Newnal
Personal Data Management
Architecture

How to build personalized services
without holding customer data

This document explains how Newnal's data architecture protects personal data and, at the same time, makes it available for use.

NEWNAL Inc. · 2026

Contents

Overview 3

1. The Core Idea — the Data Fortress and the Data Square 4
2. Terms 5
3. The Personal Data Node 5
4. Security — Against External Attacks and Insider Misuse 6
5. Principles of the Architecture 8
6. The Partner's Role and Responsibilities 9
7. Evidence 11
8. How This Relates to Existing Infrastructure 11
9. Regulatory Alignment 12
10. Frequently Asked Questions 13

Contact 14

Overview

Digital services to date have protected data by gathering users' data on the company's central servers and defending them against outside intrusion. Newnal calls this approach — keeping data gathered on a central server — the **data fortress**. A data fortress blocks outside intrusion, but it cannot stop an inside employee who holds reading privileges, or an outside attacker who steals that employee's account. Because only the company can see inside the fortress, users cannot see how their own data is used. And because a company must bring data onto its own servers in order to use it, the moment it does, the responsibilities of custody, breach, and regulation follow.

Newnal changed the direction of protection. Information that identifies a person and sensitive records are encrypted so that only the customer — the owner of the data — can open them with the key on their own device, and the record of every use of the data goes onto a public ledger where anyone can check it. Newnal calls this approach — publishing the records of use — the **data square**. In the data square, services do not take the data; they call the scope the customer has permitted, so a company can use data without taking on liability. Newnal's data architecture is a structure for protection and, at the same time, a structure for use. It does not replace the cloud, AI models, or operating systems — it is a layer that sits on top of existing infrastructure (Section 8).

How Newnal works

The company does not gather customer data. Customer data is stored in a **personal data node** — one per customer. The node runs in the cloud, but the encryption key that opens it exists only on the customer's device. Partner services call the node's data within the scope the customer has permitted. The records of permission and access remain on a public ledger outside Newnal, which even Newnal cannot alter.

> **Customer data is stored in the customer's personal data node. Partner services use only the data the customer has permitted.**

Why security and use work at the same time

Why customer data is safe	Why partners can still use customer data
There is no database that gathers every customer's data. One hack yields one person's data, and even that data cannot be used to identify or contact anyone.	The data stays in the node, and the partner's service calls the permitted scope. Because the data never moves, no liability arises.
The key that opens a node exists only on the customer's device. Neither a Newnal employee nor a partner employee can open it.	When the customer grants permission, the partner's data area is created inside the node, and the partner builds personalized services on the data in its own area.
Identifying information such as legal names and phone numbers does not exist in the system. Stolen data cannot be traced to anyone.	Identification, contact, and authentication are handled by the DID and the customer's device. Login, notifications, and subscription checks work without identifying information.
Every access is recorded on the public ledger and reported to the customer.	Customers check the records and grant partners permission to their data. The more certain the protection, the wider the scope they permit.

What changes for partners

Partners build personalized services on the data customers have permitted. They build no member database and store no personal information, so they bear no breach liability. The brand, the sales revenue, the subscription revenue, and the customer relationship belong to the partner.

> **Partners' existing systems do not change.** Newnal's data architecture is a separate structure for Newnal devices. A partner's existing member database, payment, and customer-support systems keep operating exactly as they do today. When the same customer is both an existing member and a Newnal device user, logging in on the device with the existing account connects the two systems. Section 6.3 explains how.

Proof

COOV, the vaccine pass Newnal built and operated: 43 million users, up to 30 million verifications a day, 260 million DIDs issued, and some 90 patents registered or filed.

---

1. The Core Idea — the Data Fortress and the Data Square

Comparison	Data fortress (services to date)	Data square (Newnal)
Identifying information and sensitive records	Stored on company servers, where company employees can open them.	Encrypted and stored in the customer's personal data node; opened only with the customer's key.
Records of how data was used	Exist only inside the company.	Recorded on a public ledger. The customer and outside auditors can see them.
When unauthorized use occurs	It stays hidden inside the company.	It is recorded and reported to the customer, so it surfaces immediately.
How data is used	The company brings the data onto its own servers.	The service calls the permitted scope in the customer's node.
The price of use	The responsibilities of custody, breach, and regulation.	No liability arises. Only a record of use remains.
Protection versus use	More protection means less use; more use weakens protection.	More protection brings more permission from customers, and more permission brings more use.

