

GUIDE FOR DATA FIDUCIARIES · DPDP ACT 2023 & RULES 2025

From your first sign-in to everyday compliance.

A step-by-step walkthrough of Nyvika for the people who run privacy at an Indian company: setting it up on day one, and the work of every day after.

Part I · Day one

Accept your invitation, secure your account, and set up purposes, the notice, processors, your team and your website

Part II · Every day

Rights requests, consent proof, notice changes, breaches, data discovery, DPIAs, cookies and retention

Part III · Reference

What the law asks and where Nyvika answers it, every deadline, routines, roles and troubleshooting

Read this first

This guide takes your organisation, a *Data Fiduciary* under the Digital Personal Data Protection Act, 2023, from the invitation email to running privacy compliance in Nyvika every day. It is written for the people who will use the console: the Data Protection Officer, the Grievance Officer and the privacy team.

How it is organised

- **Part I · Day one** follows Acme Retail's DPO, Ananya Sharma, as she sets up a brand-new organisation. Do the chapters in order; together they take an afternoon.
- **Part II · Every day** shows the same company a few months later, with real activity: customers consenting and changing their minds, rights requests, a breach, audits. Use it as a manual for each area.
- **Part III · Reference** collects what you will look up: which part of the law each screen answers to, every deadline, routines, roles, troubleshooting and a glossary.

Conventions

- Numbered steps are things to do, in order.
- **DPDP** boxes quote the part of the Act or the DPDP Rules, 2025 that a step answers to.
- **Built in** boxes are rules Nyvika enforces for you, so nobody can get them wrong by accident.
- **Tip** and **Watch out** boxes are advice from experience.
- The line under each chapter title says **who** can do it (see the roles table in Part III).

ABOUT THE EXAMPLES

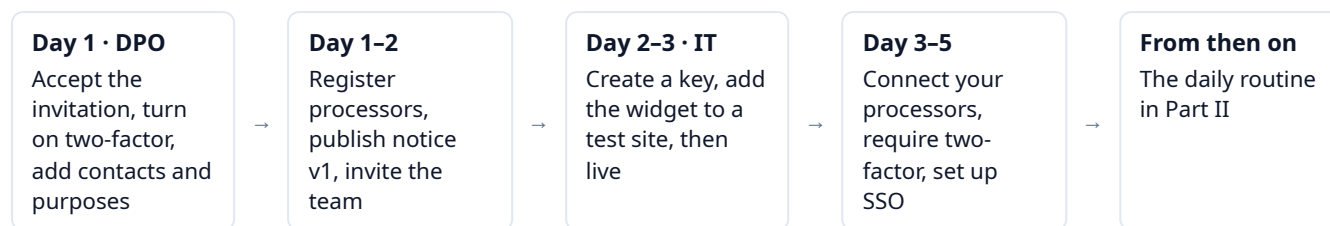
Acme Retail India Pvt. Ltd., its customers and staff are fictional. Every screenshot comes from the running product: Part I from a freshly created organisation, Part II from Nyvika's demo organisation. Data discovery and the cookie crawler are simulated in this version and are marked where they appear. Nothing in this guide is legal advice; confirm your obligations with your counsel.

What to have ready

Setting up goes quickly when these answers are at hand. None of them has to be perfect on day one; everything can be changed later, and Nyvika keeps a record of every change.

You'll need	Why	Used in
Names and work emails of your Grievance Officer and Data Protection Officer	You must publish whom people can contact about their data, and how to raise a grievance (s.8(9), s.8(10), Rule 9).	Chapter 4
A list of why you collect personal data : accounts and orders, marketing, analytics, legal records...	Each reason becomes a <i>purpose</i> , consented to separately (s.6(1)).	Chapter 5
For each purpose: what data it uses and how long you keep it	Shown on the notice; also the yardstick for data minimisation and deletion (s.8(7)).	Chapter 5
Your processors : CRM, email, payments, delivery, support, analytics, hosting — and whether each has a signed data processing agreement	Processors may only be engaged under a valid contract (s.8(2)); they must be told about withdrawals and erasures.	Chapter 6
The people who will use the console and their roles	Everyone signs in as themselves, so every action is attributed.	Chapter 8
Optional: your company's single sign-on details (Microsoft Entra ID, Google Workspace, Okta...)	Lets your team sign in with their work accounts.	Chapter 9
Optional: the channels you collect consent on (app, IVR, kiosk, call centre) and the journeys that ask for it (app sign-up, home delivery)	Each channel can have its own wording; each journey can present exactly its own purposes.	Chapter 5, 11
Optional: admin access to your CRM, marketing tools and other processors	So withdrawals and erasures reach them automatically.	Chapter 10
Someone who can add a script to your website	The consent banner and notice run on your site.	Chapter 11

