

Consent you can prove. Rights you can meet. Breaches you can report in time.

Nyvika is the compliance platform for Indian Data Fiduciaries: it records every consent as tamper-evident evidence, runs the rights and grievance helpdesk against the law's clocks, and gets you through a breach with the 72-hour report already drafted.

Evidence, not assurances

Every consent and every action on a request is hash-chained; auditors verify it in one click.

Built for India

Notices in English and all 22 scheduled languages, Indian identifiers, IST clocks, Rule-by-Rule guidance.

Live in 30 days

One script on your website, two API calls from your systems, your data on your own servers.

PREPARED FOR

Data Fiduciaries preparing for the DPDP Act, 2023 and the DPDP Rules, 2025

Why this matters now

The Digital Personal Data Protection Act, 2023 turns every Indian company that decides how personal data is used — every *Data Fiduciary* — into an organisation that must be able to show, for each person, what it asked, what they agreed to, what it did when they changed their mind, and how quickly it acted when they exercised a right or when something went wrong.

₹250 cr

maximum penalty per instance for failing to take reasonable security safeguards

72 hours

to file the detailed breach report with the Data Protection Board (Rule 7)

30 days

a common internal deadline for rights requests; grievances must be redressed within 90 days (Rule 14)

22 + 1

languages a notice may have to be offered in — every scheduled language plus English (Rule 3)

Most organisations have a cookie banner, a privacy policy and a shared mailbox. None of that produces **evidence**. When the Board or an auditor asks "show me that this person consented to marketing, and that you stopped when they withdrew", a CRM export is not an answer.

What Nyvika does

Nyvika is a single platform that covers the whole obligation, end to end:

Consent, as evidence

Itemised notices in the person's language; a consent ledger where every decision is hash-chained and verifiable years later.

Rights and grievances

A self-service Privacy Centre for your customers and a helpdesk for your team, with the statutory clocks built in.

Breach response

A 72-hour clock, an ordered checklist, the Board report and bilingual notices to affected people — drafted for you.

Where the data lives

Discovery of personal data across your systems, a register of processors and their agreements, and data-flow maps.

Retention that erases

Retention periods enforced per purpose, inactivity warnings, and processors instructed to erase — automatically.

Proof for the Board

Nine reports, an integrity check of every chain, and an audit log of everything your team did.

THREE PROMISES

- ✓ **Evidence, not assurances.** Consent artefacts and request timelines are append-only hash chains. Tampering is detectable; verification is one click.
- ✓ **Built for India.** All 22 scheduled languages, Aadhaar/PAN/UPI-aware discovery, IST clocks, and every screen annotated with the section or Rule it answers to.
- ✓ **Live in 30 days.** One script tag on your website, two API calls from your systems, and your data stays on your own servers.

What the law asks of a Data Fiduciary

The Act was passed in August 2023; the DPDP Rules, 2025 that make it operational were notified in November 2025, with most obligations applying after a transition period — in practice, before the next financial year is out. Your counsel can confirm the exact dates for your organisation.

Obligation	Where	What it means in practice
Notice and consent	s.5, s.6, Rule 3	Before or at the time of asking, tell people each purpose, itemised, in English or any scheduled language. Consent must be free, specific, informed and unambiguous — no pre-ticked boxes, no bundling.
Withdrawal	s.6(4), s.6(6)	Withdrawing must be as easy as giving consent, and processing — including by your processors — must stop.
Rights of access, correction and erasure	s.11, s.12	People may ask what you hold, correct it, or have it erased. You must verify who is asking and respond within the period you publish.
Grievance redressal	s.13, Rule 14	A published grievance channel; grievances redressed within 90 days, after which the person may go to the Board.
Nomination	s.14	People may nominate someone to exercise their rights on death or incapacity.
Security safeguards	s.8(5), Rule 6	Reasonable safeguards, including encryption, access control, logging and the ability to detect breaches.
Breach notification	s.8(6), Rule 7	Intimate the Board and every affected person without delay; file a detailed report with the Board within 72 hours.
Erasure and retention	s.8(7), Rule 8	Erase personal data once the purpose is served or consent withdrawn — and make your processors do the same. Warn people before erasing for inactivity.
Processors and contracts	s.8(2)	Only engage processors under a valid contract; you remain accountable for what they do.
Contact details	s.8(9), Rule 9	Publish the contact of the person who answers questions about personal data (a Data Protection Officer for significant fiduciaries).
Significant Data Fiduciaries	s.10, Rule 12	If notified as significant: a resident DPO, periodic Data Protection Impact Assessments and independent audits.

Penalties, and when it applies

The Act is in force; the Rules give Data Fiduciaries a transition period to be ready. The penalties are set out in the Act's Schedule and apply per instance.

AUGUST 2023

The Act is passed

The Digital Personal Data Protection Act, 2023 receives assent: consent, rights, breach notification, erasure and penalties are law.

NOVEMBER 2025

The Rules are notified

The DPDP Rules, 2025 set the detail: notice content and languages, breach reporting within 72 hours, grievance redressal, retention, and a phased start.

TRANSITION PERIOD

Get ready

Register purposes, publish itemised notices, stand up the Privacy Centre and helpdesk, rehearse a breach, connect processors — and start building evidence now.

IN FORCE

Evidence on demand

From the day the obligations apply, the Board, auditors and customers can ask you to show what you did — for any person, on any date.