What the data square makes public is the record of use. The contents of the data are not published; they are encrypted. Because customers can confirm ownership of their data through records rather than through faith, Newnal calls the ownership the data square creates **verifiable ownership**.

The direction of login also flips. In a data fortress, the user logs in to the service and hands data over. In the data square, the service requests access to the user's node, and the user approves. Newnal calls this way of a service requesting access from the user **Reverse Login**.

Newnal's data architecture does not give up use for the sake of protection; use becomes possible as the result of changing the direction of protection. The remaining sections explain the structures behind the right-hand column of the table above.

---

2. Terms

Term	Meaning
DID (digital identity)	An identifier that points to a person in place of a legal name or a company account. The customer's device creates it and registers it on the public ledger. Ownership is proven by the encryption key on the customer's device.
Personal data node	A unit of data storage, one per customer. It runs in the cloud, but it is registered to the customer's DID, opens only with the customer's key, and can be moved by the customer to another cloud. Explained in Section 3.
Data sphere	A per-service data area inside the personal data node — one per partner. When the customer grants permission, the partner's area is created inside the customer's node, and the partner sees only its own area.
Agent Place	Newnal's service platform, where partner services are registered and run.
InfraBlockchain (public ledger)	The public blockchain that carries the registry of DIDs, the records of permission and access, the range of data each service may read and write, and the settlement ledger. It operates without issuing cryptocurrency, stores no original data, and even Newnal cannot alter its records.

---

3. The Personal Data Node

When told "the customer owns the data," partners ask two things. "Does that mean it is stored on the customer's device?" "If it is stored in the cloud, isn't that server storage after all?"

It is not stored on the device. The personal data node is a program and storage that run in the cloud. The device holds only the encryption key that opens the node and a small private store. The node keeps operating even while the device is off.

It lives in the cloud, but it differs from company-server storage. The storage location is the same; the following five things differ.

Comparison	A company-server database	The personal data node
The unit of data	Every customer's data goes into one database.	Each customer has one node of their own.
Who it is registered to	It belongs to the company's account system; it is the company's asset.	It is registered to the customer's DID. The registration record is on the public ledger.

Comparison	A company-server database	The personal data node
Who can open it	Company employees with database privileges.	Only the encryption key on the customer's device opens it. Neither the cloud operator nor Newnal can.
The execution environment	An ordinary server. Server administrators can see the contents.	A confidential execution environment with memory-level encryption. Even cloud administrators cannot see the contents through software access. Whether the running code matches the published code can be verified from outside.
Can it be moved	It sits on servers the company chose.	The customer can move the node to another cloud.

In this document, "the customer owns the data" means three conditions: the data is registered to the customer's DID, the key that opens it exists only on the customer's device, and the customer can move the node. Storage location is not the criterion of ownership.

---

4. Security — Against External Attacks and Insider Misuse

4.1 The means of identification, contact, and authentication

What a company needs	The means until now	Newnal's means
Identification — recognizing the same customer next time	Legal name, national ID number, account ID	DID
Contact — sending the customer a message	Phone number, email, app push	DID-based closed-network communication. Only parties the customer has permitted can connect.
Authentication — confirming the customer is who they claim	Phone verification, email verification, passwords	The customer's device and the encryption key inside it

Companies have collected legal names and phone numbers because there was no other means of identification, contact, and authentication. The problem lies in how they are stored. Services to date keep legal names, phone numbers, accounts, and sensitive records together in one table, and put millions of such tables on one server. That is why a single leak becomes a mass incident. Newnal replaces the means for all three functions, and stores the records that remain in a separate node for each customer.