Your first week at a glance



Who does what

Nyvika has four roles. Give each person the least access their job needs; you can change roles at any time.

Role	Typically	Can
Data Protection Officer	The DPO or head of privacy	Everything, including publishing the notice, approving DPIAs, API keys, team and security settings.
Grievance Officer	Customer-rights and complaints team	Handle rights requests and grievances; report and manage breaches.
Privacy Analyst	Privacy or data-governance staff	Edit purposes and draft notices, run discovery, manage processors, DPIAs and cookies.
Viewer	Internal audit, legal, leadership	See everything, change nothing.

PART I

Day one: setting up

Ananya Sharma has just been appointed Data Protection Officer at Acme Retail. Nyvika has created the organisation for her. Everything else, she does herself, in the eleven chapters that follow.

Accept your invitation

Who: everyone, once.

Nobody chooses a password for you. You receive an email with a single-use link and set your own.

Subject: You're invited to Acme Retail India Pvt. Ltd. on Nyvika
From: Acme Retail India Pvt. Ltd. via Nyvika

Hello Ananya Sharma,

You have been invited to Acme Retail India Pvt. Ltd.'s privacy compliance console on Nyvika, as Data Protection Officer.

Set your password and sign in here (the link works once, for 7 days):
<https://nyvika.example.com/invite/...>

If you weren't expecting this, you can ignore this email.

- 1 Open the link. The page greets you by name and shows your organisation and role.
- 2 Choose a password and type it twice. It needs at least 10 characters, can't be a commonly used password and can't be your email address. A few unrelated words make a strong, memorable password.
- 3 Select **Set password and sign in**. You land on the compliance overview.

The invitation page. If your organisation signs in with single sign-on, this page offers *Sign in with single sign-on* instead of a password.

If the link doesn't work: links expire after 7 days and work once. Ask your DPO to select **Resend** on Settings → Team (the old link stops working). For the organisation's first DPO, Nyvika's operators can send a new one.

Protect your account

Who: everyone. Strongly recommended for the DPO before anything else.

Your console account can see who consented to what and can erase people's data. A password alone is not enough protection for that. Two-factor authentication adds a 6-digit code from an app on your phone.

- 1 Select **Sign-in security** under your name at the bottom of the sidebar.
- 2 Select **Set up two-factor** and scan the QR code with an authenticator app — Google Authenticator, Microsoft Authenticator, 1Password or similar. If you can't scan, type the key shown under the code.
- 3 Enter the 6-digit code the app shows and select **Turn on**.
- 4 Save the ten recovery codes somewhere safe — a password manager, or printed and locked away. They are shown once.

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](#)

Your sign-in security

Your password and the second step that protects your console account.

Two-factor authentication

After your password, you'll enter a code from an authenticator app such as Google Authenticator, Microsoft Authenticator or 1Password.

1. Scan this with your authenticator app.

Can't scan? Enter this key instead: VHKI 4EST 4ZV6 MRZ3 B5GE Q3IY RN16 KMK7

2. Enter the 6-digit code it shows.

Authentication code

[Turn on](#) [Cancel](#)

Password

Changing it signs you out of every other browser and device.

[Change password](#)

Setting up two-factor. The code only turns on once you've proved your app works by entering a code from it.

Your sign-in security
Your password and the second step that protects your console account.

Save your recovery codes
If you lose your phone, each of these lets you sign in once. They won't be shown again — keep them in your password manager or somewhere safe offline.

tquc-cbqn	6dwj-cyuJ
v4gz-p26u	v5bk-3zq6
gath-x7hb	mm8r-23y4
erpz-cdt5	y758-htnf
tjca-f56b	uj5f-c7ex

[Copy codes](#) [I've saved them](#)

Password
Changing it signs you out of every other browser and device.