PENALTIES (SCHEDULE)

- Up to **₹250 crore** — failing to take reasonable security safeguards
- Up to **₹200 crore** — failing to notify the Board or affected people of a breach
- Up to **₹200 crore** — breaching obligations about children's data
- Up to **₹150 crore** — a Significant Data Fiduciary's additional duties
- Up to **₹50 crore** — any other provision

WHAT USUALLY GOES WRONG

- Consent exists somewhere in a CRM field — with no record of what notice the person actually saw.
- A withdrawal is honoured in one system and forgotten in three others.
- Rights requests arrive by email and quietly miss the deadline.
- A breach is discovered on a Friday; nobody knows the 72 hours have started.
- Data is kept forever because nothing is responsible for deleting it.

This document summarises the law for orientation; it is not legal advice. Nyvika's screens cite the section or Rule each step answers to, so your counsel can check the mapping directly.

Nyvika in one picture

Your website, apps and call centre ask for consent through Nyvika. Your customers manage it in a hosted Privacy Centre. Your privacy team works from one console where every obligation has a screen, a clock and a report.

Your website & apps

The Nyvika widget shows the notice and records consent; kiosks, IVR and call centres record through the API.



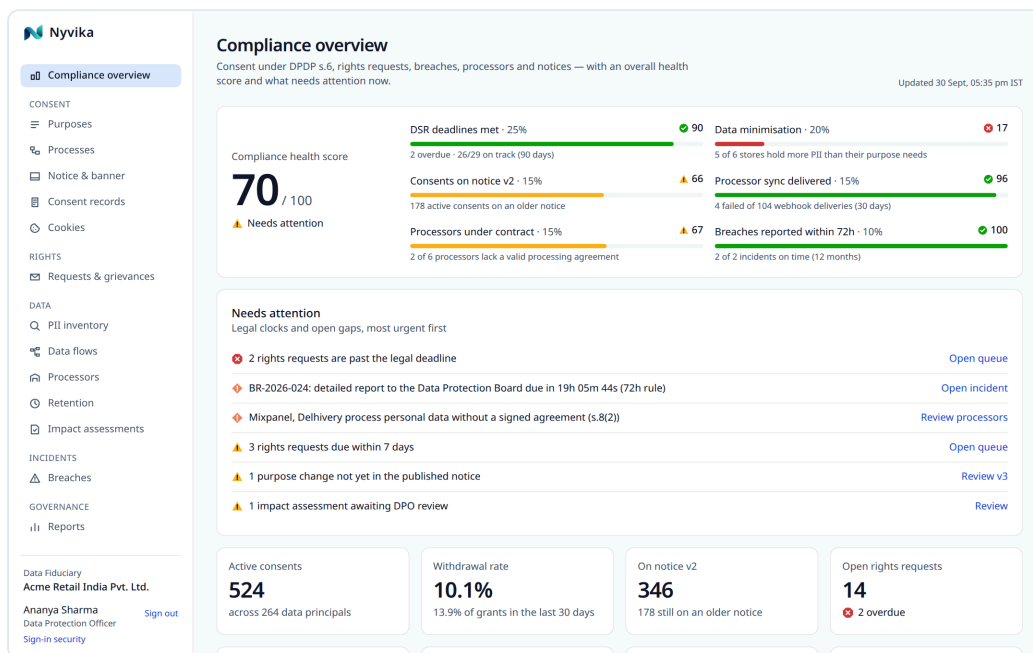
Nyvika

Consent ledger · Privacy Centre · Rights helpdesk · Breach register · Discovery · Processors · DPIA · Retention · Reports · Audit log



Your processors

Withdrawals and erasures are pushed to HubSpot, Salesforce and other systems automatically, with a delivery log.



The compliance overview. One score built from the things the law measures — notice coverage, consent health, requests within deadline, breaches reported in time, processor agreements — and a list of what needs attention today.

1 Consent

Purpose register, itemised notices in every language, the widget, the ledger, re-consent when a notice changes, business-process routing for apps, IVR and kiosks.

2 Rights

Privacy Centre with one-time-code sign-in; access, correction, erasure, nomination and grievance requests worked in a helpdesk with the clock visible.

3 Incidents

Breach register with the Rule 7 checklist, the 72-hour clock, a drafted Board report and bilingual notices sent to affected people.

4 Data

Discovery scans that find Aadhaar, PAN, UPI and more across your stores; data-flow maps; a processor register with agreements, reviews and risk.

5 Governance

Data Protection Impact Assessments with a scored questionnaire and review; retention that erases; cookie banner and inventory.

6 Proof

Nine exportable reports, a one-click integrity check of every chain, an audit log of every action, and team roles with two-factor and single sign-on.

Consent your customers understand — and you can prove

Nyvika replaces "I agree to the terms" with an itemised notice: one switch per purpose, off by default, in the customer's language. What they saw and what they chose becomes a permanent, tamper-evident record.