4.2 Comparison by attack path

Most real breaches happen along three paths: an inside employee with reading privileges leaks the data, an outside attacker steals an employee's account and gains access, or an outside attacker breaks into the server and copies the database. All three paths rest on the same premises — that every customer's data is in one place, and that reading privileges exist inside the company. Newnal's data architecture has neither.

Attack path	The company-server model	Newnal's data architecture
An insider leaks data using their privileges	They query all customer data with legitimate privileges, so security systems cannot stop them.	No employee can open customer data. Newnal's administrator privileges are for operating nodes, not for reading them.
An outside attacker steals an employee account	The stolen account's privileges give access to the database.	The account they steal carries no reading privileges.
An outside attacker breaks into a server	Millions of people's data is copied at once, and the copy carries legal names and contact details.	One node holds one person's data, encrypted, with no legal names or contact details.
A server administrator looks inside the server	On an ordinary server, an administrator with top privileges can see memory and disk.	The node runs in a confidential computing environment provided by the cloud vendor. Even an administrator with top privileges cannot see it through software access. Physical attack remains, but one node holds only one person.
Newnal quietly changes the code	There is no way to know from outside.	The confidential execution environment submits evidence to the outside that the running code matches the published code (remote attestation).
A partner service reaches beyond its permitted scope	The scope is kept only by the company's promise.	Each service's access scope is registered on the public ledger, and calls outside the scope do not execute. Access inside the scope is also recorded and reported to the customer.
The customer's device is attacked	Not applicable.	One person's data is exposed at most, and even that data cannot identify or reach anyone. The keys sit in the device's hardware security area.

4.3 Why hacking is not worth it

In the company-server model, one break-in on one server yields millions of people's data, and because that data comes with legal names and contact details, it can be used for crime right away. That is why mass breaches keep recurring.

In Newnal's data architecture, hacking becomes pointless at two stages.

First, hacking at scale does not exist. There is no server that gathers every customer's data. One personal data node holds one person's data, and opening a node requires attacking that person's device separately. Obtaining tens of thousands of people's data means repeating the same attack tens of thousands of times.

Second, even one person's data is useless once obtained. Suppose an attacker spends heavily and opens one person's node: the data contains no legal name, national ID number, phone number, email, or address. The attacker cannot tell

whose data it is, and cannot contact its owner. For a leak to become an incident, three things must be present together — sensitive records, information saying whose they are, and a means of reaching that person — and Newnal's architecture lacks the latter two.

	The company-server model	Newnal's data architecture
What one hack yields	Millions of people's data	One person's data
Can the data identify anyone?	Yes. Legal names and national ID numbers come with it.	No. There is no identifying information.
Can the data reach anyone?	Yes. Phone numbers and emails come with it.	No. There are no contact details.

Newnal prevents breach incidents not by blocking intrusion completely, but by making sure an intrusion yields nothing at scale, and nothing usable.

4.4 Key custody and management

The key that opens the node sits in the hardware security area of the customer's device. Newnal's servers hold no keys. Customers who want it can use Newnal's key management service, which stores key information separately per customer and releases a key only to a customer who passes identity verification. Verification uses the recovery methods the customer set at registration; the types of methods are listed in the technical documentation. Administrator privileges cannot query keys, so there is no way to obtain many customers' keys through a single intrusion.