[Change password](#)

Data Fiduciary
Acme Retail India Pvt. Ltd.

Ananya Sharma
Data Protection Officer
[Sign out](#)
[Sign-in security](#)

Recovery codes. Each lets you sign in once without your phone. The same page lets you change your password (which signs you out everywhere else), create new recovery codes or turn two-factor off.

Sign in to the console
For the Data Protection Office and privacy team.

Enter the 6-digit code from your authenticator app.

Authentication code
123 456

[Verify](#)

[Use a recovery code](#) [Back](#)

Consent ledger · Rights helpdesk · PII discovery · Breach register · DPAA

Signing in from now on: password, then the code from your app — or *Use a recovery code*.

Forgot your password?
We'll email you a link to choose a new one.

Work email

[Email me a link](#)

[Back to sign in](#)

Consent ledger · Rights helpdesk · PII discovery · Breach register · DPAA

Forgot password? on the sign-in page emails a link that works once, for an hour.

BUILT IN

- Each code works once; a code seen by someone over your shoulder is useless to them.
- Resetting a forgotten password signs you out on every device, and two-factor still applies at the next sign-in.
- The forgotten-password page gives the same answer whether or not an address has an account.
- Sessions last 8 hours. Every sign-in is written to the audit log, including how it was made.

LOST YOUR PHONE?

Sign in with a recovery code, then set two-factor up again on your new phone. If you have no codes left, the DPO can reset your two-factor from Settings → Security; you'll set it up again at your next sign-in.

Your overview and the setup checklist

Who: everyone sees it; the DPO works through it.

The compliance overview is where every working day starts. In a new organisation it opens with a checklist of five things to do before Nyvika can protect anyone.

Nyvika

Compliance overview

Consent under DPDP s.6, rights requests, breaches, processors and notices — with an overall health score and what needs attention now. Updated 30 Sept, 05:31 pm IST

Finish setting up Acme Retail India Pvt. Ltd. 0 of 5 done

Until these are done, the health score below only reflects an empty record — it doesn't mean you're compliant yet.

- Add your Grievance Officer and DPO contacts**
Published in your notice, as s.8(9), s.8(10) and Rule 9 require. [Add contacts](#)
- Define why you collect personal data**
One purpose per reason, with the data it needs and how long you keep it. [Add purposes](#)
- Publish your privacy notice**
Built from your purposes; people see it before they consent (s.5). [Review and publish](#)
- Register the processors that handle data for you**
CRMs, email tools, payment providers — so withdrawals and erasures reach them. [Add processors](#)
- Start recording consent on your website**
Create a publishable key and add the consent widget; the first recorded consent completes this. [Get a key](#)

Compliance health score

100 / 100
Healthy

Metric	Progress	Status
DSR deadlines met · 25%	0 overdue · 0/0 on track (90 days)	100
Data minimisation · 20%	0 of 0 stores hold more PII than their purpose needs	100
Consents on notice v1 · 15%	0 active consents on an older notice	100
Processor sync delivered · 15%	0 failed of 0 webhook deliveries (30 days)	100
Processors under contract · 15%	0 of 0 processors lack a valid processing agreement	100
Breaches reported within 72h · 10%	No incidents in 12 months	100

Needs attention
Legal clocks and open gaps, most urgent first

Nothing outstanding

Left sidebar:

- CONSENT
 - Purposes
 - Processes
 - Notice & banner
 - Consent records
 - Cookies
- RIGHTS
 - Requests & grievances
- DATA
 - PII inventory
 - Data flows
 - Processors
 - Retention
 - Impact assessments
- INCIDENTS
 - Breaches
- GOVERNANCE
 - Reports

User info: Data Fiduciary: Acme Retail India Pvt. Ltd. | Ananya Sharma, Data Protection Officer | [Sign out](#) | [Sign-in security](#)

A new organisation. Each step links to the screen where it's done and ticks itself off as you go.

WATCH OUT

Below the checklist, the health score reads 100 because nothing has gone wrong yet — there is nothing recorded at all. The checklist says so until setup is complete; don't quote the score before then.