The screenshot shows a web browser window with the URL 'Demo client website. Acme Retail embeds the Nyvika widget. Walkthrough · Back to console'. The page header includes 'acme RETAIL', 'Shop', 'Sign in', 'Create account', and a shopping cart icon with '0' items. The main content area is titled 'Create your account' with the subtext 'Track orders, save addresses and check out faster.' Below this are input fields for 'Full name', 'Email or mobile number', and 'Password'. A note states 'Demo only: the password is never sent or stored.' There is a 'Create account' button and a link 'Already shopping with us? Sign in'. On the right, a Nyvika consent widget is displayed, titled 'Your privacy choices' with a language dropdown set to 'English'. The widget lists four categories: 'Account & orders' (switched 'On'), 'Product analytics' (switched 'Off'), 'Offers & newsletters' (switched 'On'), and 'Tax & legal records' (marked 'No consent needed'). Each category provides details on data usage, retention periods, and sharing. At the bottom of the widget, it states 'You can withdraw any consent at any time, as easily as you gave it, from the preference centre. Privacy centre' and 'If you are not satisfied with how we handle your data, you may complain to our grievance'.

The notice on a sign-up page. Each purpose is named, explained and switched off until the person turns it on. Legitimate uses are disclosed without a switch. Creating an account never implies consent.

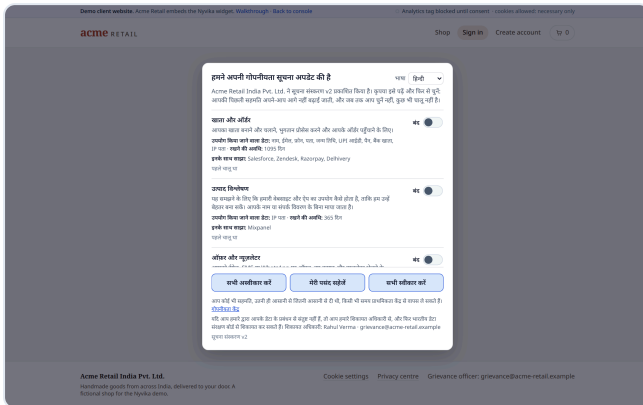
What makes it evidence

- Every decision is stored with the **exact notice version** the person saw, the language, the channel and the time.
- Each record carries a hash of the previous one — a chain per person and one for the whole organisation — so a changed or deleted record is detectable.
- Identifiers are stored as keyed hashes: the ledger itself contains no email addresses or phone numbers.

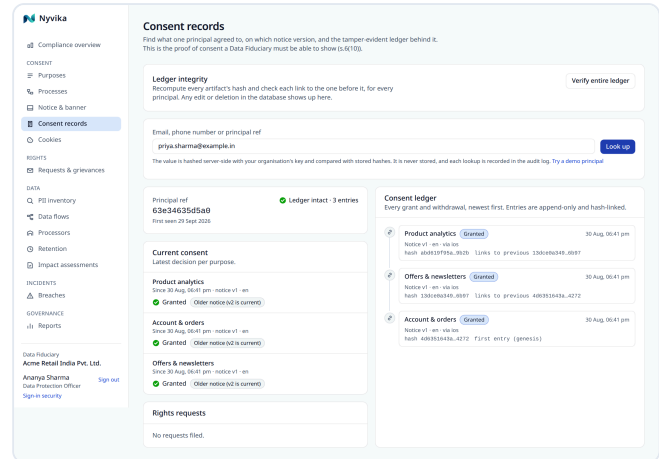
When the notice changes

- Publishing a new version freezes the old one; the difference is shown to your team before publishing.
- If the change needs fresh consent, customers are asked again on their next visit — in their language — and nothing is assumed.
- Channel-specific wording (a spoken IVR script, a short kiosk text) and per-app business processes are supported for organisations that ask for consent in many places.

- An auditor verifies a whole chain, or one person's, in a click.



Re-consent, in Hindi. The same notice in any of the scheduled languages; the person's choice is recorded per language.



Consent records in the console. Look up one person, see every decision in order, and verify the chain.

THE LAW, ANSWERED

s.5 (notice), s.6 (free, specific, informed, unambiguous consent; withdrawal as easy as giving it), Rule 3 (itemised notice in English or a scheduled language). No dark patterns: Reject, Customise and Accept are equal in size; switches start off; there is no close button that implies consent.

Withdrawal as easy as consent; rights within the deadline

Customers get a hosted Privacy Centre — sign in with a one-time code, see everything they agreed to, withdraw in a click, and file a request. Your team gets a helpdesk that never lets a deadline slip quietly.

Privacy centre - Acme Retail India Pvt. Ltd. Language: English Sign out

See what Acme Retail India Pvt. Ltd. may do with your personal data, change your consent at any time, and exercise your rights under the Digital Personal Data Protection Act, 2023.

Verified: reference 63e34655d5a0

My consents My requests Make a request Privacy notice

Our privacy notice has changed
You gave consent under an earlier notice (v1). Notice v2 changes what we tell you, so please confirm your choices or change them below.

[Confirm my current choices](#) [Change my choices](#)

Purposes that need your consent
Each purpose has its own switch. Turning one off withdraws your consent straight away; turning it on gives consent under notice v2.

Account & orders
To choose and run your account, process payments and deliver your orders.
Data used: Name, Email, Phone, Address, Date of birth, (PIN), PAN, Bank account, IP address. Kept for: 1095 days
Shared with: Salesforce, Zendesk, Razorpay, Delivery
On since 30 Aug 2023 - notice v1 On

Product analytics
To understand how our website and app are used so we can improve them. Measured without your name or contact details.
Data used: IP address. Kept for: 365 days
Shared with: Mixpanel
On since 30 Aug 2023 - notice v1 On

Offers & newsletters
To send you offers, new arrivals and newsletters by email, SMS or WhatsApp.
Data used: Name, Email, Phone. Kept for: 730 days
Shared with: HubSpot, Sendinblue
On since 30 Aug 2023 - notice v1 On

Purposes that don't need your consent
We process this under a legitimate use permitted by law (DPDP s.7). It's listed so you know about it.