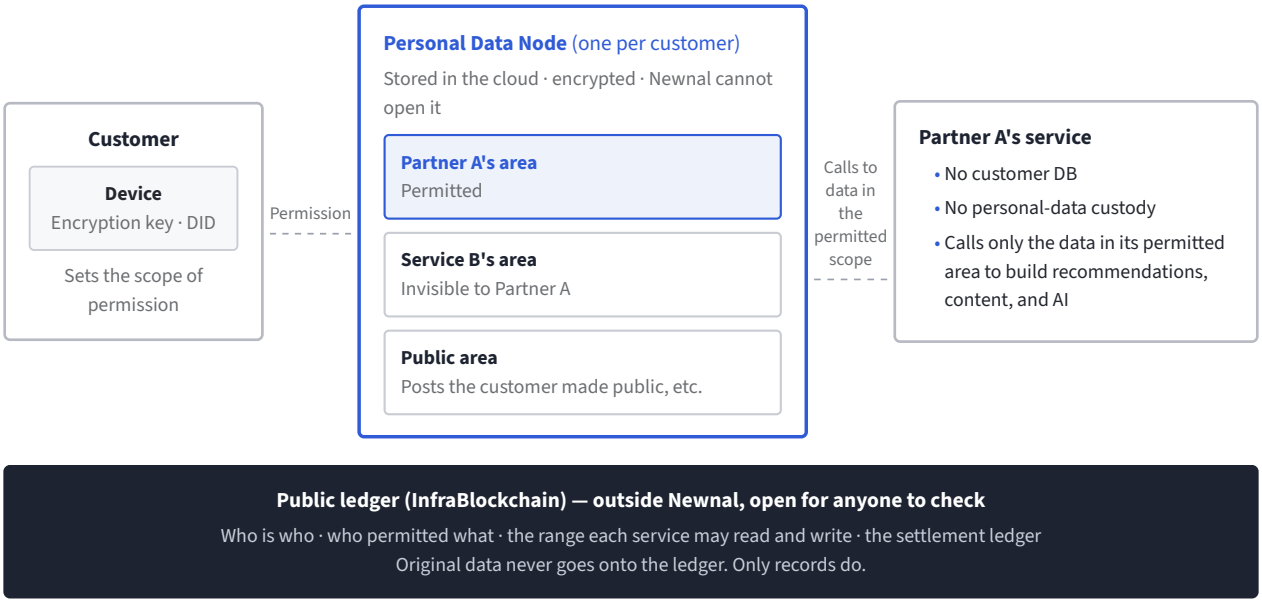
4.5 Remaining risks

A targeted attack on one person's device can expose that one person's data. Even the exposed data carries no identifying information and no contact details. The system cannot stop a customer from writing their own name into a story or a review; even a record that contains a name carries no phone number and no address. Payment information held by payment processors and sales channels sits outside Newnal's architecture and is the responsibility of those operators.

---

5. Principles of the Architecture

1. **Every customer has one personal data node.** The node is registered to the customer's DID, opens only with the customer's key, and can be moved by the customer.
2. **The system stores no names, phone numbers, or national ID numbers.** Identification, contact, and authentication are handled by the DID and the customer's device.
3. **A partner's service sees only the data area permitted to it.** The same customer's other service areas are invisible. When the customer revokes permission, access stops immediately.
4. **Every access is recorded and reported to the customer.** Outside auditors can verify the records.
5. **The records of ownership, permission, and access live on a public ledger outside Newnal.** Only records go onto the ledger — original data never does.



6. The Partner's Role and Responsibilities

What the partner does	What the partner does not do	What the partner gets
Service planning and operation	Building a member database	Personalized services built on data customers have permitted
Brand, sales, pricing, product lineup	Storing personal information	Sales revenue, subscription revenue, the customer relationship
Registering the data fields and API contract it will handle (Newnal does this with the partner)	Building login and identity-verification systems	No custody or breach liability
The screens and copy that ask customers for permission	Building notification infrastructure	Automatic settlement per DID
Designing content, recommendations, and AI responses	Operating a breach-response program	No need to acquire customer data before launching a service
Payment (through the payment channels used today)	Hiring data-security staff	

6.1 Launch procedure

1. Register	2. Permission	3. Use	4. Settlement
The partner registers the data schema and API contract it will handle on the public ledger.	The partner's service requests access to the customer's node (Reverse Login); when the customer approves, the partner's area is created inside the node.	The partner's service calls data in the permitted scope to build recommendations, content, and AI responses.	The DID-based settlement ledger executes fees and revenue automatically.

6.2 Replacing what the account used to do

Function	The method until now	Newnal's method
Login and identity check	ID, password, phone verification	The DID and the device provide the proof.
Contact and notification	Phone number, email, app push	DID-based closed-network communication. Only parties the customer has permitted can connect.
Subscription and entitlement	Payment history linked to an account	Only the credential "this device's subscription is valid" is verified.
Payment, refunds, support	Account lookup	The sales channels and payment processors in use today keep handling it.
Personalization and recommendation	Combined with the user profile on the server	Combined inside the customer's node, with the customer's key.
Loss and recovery	Identity check by national ID number or phone number	A recovery procedure the customer drives. A guardian takes part for minor customers.