The five steps are covered in the chapters that follow. Registering processors comes before publishing, so the notice can say whom data is shared with:

Checklist step	Done when	Chapter
Add your Grievance Officer and DPO contacts	Both email addresses are saved	4
Define why you collect personal data	At least one active purpose	5
Publish your privacy notice	Notice v1 is published	7
Register the processors that handle data for you	At least one processor	6
Start recording consent on your website	The first consent arrives from your site	11

Organisation details

Who: DPO.

These contacts appear on your privacy notice and in the Privacy Centre, so people know whom to ask about their data.

- 1 Go to **Settings** → **Organisation**.
- 2 Enter the Grievance Officer's and the DPO's names and business email addresses. Use role mailboxes (such as `grievance@`) rather than personal ones if you can, so they survive staff changes.
- 3 Enter your **Privacy Centre URL**: the web address of the hosted Privacy Centre (Chapter 11), or your own privacy page.
- 4 Choose which processor connections are switched on (Chapter 10), then save.

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](#)

Settings

Who your principals can contact, who can use the console, how your systems connect, and the record of everything done here.

Organisation Team Security API keys Integrations Processor sync Notifications Audit log

Data Fiduciary
Acme Retail India Pvt. Ltd.
shop.acme-retail.example · notice v1 is live

Contacts on the notice
Every notice must say whom to contact about a grievance and, for a Significant Data Fiduciary, the DPO (s.5(1), s.8(9), Rule 9). These are printed on the banner and the rights portal. [Changes are published with the next notice version.](#)

Grievance officer name: Grievance officer email:

Data Protection Officer name: Data Protection Officer email:

Rights portal URL:

Processor sync
When a principal withdraws consent or has data erased, processors must stop too (s.8(7), s.6(6)). Enabled integrations receive each change as a signed webhook; see [delivery log](#).

HubSpot
Withdrawals and erasures are pushed to HubSpot so marketing stops at once. ☒ On

Salesforce
Withdrawals and erasures are pushed to Salesforce CRM. ☒ On

Settings → **Organisation**. Contacts are part of the notice: after changing them, publish a new notice version so people see the new details.

DPDP · S.8(9), S.8(10), S.5(1) · RULE 9

A Data Fiduciary must publish the business contact information of its Data Protection Officer, if it has one, or of a person who can answer questions about its processing, and must run an effective grievance mechanism. The notice must say how to exercise rights and how to complain to the Board.

Define your purposes

Who: DPO or Privacy Analyst.

A purpose is one reason you process personal data. Consent is asked for, recorded and withdrawn per purpose, so a customer can agree to order delivery without agreeing to marketing.

- 1 Go to **Purposes** and select **Add purpose**.
- 2 **Code:** a short identifier such as `MARKETING`. Your developers use it; it can't be changed later.
- 3 **Legal basis:** *Consent* (s.6) for most purposes — the notice shows an On/Off switch that starts Off. Choose *Legitimate use* (s.7) only where the law allows processing without consent, such as keeping tax records; it's disclosed on the notice, without a switch.
- 4 **Personal data used:** tick only the categories this purpose really needs. This list is shown on the notice and is also the data-minimisation rule: discovery flags any system tagged with this purpose that holds more.
- 5 **Retention (days):** how long you keep the data once the purpose is served or consent is withdrawn. Nyvika uses this to propose deletions (Chapter 24).
- 6 **Wording:** a name and a plain-language description in English. Add translations for the languages your customers use — any of the 22 languages of the Eighth Schedule. Customers can then read the notice in them.
- 7 Select **Add purpose**. Repeat for each reason.

DPDP · S.6(1), S.5, S.8(7)

Consent must be free, specific, informed, unconditional and unambiguous, limited to the data necessary for the specified purpose. Data must be erased once the purpose is no longer served or consent is withdrawn, unless the law requires keeping it.

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

Purpose register

Every purpose you process personal data for, its lawful basis, the data it needs and how long you keep it. DPDP s.6(1) requires consent to be specific to each purpose, so each one here gets its own switch on the notice.

Active purposes

4

0 retired

Consent-based (s.6)

3

shown with an On/Off switch

Legitimate use (s.7)

1

disclosed, no switch

Notice languages

2

English plus translations

4 changes waiting to be published.