Tax & legal records
To keep invoices and transaction records for 8 years, as GST law requires. This does not need your consent (DPDP s.7).
Data used: Name, Address, Phone, PAN. Kept for: 2020 days
Shared with: Not shared with third parties No consent needed

Privacy centre powered by Nyvika

Privacy centre - Acme Retail India Pvt. Ltd. Language: English Sign out

See what Acme Retail India Pvt. Ltd. may do with your personal data, change your consent at any time, and exercise your rights under the Digital Personal Data Protection Act, 2023.

Verified: reference 63e34655d5a0

My consents My requests **Make a request** Privacy notice

Choose what you'd like to do. We must respond within 30 days, and resolve grievances within 90 days.

Get a summary of my data
A summary of the personal data we hold about you, what we've kept for and who we've shared it with (s.17).

Correct my data
Correct, complete or update personal data that is wrong or out of date (s.13).

Erase my data
Delete your personal data, unless a law requires us to keep it (s.13).

Nominate someone
Name someone who can exercise these rights for you. Give them or your self access to the account (s.16).

Raise a grievance
Complain about how we have handled your personal data (s.15).

Nominate someone
Nominee's full name Relationship to you Nominee's email or phone number

Anything else? (optional)

[Submit request](#)

Filing a request. Access, correction, erasure, nomination or grievance — with the deadline stated up front.

The Privacy Centre. A person's current consents, with a switch to withdraw each one; their requests and the status of each.

Nyvika

Compliance overview

CONSENT

Purposes

Processes

Notice & banner

Consent records

Cookies

RIGHTS

Requests & grievances

DATA

PII inventory

Data flows

Processors

Retention

Impact assessments

INCIDENTS

Breaches

GOVERNANCE

Reports

Data Fiduciary

Acme Retail India Pvt. Ltd.

Ananya Sharma

Data Protection Officer

Sign-in security

Sign out

Requests & grievances

Rights requests from Data Principals (DPDP ss.11–14) must be resolved within 30 days, grievances within 90 days (Rule 14). Every action lands on a tamper-evident timeline.

Open

14

pending, in progress or on hold

Overdue

2

past the legal deadline

Due within 7 days

3

not yet overdue

Awaiting identity check

2

export and erasure are blocked until verified

View

Open

Fulfilled

Rejected

All

Type

All types

Access

Correction

Erasure

Nomination

Grievance

Assignee

Anyone

Me

Unassigned

Request	Identity	Channel	Assignee	Status	Filed	Deadline
NV-2026-000177 Erasure · DPDP s.12(3) Principal ab8ddb5cae8	ID verified	Privacy portal	Rahul Verma	In progress	26 Aug 2026	Overdue by 4d 22h 54m Day 30 of 30
NV-2026-000178 Access · DPDP s.11 Principal d5d698cd6d13	ID verified	Website form	Rahul Verma	In progress	29 Aug 2026	Overdue by 2d 10h 54m Day 30 of 30
NV-2026-000179 Erasure · DPDP s.12(3) Principal b39eb91ec746	ID not verified	Email	Unassigned	Pending	2 Sept 2026	2d 01h 05m Day 27 of 30
NV-2026-000180 Correction · DPDP s.12 Principal a5e371165fae	ID verified	Website form	Rahul Verma	On hold	4 Sept 2026	4d 01h 05m Day 25 of 30
NV-2026-000181 Access · DPDP s.11 Principal ac3f9210d206	ID verified	Privacy portal	Unassigned	Pending	5 Sept 2026	5d 01h 05m Day 24 of 30
NV-2026-000183 Erasure · DPDP s.12(3) Principal bca58e604749	ID verified	Privacy portal	Ananya Sharma	In progress	11 Sept 2026	11d 01h 05m Day 18 of 30
NV-2026-000184 Nomination · DPDP s.14	ID verified	Privacy portal	Unassigned	Pending	15 Sept 2026	15d 01h 05m

The helpdesk queue. Every open request with its deadline, days remaining, identity status and assignee. Overdue and due-soon items surface on the overview and in the daily digest.

Identity first

Erasure and access are blocked until identity is verified — by the one-time code or by your officer on a call-back.

Erasure that reaches processors

Executing an erasure withdraws every consent, redacts the ledger, and instructs each connected processor to erase — with a delivery log.

A timeline that can't be edited

Every note, status change and message to the person is hash-chained; the person sees the public entries in the Privacy Centre.

THE LAW, ANSWERED

s.6(4) and s.6(6) (withdrawal, and stopping processors), s.11 (access), s.12 (correction and erasure), s.13 and Rule 14 (grievance redressal within 90 days), s.14 (nomination). The response period for rights requests is configurable and shown on every request.

Breaches: the 72-hour clock, with the report already drafted

The moment your team records when a breach was detected, Nyvika starts the clock and lays out the Rule 7 steps in order. The Board report and the notices to affected people are drafted from what you have entered.