6.3 Working alongside existing systems

Newnal's data architecture runs in parallel with the partner's existing systems. The existing member database, payment, customer-support, and content systems keep operating exactly as they do now — nothing is changed. Newnal-device services run on the personal data node and Agent Place, and they share no data with the existing systems.

When the same customer is both an existing member and a Newnal device user, the connection is made through the following steps.

Step	What happens
1. Login	The customer logs in on the Newnal device with their existing partner account. Authentication is handled by the partner's existing system, exactly the way it is handled today.
2. Credential issuance	Once authentication completes, the partner issues a credential stating "the user of this device is our member." The credential carries only the fields the service needs, such as membership tier and subscription status.

Step	What happens
3. Storage	The credential is stored on the customer's device and in the personal data node.
4. Verification	When the partner's service needs to know whether the customer is an existing member, it verifies only the credential. It does not query the existing database.

The connection information exists only on the customer's device. The partner's database does not store the customer's DID, and the customer's node does not store a legal name or contact details. If the existing database leaks, it cannot be linked to the node's data; if the node is exposed, it cannot be linked to the members in the existing database. This is the same mechanism by which payment (the table in 6.2) and subscription checks work through credentials.

The one new thing the partner does is issue a credential. The existing systems' data structures, storage locations, and operating procedures do not change.

---

7. Evidence

Operation at national scale. COOV, the vaccine pass Newnal built and operated, was used every day by 43 million people in Korea; more than 30 million verifications were processed on peak days; and more than 260 million DIDs were issued. The data handled included medical records, legal names, national ID numbers, and passport numbers. Originals stayed on the issuing authorities' servers, and individuals' devices held only credentials. What COOV verified at national scale is the DID, the credential, and the public ledger. The personal data node is a component added after COOV, and it is currently in operation on Newnal aios.

Public ledger. The records of ownership, permission, and access are on the public ledger. A partner's auditors or outside institutions can check them without going through Newnal.

Remote attestation. The confidential execution environment submits evidence to the outside that the running code matches the published code. Third parties verify it using the hardware manufacturer's attestation scheme; Newnal takes no part in the verification.

A public blockchain without cryptocurrency. InfraBlockchain operates without issuing cryptocurrency. Its consensus algorithm is patented in the United States, internationally, and in Korea, and its fees are stable.

---

8. How This Relates to Existing Infrastructure

Newnal's data architecture does not replace the cloud, AI models, or operating systems. It is a layer that sits on top of existing infrastructure: it leaves what that infrastructure does untouched, and adds only the way personal data is handled.

Existing infrastructure	What it does	What Newnal's architecture adds
Cloud	Runs the personal data nodes. The confidential computing environment the nodes run in is technology the cloud vendor provides.	Each customer gets a node of their own, so cloud usage grows as users grow.
AI models	Take the data the customer has permitted as context and produce personalized responses.	A model company can use a person's context without storing personal data. Personalization becomes possible without the liabilities of custody, breach, and regulation.
Operating systems and devices	Handle login, notifications, and payment.	Newnal aios ships as a security layer on existing Android devices, and as a standalone operating system on dedicated devices. Existing devices and app ecosystems stay as they are.
Existing services	Run the member database, payment, and customer support.	Nothing changes. The same customer is connected through credentials (6.3).

As the use of intelligence on Newnal's architecture grows, the use of the cloud and of models grows with it. Newnal is not a competitor to existing infrastructure companies but a user of them. A company that adopts Newnal's architecture can handle personal data the same way on its own cloud, its own models, and its own devices.

---

9. Regulatory Alignment

Privacy regulation applies according to two tests: whether the data can identify a person, and whether the company collected it. Newnal's architecture is designed to minimize the scope that meets either condition. The permission and access records on the public ledger are pseudonymous records at the DID level, and under some regulations pseudonymous records may still count as personal data.