Principals keep seeing notice (none yet) until v1 is published.

Review in Notice & banner →

New purpose

Changes are saved to the register now and reach principals when you publish the next notice version.

Code

LOYALTY_PROGRAMME

Upper snake case. Used by your API calls and in every consent artifact; it can't be changed later.

Retention (days)

365

About 1.0 years. Data is erased when the purpose is served or consent is withdrawn, s.8(7).

Legal basis

Consent · s.6

s.6 — the principal chooses. The notice shows an On/Off switch that starts Off, and they can withdraw at any time.

Legitimate use · s.7

s.7 — permitted without consent (e.g. a legal obligation such as tax records). Disclosed on the notice, but no consent switch is shown.

Personal data used

Listed on the notice, and also the data-minimisation allow-list: discovery flags any store tagged with this purpose that holds categories not ticked here.

☐ Aadhaar

critical

☐ Card number

critical

☐ PAN

high

☐ Passport

high

☐ Voter ID (EPIC)

high

☐ Bank account

high

☐ Phone

medium

☐ Email

medium

☐ UPI ID

medium

☐ Date of birth

medium

☐ Address

medium

☐ Name

low

☐ IP address

low

Wording shown to principals

s.5(3): principals may read the notice in English or any Eighth Schedule language. English is required; any language you add here becomes selectable on the notice.

English required

+ Add language ▾

Name (English)

Loyalty programme

Description (English)

What you do with the data and why, in plain words.

0/600

Wording for specific channels (optional)

Give a channel its own wording — a script read out on an IVR call, a short text for a kiosk. People on that channel see it in their language; where there is none, they see the wording above. Frozen with each published notice version.

Channel

Language

IVR (phone menu) ▾

English ▾

Add wording

Add purpose

Cancel

Purposes

Edit a purpose to change its wording, data or retention.

Purpose	Legal basis	Data categories	Retention	Processors	Languages	Status	Actions
Account & orders CORE_SERVICE To create and run your account, process payments and deliver...	Consent · s.6	Name Email Phone Address Date of birth UPI ID PAN Bank account IP address	3 yr	Not shared	English, Hindi	Active	Edit Retire
Product analytics ANALYTICS To understand how our website and app are used so we can...	Consent · s.6	IP address	1 yr	Not shared	English, Hindi	Active	Edit Retire
Offers & newsletters MARKETING To send you offers, new arrivals and newsletters by email, SMS...	Consent · s.6	Name Email Phone	2 yr	Not shared	English, Hindi	Active	Edit Retire
Tax & legal records LEGAL_COMPLIANCE To keep invoices and transaction records for 8 year...	Legitimate use · s.7	Name Address Phone PAN	8 yr	Not shared	English, Hindi	Active	Edit Retire

A new purpose. Each choice is explained on the form.

Nyvika · Guide for Data Fiduciaries

11 / 65

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

Purpose register

Every purpose you process personal data for, its lawful basis, the data it needs and how long you keep it. DPDP s.6(1) requires consent to be specific to each purpose, so each one here gets its own switch on the notice.

Active purposes

4

0 retired

Consent-based (s.6)

3

shown with an On/Off switch

Legitimate use (s.7)

1

disclosed, no switch

Notice languages

2

English plus translations

4 changes waiting to be published. Principals keep seeing notice (none yet) until v1 is published.

Review in Notice & banner →

Purposes

Edit a purpose to change its wording, data or retention.

New purpose

Purpose	Legal basis	Data categories	Retention	Processors	Languages	Status	Actions
Account & orders CORE_SERVICE To create and run your account, process payments and deliver...	Consent · s.6	Name Email Phone Address Date of birth UPI ID PAN Bank account IP address	3 yr	Not shared	English, Hindi	Active	Edit Retire
Product analytics ANALYTICS To understand how our website and app are used so we can...	Consent · s.6	IP address	1 yr	Not shared	English, Hindi	Active	Edit Retire
Offers & newsletters MARKETING To send you offers, new arrivals and newsletters by email, SMS...	Consent · s.6	Name Email Phone	2 yr	Not shared	English, Hindi	Active	Edit Retire
Tax & legal records LEGAL_COMPLIANCE To keep invoices and...	Legitimate use · s.7	Name Address Phone PAN	8 yr	Not shared	English, Hindi	Active	Edit Retire

Acme's purpose register after day one: account and orders, analytics and marketing by consent; legal compliance as a legitimate use. Hindi wording was added for each.