Compliance overview

CONSENT

Purposes

Processes

Notice & banner

Consent records

Cookies

RIGHTS

Requests & grievances

DATA

PII inventory

Data flows

Processors

Retention

Impact assessments

INCIDENTS

Breaches

GOVERNANCE

Reports

Data Fiduciary

Acme Retail India Pvt. Ltd.

Ananya Sharma

Data Protection Officer

Sign-in security

Sign out

← Breaches

BR-2026-024 · Credential-stuffing attack on customer accounts

Medium Investigating

Detailed report to the Data Protection Board · Rule 7(2)(b)

19h 05m 32s left

Detected 28 Sept, 12:41 pm

Due 1 Oct, 12:41 pm

Hour 52 of 72 since the breach was detected

Response checklist · Rule 7

Work through the steps in order. Each is timestamped as evidence for the Board.

1 Contain the breach

Stop further exposure — revoke access, rotate credentials, close the gap. s.8(5) requires reasonable security safeguards.

Mark contained

2 Intimate the Data Protection Board

Rule 7(2)(a): without delay, a description of the breach — its nature, extent, timing, location and likely impact.

Done 28 Sept, 03:41 pm

3 File the detailed report with the Board

Rule 7(2)(b): within 72 hours of becoming aware — facts, circumstances and reasons, mitigation, findings about who caused it, remedial measures and the notices sent to principals.

Record detailed report

4 Notify affected Data Principals

Rule 7(1): without delay, in clear and plain language, through their user account or registered email or phone.

Record principal notification

5 Resolve

Remediation is complete and the cause is addressed. Record the remediation above first.

Contain the breach first.

Mark resolved

6 Close the incident

Only once the Board has the detailed report and every affected principal has been notified. First file the detailed report with the Board, notify affected principals, resolve the incident.

Close incident

What happened

Login attempts using leaked passwords from another site succeeded on a number of customer accounts; attackers viewed saved addresses and phone numbers.

Occurred Not yet established

Detected 28 Sept, 12:41 pm

Principals affected ~380

Affected systems & data

Systems

Postgres Production DB · ap-south-1

Personal data categories

Email Phone Address

Cause & remediation

Update as the investigation progresses. Both feed the Board report.

Cause — events, circumstances and reasons

Password reuse from a third-party breach; no rate limiting on the legacy mobile login endpoint.

Remediation — measures to mitigate and prevent recurrence

What has been done and what is planned.

Save

An incident. The clock, the ordered checklist — contain, intimate the Board, report within 72 hours, notify affected people, resolve, close — with the timestamps that prove each step, and the affected systems and categories of data.

Send the notice to affected people
 Rule 7(1): without delay, in plain language, to their registered email or phone. Each person gets it by email, or a short SMS pointing to your grievance officer if we only have their phone number.

Who is affected

☒ Only these people — paste the affected emails and phone numbers, one per line

rohan.asht@example.in
 kavya.nair@example.in
 +91 98765 43210

☐ Everyone we hold an email or phone number for — when you can't tell who was affected

The notice (English)

Subject
 Important — a personal data breach affecting your data at Acme Retail India Pvt. Ltd.

Message

Dear user,

We are writing to tell you about a personal data breach at Acme Retail India Pvt. Ltd. that involves your personal data.

What happened
 A scheduled export of the newsletter list was written to a publicly readable storage folder for six hours. We became aware of it on 29 September 2026 at 09:36 pm IST. It began on 29 September 2026 at 11:36 am IST.

What data was involved
 Name, Email, Phone

What this could mean for you

☐ Also send a Hindi version to people who use Nyvika in Hindi

[Send 3 notices](#) [Change](#) 2 by email, 1 by SMS

Notifying affected people. Bilingual notices by email and SMS to everyone whose data was in the affected systems, sent from the incident and recorded on it.

Why it holds up

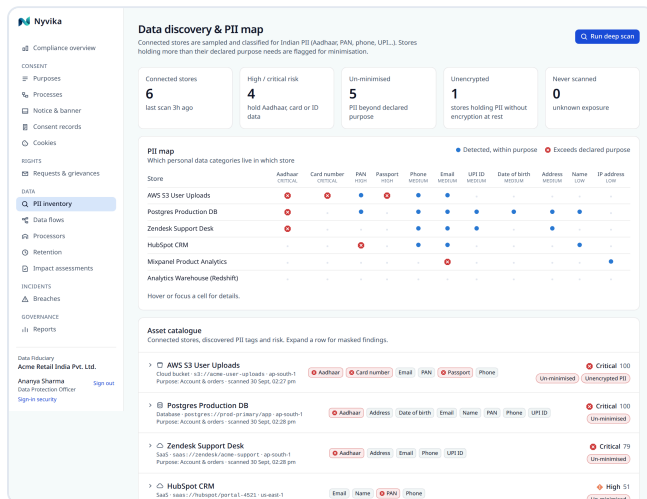
- Steps can only be taken in order and only once; closing requires the Board report and the notices to be done.
- Every step is on the incident's timeline and in the audit log, with the person who took it.
- The breach register report shows, for the year, whether every incident met 72 hours.
- Affected people are found from what you record about the incident — no separate mailing list to build at 2 a.m.