What regulation requires	The company-server response	The Newnal-architecture response
Data minimization GDPR Art. 5	The company reduces the fields it collects.	Identifiers and contact details are not collected.
Withdrawal as easy as consent GDPR Art. 7	The company operates a consent management system.	Revoking stops access immediately.
Privacy by design GDPR Art. 25	The company adds review to its development process.	The architecture itself meets the requirement.
Right to erasure GDPR Art. 17	The company finds and deletes scattered copies.	The company never held a copy.

What regulation requires	The company-server response	The Newnal-architecture response
Right to portability GDPR Art. 20	The company builds an export feature.	The customer moves the whole node to another cloud.
Right of access GDPR Art. 15	The company receives requests and replies.	Every access is recorded and reported to the person.
Breach notification GDPR Arts. 33–34	The company notifies within 72 hours.	Designed so that leaked data cannot be traced to anyone.
Limits on international transfer GDPR Ch. V	The company runs transfer assessments and standard contracts.	Node locations can be placed per jurisdiction.
Protection of children GDPR Art. 8 · COPPA	The company verifies age and obtains guardian consent.	Children's identifiers and contact details are not collected, and the guardian is the subject of payment and consent.

The table above does not substitute for legal judgment. Detailed application by jurisdiction is settled together with the partner's legal review, and Newnal provides the technical materials required.

---

10. Frequently Asked Questions

Q1. What happens to the partner's existing database and systems?

They keep operating as they are. Newnal's data architecture is a separate structure for Newnal devices; it does not change or migrate existing systems. When the same customer is an existing member, the customer logs in on the device with the existing account and the partner issues a membership credential. No DID remains in the partner's database, and no legal name remains in the node (6.3).

Q2. Without a member DB, how do we know customer counts and who is active?

Every customer who has granted permission to the partner's sphere is the partner's customer. Customer counts, activity, and subscription status are tallied at the DID level. No roster of legal names and contact details ever comes into being.

Q3. Who owns the data created inside the partner's service?

It stays in the partner's area inside the customer's node. Ownership belongs to the customer, and the partner can keep using it within the permitted scope. The partner's content and recommendation logic remain the partner's assets.

Q4. If the partner owns the sphere, can it see all the data of the customers who joined?

No. The owner holds only the authority to open the sphere and set participation eligibility. Opening a customer's records requires that customer's signature.

Q5. What if the customer revokes permission?

Access stops immediately. The partner never held a copy, so there is no data to delete.

Q6. What about payment and subscriptions?

The sales channels and payment processors in use today keep handling them. Only credentials pass into Newnal's system. For a minor customer the payer is the guardian, so a minor's payment information never comes into existence in the system.

Q7. What if a customer writes their own name into a story or a review?

The system cannot stop that. Newnal's claim is not "identification is impossible" but "the legal names, contact details, and accounts that would link a record to a real person do not exist in the system."

Q8. If a customer loses their device, do they lose their data?

No. Originals are encrypted and stored redundantly, and keys are recovered through the recovery methods the customer set (Section 4).

Q9. Who is responsible if something goes wrong?

Operating the network and maintaining the architecture are Newnal's responsibility, and Newnal proves its performance through external audit. Partners neither own nor store the data, so they bear no data liability.

Q10. What if law enforcement demands data?

All Newnal can produce is encrypted originals and access records. Whether they are opened is decided by the owner of the data.

Q11. Can a partner's employee leak customer data?

A partner's employees cannot reach data outside the permitted scope, and every access within the scope is recorded and reported to the customer. Even the data within the scope carries no legal names and no contact details. The same holds if an employee's account is stolen.

Contact

Partnership inquiries partner@newnal.com

Technical documentation

newnal.com/docs/Newnal_Personal_Data_Security_Architecture_KR.pdf (Korean)

newnal.com/docs/Newnal_Personal_Data_Security_Architecture_EN.pdf (English)

> **Customer data stays in the customer's personal data node. Partners build services on the data customers have permitted, and bear no responsibility for the data. The data architecture is operated by Newnal, and Newnal answers for it.**