 자산입니다.

Q4. 파트너 기업이 스피어의 소유자이면 참여한 고객의 데이터를 다 볼 수 있는가? 아닙니다. 소유자는 스피어를 열고 참여 자격을 정하는 권한만 가집니다. 고객의 기록을 열려면 고객의 서명이 필요합니다.

Q5. 고객이 허락을 철회하면? 접근이 즉시 중단됩니다. 파트너 기업은 사본을 가진 적이 없으므로 지울 데이터가 없습니다.

Q6. 결제와 구독은? 지금 쓰는 판매 채널과 결제 대행사가 그대로 맡습니다. 뉴날 시스템에는 자격증명만 전달됩니다. 미성년 고객의 결제자는 보호자이므로 미성년자의 결제 정보는 시스템에 생기지 않습니다.

Q7. 고객이 사연이나 후기에 자기 이름을 쓰면? 시스템이 막을 수 없습니다. 뉴날의 주장은 "식별이 불가능하다"가 아니라 "기록을 실제 인물과 연결하는 실명·연락처·계정이 시스템에 없다"입니다.

Q8. 고객이 기기를 잃어버리면 데이터도 잃는가? 아닙니다. 원본은 암호화되어 분산 보관되고, 키는 고객이 설정한 복구 수단으로 복구합니다(4장).

Q9. 사고가 나면 누가 책임지는가? 망의 운영과 구조의 유지는 뉴날의 책임이며, 뉴날은 이행을 외부 감사로 증명합니다. 파트너 기업은 데이터를 소유하지도 보관하지도 않으므로 데이터 책임을 지지 않습니다.

Q10. 수사기관이 데이터를 요구하면? 뉴날이 제출할 수 있는 것은 암호화된 원본과 접근 기록뿐입니다. 열람 여부는 데이터의 주인이 결정합니다.

Q11. 파트너 기업의 직원이 고객 데이터를 유출할 수 있는가? 파트너 기업의 직원은 허락 범위 밖의 데이터에 접근할 수 없고, 범위 안의 접근은 모두 기록되어 고객에게 통보됩니다. 범위 안의 데이터에도 실명과 연락처는 없습니다. 직원 계정이 탈취되어도 같습니다.

문의

파트너십 문의 partner@newnal.com
기술 문서
newnal.com/docs/Newnal_Personal_Data_Security_Architecture_KR.pdf (한국어)
newnal.com/docs/Newnal_Personal_Data_Security_Architecture_EN.pdf (영어)

> **고객 데이터는 고객의 개인 데이터 노드에 남습니다. 파트너 기업은 허락된 데이터로 서비스를 만들고, 데이터의 책임은 지지 않습니다. 데이터 관리 구조는 뉴날이 운영하고 책임집니다.**