THE LAW, ANSWERED

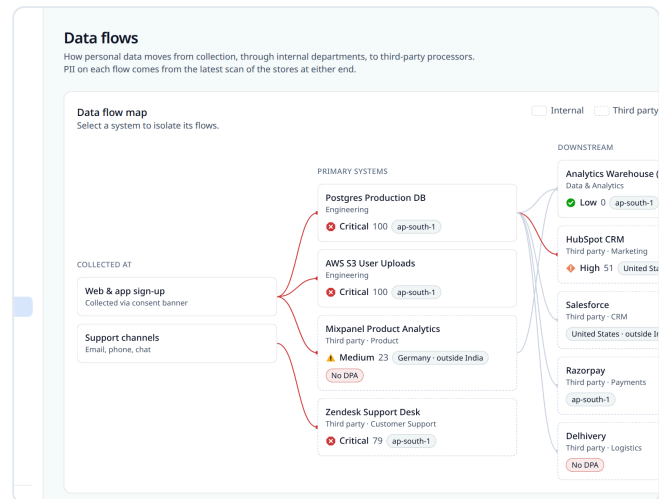
s.8(6) and Rule 7: intimate the Board and each affected person without delay; a detailed report to the Board within 72 hours covering nature, extent, timing, impact, mitigation, cause and remediation.

Know where personal data lives, who touches it, and why

You cannot protect, retain or erase what you cannot find. Nyvika scans your data stores for personal data, maps how it flows to processors, and keeps the register of contracts and reviews the law expects you to have.



PII discovery. Each connected store, the categories of personal data found in it (Aadhaar, PAN, card numbers, phone, email, UPI...), and a risk score. Findings are masked; raw values are never stored.



Data flows. Which purposes use which stores and which processors — the map behind your record of processing.

Processors

Everyone who processes personal data on your behalf. Under DPDP s.8(2) you may engage a Data Processor only under a valid contract, and you stay responsible for what they do with the data.

Active processors: 6 (2 synced automatically) | Without a signed DPA: 2 (no valid contract) | DPAs expiring ≤ 30 days: 2 (none expired) | Outside India: 3 (Germany, United States)

Purposes connect this register to consent. The purposes you tick for a processor decide what the consent notice lists as "shared with" for that purpose which processors receive instructions to stop and erase when a Data Principal withdraws consent or asks for erasure (s.6(6), s.8(7)). Processors with or Salesforce integration are updated automatically; the rest are notified for manual action.

Register

Highest risk first. Offboarded processors are listed at the bottom.

Processor - sync	Location	Purposes	Data received	Processing agreement	Security review	Risk
Mixpanel Product analytics Analytics Manual sync	Germany	Product analytics	IP address, Email	Awaiting Signature	In progress	High 58 why
Delivery Last mile delivery Logistics Manual sync	India	Account & orders	Name, Phone, Address	No agreement	Not started	High 54 why
Razorpay Payment gateway Payments Manual sync	India	Account & orders	Name, Phone, UPI ID, Card number	Signed (expires in 29 days (29 Oct 2026))	Passed	High 50 why
Salesforce Customer relationship management CRM	United States	Account & orders, Offers & newsletters	Name, Email, Phone, Address	Signed (expires in 20 days (19 Oct 2026))	Passed	Medium 30 why

Processors. Service, country, the purposes and data each one handles, agreement status, security review and a risk rating.

Nyvika

Personalised recommendations engine

Answer each question for this processing. The risk score updates live; flagged answers need a mitigation before the DPDP signs off.

What's being assessed

Recommend products from browsing and purchase history in the app and on the website.

PURPOSES

Personalised recommendations

SYSTEMS

Postgres Production DB, Analytics Warehouse (Redshift)

PROCESSORS

None linked

Locked while in review.

Data

What personal data is involved and how long it is kept.

Q1: Does the processing involve Aadhaar, financial account, card, health or biometric data?
Yes No Not applicable

Q2: Is personal data collected beyond what the stated purposes need?
Yes No Not applicable

Q3: Is there a defined retention period after which data is erased?
Yes No Not applicable

Principals

Whose data it is. Children's data needs verifiable parental consent (s.9).

Q4: Does the processing involve children's data (under 18)?
Yes No Not applicable

Q5: Is verifiable parental consent obtained where children are involved?
Yes No Not applicable

Review

Decision note: Recommend products from browsing and purchase history in the app and on the website. Conditions of approval, or what must change.

Required either way: the author sees it and it goes into the audit trail.

Owner: Meera Tyer
Reviewed: Pending
Updated: 29 Sept, 06:41 pm

Risk

Score: 12 of 12 answered
Raising the risk (4):
+8 Will more than 1 lakh Data Principals be affected?
+12 Does the processing involve profiling or automated decisions with significant effect?
+10 Does it involve tracking or behavioural monitoring?
+18 Is the data encrypted at rest and in transit?

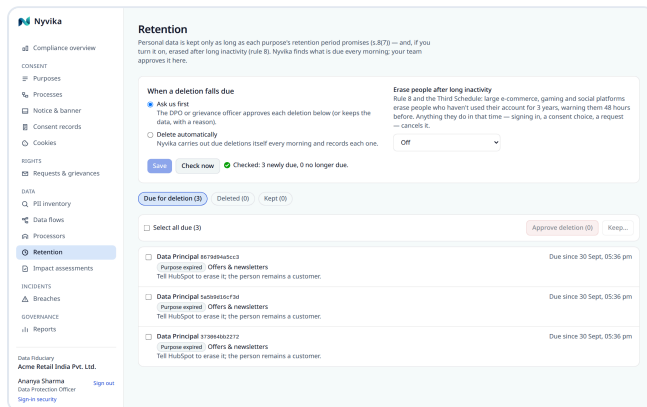
Impact assessments. A scored questionnaire, mitigations, an owner and a reviewer — the DPIA a Significant Data Fiduciary must produce, useful to everyone else.