TIP · WRITING GOOD PURPOSES

- One reason per purpose. "Marketing and analytics" is two purposes; bundling them is not specific consent.
- Describe what you do in words a customer understands: "Offers and news by email and SMS", not "CRM engagement".
- Retire a purpose you no longer use instead of deleting it; the history of what people agreed to stays intact.

Wording for specific channels (optional)

If you ask for consent on more than a website — a phone menu, a kiosk, a call centre — each purpose can have wording written for that channel. On an IVR call, for example, the notice has to work when read aloud.

- 1 Edit the purpose and find **Wording for specific channels**.
- 2 Choose the channel and language, select **Add wording**, and write the name and description as they should be shown or read out.
- 3 Save. The channel wording is published with the next notice version, like any other change.

Nyvika · Guide for Data Fiduciaries

12 / 65

Wording for specific channels (optional)
Give a channel its own wording — a script read out on an IVR call, a short text for a kiosk. People on that channel see it in their language; where there is none, they see the wording above. Frozen with each published notice version.

IVR (phone menu) · English

Channel: IVR (phone menu) Language: English [Edit](#)

IVR (phone menu) · English

Name: Offers by phone

Description: Press 1 to hear our offers and news on this call. Press 2 to skip.

[Remove this wording](#)

An IVR script for the offers purpose. People on that channel get this wording in their language; where there is none, they get the purpose's normal wording in their language — the language always comes first.

Business processes (optional)

A business process is one journey that asks for consent — your app's sign-up screen, home delivery, a loyalty programme — with the purposes it presents, in order. Apps then ask for "their" screen, and each consent records which journey it came from.

- 1 Go to **Processes** (under Consent) and select **Add process**.
- 2 Give it a code (such as `APP_SIGNUP`), a name, the owning team and the channels it runs on.
- 3 Add its purposes and put them in the order the screen shows them.

- 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 out](#)
[Sign-in security](#)

Business processes

The journeys that ask for consent — an app's sign-up, home delivery, a loyalty programme — and the purposes each one presents, in order. Apps request their process by name (or a label on their API key), so every screen shows exactly the right purposes.

Processes
Consent recorded through a process carries its code, in the tamper-evident record. Route API keys to processes under [Settings](#) → [API keys](#).
[Add process](#)

Added App sign-up.

Process	Purposes, in order	Channels	Consents, 30 days	Status	Actions
App sign-up APP_SIGNUP · Digital The sign-up screen of the Acme app	1. Account & orders 2. Offers & newsletters 3. Product analytics	Mobile app	0	Active Updated 30 Sept, 05:32 pm	Edit Retire

Processes, with each journey's purposes in order and how many consents came through it in the last 30 days. Retire a process when the journey is withdrawn; consents already given keep it.

Register your processors

Who: DPO or Privacy Analyst.

Processors are the companies that handle personal data on your behalf. The register drives the "Shared with" line on your notice and decides who is told when someone withdraws consent or asks to be erased.

- 1 Go to **Processors** and add each one: name, the service it provides, category and the country (and region) where it processes data.
- 2 Link it to the **purposes** it serves and tick the **data categories** it receives.
- 3 Record the **data processing agreement**: signed (with dates), pending or none; and the result of your security review.
- 4 For processors Nyvika has a connector for, set the integration so Nyvika can instruct them directly (Chapter 10).

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: 0 (none expired)

Outside India: 3 (Germany, United States)

Register

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

Processor - sync	Location	Purposes	Data received	Processing agreement	Security review	Risk	
Razorpay Payment gateway Payments Manual sync	India ap-south-1	Account & orders	Name Email Phone UPI ID Card number	Signed no expiry date	Not started	High 60	why Edit
Mixpanel Product analytics Analytics Manual sync	Germany eu-central-1 → Cross-border	Product analytics	IP address Email	Awaiting signature	Not started	High 58	why Edit
Delhivery Last-mile delivery Logistics Manual sync	India	Account & orders	Name Phone Address	No agreement	Not started	High 54	why Edit
Salesforce Customer relationship management CRM	United States → Cross-border	Account & orders Offers & newsletters	Name Email Phone Address	Signed no expiry date	Not started	Medium 40	why Edit

The **processor register**, sorted by risk. Each risk badge explains itself: missing agreements, sensitive data and processing outside India raise it.