THE LAW, ANSWERED

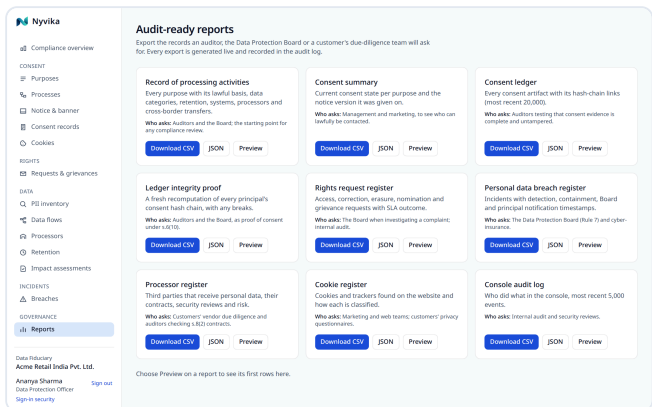
s.8(2) (processors only under contract), s.8(5) and Rule 6 (reasonable safeguards, which start with knowing what you hold), s.10 and Rule 12 (DPIAs and audits for Significant Data Fiduciaries).

Retention that actually erases; reports the Board will accept

Each purpose carries a retention period. When it lapses, or when someone has been inactive for the period you set, Nyvika opens a review, warns the person, and then withdraws, redacts and instructs processors — automatically if you want it to.



The retention queue. What is due, why, and what will happen — approve, dismiss with a reason, or let automatic mode run it.



Reports. Record of processing, consent ledger, consent summary, request register, breach register, processor register, cookie register, audit log, and the ledger-integrity proof.

Cookie compliance included

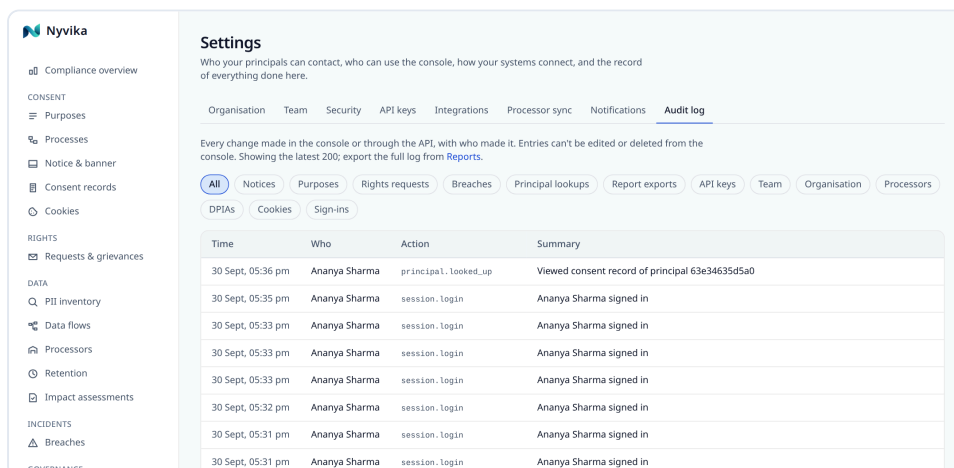
A cookie banner with equal Reject/Accept choices that actually blocks scripts until allowed, and a classified inventory.

An audit log of everything

Every change your team makes — who, what, when — is recorded and exportable. Lookups of a person's data are logged too.

Integrity on demand

One click recomputes every hash chain and reports whether anything has been altered since it was written.



The audit log. Publishing a notice, executing an erasure, sending a breach notice, exporting a report — all here, filterable and exportable.

Built for India, and built to be trusted

Every scheduled language

Notices in English and all 22 languages of the Eighth Schedule; the Privacy Centre in English and Hindi; notices to people bilingual.

Indian identifiers, Indian clocks

Discovery recognises Aadhaar, PAN, passport, voter ID, UPI and Indian phone numbers; deadlines run in IST; every step cites the section or Rule.

No dark patterns, by construction

Switches start off; Reject, Customise and Accept are equal; there is no "close" that means yes. The widget enforces this — your designers can't accidentally undo it.

Privacy by design

People are identified by keyed hashes; contact addresses live in an encrypted vault used only to carry out their instructions, and are destroyed after erasure.

Secure by default

Role-based access for your team, two-factor authentication (required organisation-wide if you choose), single sign-on with your identity provider, and a full audit log.

Your data on your servers

Nyvika runs in your cloud account or data centre from a standard container image, on PostgreSQL. Nothing about your customers leaves your infrastructure unless you connect a processor.

Fits the systems you already have

- **Website:** one script tag; the notice, cookie banner and re-consent are handled by the widget.
- **Apps, kiosks, IVR, call centres, paper forms:** consent recorded through the API, with wording per channel and a business process per journey.
- **CRM and marketing:** withdrawals and erasures pushed to HubSpot and Salesforce today; other processors through the same connector interface.
- **Email and SMS:** one-time codes, request updates and breach notices through your SMTP provider and MSG91 or Twilio.
- **Identity:** single sign-on through any OpenID Connect provider (Google Workspace, Microsoft Entra, Okta).

"Show me this person's consent" becomes a two-second answer with a hash that anyone can recompute — not a week of pulling exports from four systems.

Compared with the alternatives

Three routes are common: extend the cookie-banner tool you already pay for, adopt a global privacy suite built for GDPR and adapted for India, or build in-house. Each covers part of the obligation.

Capability	Cookie-banner tools	Global privacy suites	Build in-house	Nyvika
Itemised notice per purpose, off by default, 22 languages	Cookies only	Translation is your job	Months of work	Yes
Tamper-evident consent evidence	No	Logs, not chains	Rarely	Hash-chained, verifiable
Withdrawal pushed to processors	No	Via integrations you configure	Per system	Built in, with a delivery log
Rights helpdesk with deadlines and identity checks	No	Yes	Usually a ticketing tool	Yes, DPDP clocks
Breach register with the 72-hour clock, Board report and notices	No	GDPR templates	No	Rule 7, drafted for you
Discovery of Indian identifiers; processor register; DPIA	No	Yes	No	Yes
Retention that erases and tells processors	No	Policies, not execution	Per system	Yes
Runs on your own infrastructure	SaaS only	Usually SaaS	Yes	Yes, or managed
Time to first value	Days (for cookies)	Quarters	Quarters	Weeks

Assessments are of typical products in each category, not of any named vendor; ask us for a side-by-side with a specific tool you are evaluating.

THE HONEST SUMMARY

A cookie tool solves cookies. A global suite gives you a policy framework and a lot of configuration. Building it yourself gives you exactly what you specify — and a permanent maintenance obligation. Nyvika gives you the DPDP obligation as working software, in weeks, with the evidence built in.

Thirty days to go-live

Most organisations are live on their website within a month, with apps and other channels following. The work on your side is small and mostly decisions, not engineering.

WEEK 1

Set up

We deploy Nyvika in your cloud account (or ours). Your DPO and team are invited; two-factor and single sign-on are switched on.

WEEK 2

Decide

Your purposes, lawful bases, retention periods and processors go into the register — we run the workshop. The notice is drafted in your languages.

WEEK 3

Connect

One script tag on the website; consent capture on sign-up; CRM and email/SMS providers connected; identity verification tested.

WEEK 4

Go live

Notice v1 published; Privacy Centre linked from your privacy policy; your team trained on the helpdesk and breach process; first reports run.

What we need from you

- A named owner (usually the DPO or head of legal) and one developer for a few days.
- Your list of purposes and processors — or two hours with the people who know.
- Access to your cloud account, or a decision to use managed hosting.
- Your SMTP and SMS provider credentials for one-time codes and notices.

What you get

- The platform, deployed and configured, with your notice published.
- A written mapping of every obligation to a Nyvika screen for your counsel.
- Training for the privacy team, the helpdesk and the incident lead.
- A run-book for the day a breach happens.

Frequently asked

Where does the data live?	On your servers or in your cloud account, in PostgreSQL. Managed hosting in India is available if you prefer not to operate it.
We have several brands.	Nyvika is multi-organisation: each brand has its own notice, keys, team and evidence, under one deployment.
Our consent already lives in the CRM.	Keep it there; Nyvika becomes the system of record and pushes withdrawals and erasures to the CRM. Consent you already hold can be recorded through the API with its original source and notice noted, so the ledger starts complete.
We are not a Significant Data Fiduciary.	Then DPIAs and audits are optional for you — but the notice, consent, rights, breach and retention obligations apply to every fiduciary.
What if the Rules change?	Deadlines, retention periods and notice content are configuration, not code. Updates that the law requires are part of the subscription.
Can we see it with our own notice?	Yes — a demo with your purposes and languages takes about a week to prepare.

How we work with you

Pilot — 6 weeks

Your website and one journey, your team on the console, a real notice published. You keep everything recorded during the pilot.

Annual subscription

Priced by the number of people whose consent you manage, not by seats — your whole team uses it. Self-hosted or managed.

Onboarding and support

Deployment, the purposes workshop, notice drafting, training and the breach run-book are included. Support in Indian business hours; incident support around the clock.

INCLUDED IN EVERY PLAN

- All modules: consent, Privacy Centre, rights helpdesk, breach register, discovery, processors, DPIA, retention, cookies, reports and audit log.
- Every scheduled language; unlimited team members; unlimited notices and versions.
- Updates required by changes to the Act or the Rules.
- The full documentation set: a guide for your privacy team, the product reference and the technical documentation for your engineers and auditors.

Next steps

1. **A 45-minute walkthrough** of the live demo, following one customer and one privacy team through consent, a rights request and a breach.
2. **A demo with your notice** — your purposes, your languages, your website — prepared within a week.
3. **A pilot proposal** with scope, timeline and pricing for your organisation.

The Act asks you to be able to prove what you did. Nyvika is how you keep the proof — from the first consent to the last erasure.

Prices are shared in a separate commercial proposal tailored to the size of your organisation. All screens in this document are from the live product with fictional demo data; nothing shown is a mock-up.