DPDP · S.8(2), S.16

A Data Fiduciary may engage a processor only under a valid contract. Transfers outside India are allowed except to countries the government restricts, so the register records each processor's location.

Processors without a signed agreement appear on the overview's attention list and lower the health score until you record one. That's intended: it is a gap the Board could ask about.

Publish your privacy notice

Who: DPO or Privacy Analyst drafts; only the DPO publishes.

You don't write the notice from scratch. Nyvika builds it from your purposes, processors and contacts; you review it and publish it as a numbered version. The published version is exactly what people consent to.

- 1 Go to **Notice & banner**. The draft shows what the next version will contain and what changed since the current one.
- 2 Read it in each language you added. Fix wording in **Purposes**; the draft updates.
- 3 Write a **change summary** (kept with the version as the record of why it changed).
- 4 For later versions, decide whether to **require re-consent** (see below). For the first version there is no one to ask.
- 5 Select publish, read the confirmation and confirm.

DPDP · S.5, S.6(10) · RULE 3

Every consent request comes with a notice itemising the data and purposes, how to withdraw and exercise rights, and how to complain to the Board, in English or any Eighth Schedule language. The fiduciary must be able to prove the notice was given: Nyvika records its version and language with every consent.

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 out

Sign-in security

Notice & banner

The privacy notice principals see before they consent (DPDP s.5): what data, for which purpose, how to withdraw and how to complain. Edits to purposes become a draft; publishing makes it the new version.

No notice has been published yet. The widget shows nothing until you publish.

Consents on older versions
0
active consents given before the current version

Pending changes

What the purpose register and organisation settings would change compared with nothing published yet.

First notice version

Publish v1

Change summary
e.g. Added personalised recommendations as a new optional purpose

Kept with the version as the record of why the notice changed.

Require re-consent

☐ Principals whose consent predates v1 are asked again on their next visit. Use it when a change affects what they agreed to (new data, new processors, a changed purpose).

Publish v1...

Live preview

Try the banner exactly as a principal would. Nothing is recorded from the preview.

Draft v1

Bottom bar

Centred modal

English

Any channel (plain wording)

https://shop.acme-retail.example/

Your privacy choices

LanguageEnglish

Acme Retail India Pvt. Ltd. processes your personal data only for the purposes below, each with your separate consent. Nothing is switched on until you choose.

Account & orders

To create and run your account, process payments and deliver your orders.

Data used: Name, Email, Phone, Address, Date of birth, UPI ID, PAN, Bank account, IP address · Kept for: 1095 days

Shared with: Salesforce, Zendesk, Razorpay, Delhivery

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

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, Salesforce

Reject all

Save my choices

Accept all

You can withdraw any consent at any time, as easily as you gave it, from the preference centre.
If you are not satisfied with how we handle your data, you may complain to our grievance officer, and then to the Data Protection Board of India. Rahul Verma · grievance@acme-retail.example
Notice version v1

What gets sent

Make a choice on the banner to see the API call the widget would make.

- The identifier (email or phone) is hashed with a tenant key on arrival; the raw value is never stored.
- Legitimate-use purposes are never sent: they need no consent (s.7).
- This is the unpublished draft. Until v1 is published, live decisions are recorded against no version.

Nyvika · Guide for Data Fiduciaries

16 / 65

Embed code

Add the widget to your website. It always renders the current published notice, so publishing a new version needs no code change. [See it live on the demo store](#) →

Replace nv_pk_... with your full publishable key. Keys are stored hashed and shown only once, when created in Settings → API keys.

1. Install

Before </body> on every page. Shows the cookie banner.

```
<script src="http://localhost:3000/widget/nyvika.js" defer></script>
<script>
  window.addEventListener("load", () => {
    Nyvika.init({ apiUrl: "http://localhost:8000", publishableKey: "nv_pk_...", language: "en" });
    Nyvika.cookieBanner();
  });
</script>
```

2. Capture purpose consent

Renders one Off-by-default switch per purpose.

```
// Show the purpose notice inside a sign-up or checkout form...
const notice = Nyvika.renderNotice(document.getElementById("consent"));

// ...and record the choices once you know who the person is.
form.addEventListener("submit", () => {
  Nyvika.capture(emailOrPhone, notice.getGranted());
});
```

3. Ask again after a re-consent notice

Call when a known principal signs in.

```
// On sign-in: if their consent predates a notice that requires re-consent,
// the current notice is shown again and the new choices are recorded.
await Nyvika.ensureConsent(emailOrPhone);
```

4. Preference centre

Lets principals review and withdraw consent.

```
// Link from your footer or account page: withdrawal must be as easy as consent (s.6(4)).
document.getElementById("privacy-choices").addEventListener("click", () => {
  Nyvika.openPreferenceCentre();
});
```

Version history

Published versions are frozen. Each consent record points to one, so this is the evidence of what principals saw.

The first draft: pending changes, the notice preview in any language, and the publish panel.

Publish v1

Change summary

First notice: account and orders, analytics, marketing offers and legal record-keeping

Kept with the version as the record of why the notice changed.

Require re-consent

☐ Principals whose consent predates v1 are asked again on their next visit. Use it when a change affects what they agreed to (new data, new processors, a changed purpose).

⚠ Publish v1 now? It replaces no version for everyone immediately and can't be unpublished; published versions are kept as evidence.

Confirm publish v1 Cancel

Publishing needs a second click. A published version replaces the previous one immediately and can't be unpublished; old versions are kept as evidence.

If purposes have channel wording, the preview has a **channel** selector, and the list of changes names the channels whose wording changed.

When to require re-consent

Tick **Require re-consent** when a change affects what people agreed to: new data, a new processor, a changed purpose. People whose consent predates the new version are asked again on their next visit (Chapter 18). Wording fixes and new translations don't need it.

Invite your team

Who: DPO.

- 1 Go to **Settings** → **Team** and select **Invite member**.
- 2 Enter the person's name and work email and choose a role. The form lists what the role can do.
- 3 Select **Send invitation**. They receive the same kind of email you did (Chapter 1).

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](#)

Settings

Who your principals can contact, who can use the console, how your systems connect, and the record of everything done here.

Organisation **Team** Security API keys Integrations Processor sync Notifications Audit log

Invite a team member

They get an email with a link to set their own password. Give people the least access their job needs.

Name: Work email:

Role:

View everything, change nothing

[Send invitation](#) [Cancel](#)

Team

Every action in the console is attributed to one of these people in the audit log.

Meera Iyer's invitation (Privacy Analyst) was emailed to meera.iyer@acme-retail.example. The link works once, until 7 Oct, 05:32 pm.

Member	Role	Last sign-in	Status	Access
Ananya Sharma (you) ananya@acme-retail.example	Data Protection Officer Handle rights requests & grievances · Edit purposes, scans, processors, DPIAs & cookies · Publish notice versions · Report & manage breaches · Approve or reject DPIAs · Manage team, API keys & organisation	30 Sept, 05:32 pm	Active	You can't remove your own access
Meera Iyer meera.iyer@acme-retail.example	Privacy Analyst Edit purposes, scans, processors, DPIAs & cookies	Never	Invited Link valid until 7 Oct, 05:32 pm	Resend Cancel invitation

Inviting a colleague. Choose the least access their job needs.

- 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 out](#)
[Sign-in security](#)

Settings

Who your principals can contact, who can use the console, how your systems connect, and the record of everything done here.

- Organisation
- Team**
- Security
- API keys
- Integrations
- Processor sync
- Notifications
- Audit log

Team

Every action in the console is attributed to one of these people in the audit log.

Vikram Rao's invitation (Viewer) was emailed to vikram.rao@acme-retail.example. The link works once, until 7 Oct, 05:32 pm.

Member	Role	Last sign-in	Status	Access
Ananya Sharma (you) ananya@acme-retail.example	Data Protection Officer Handle rights requests & grievances · Edit purposes, scans, processors, DPIAs & cookies · Publish notice versions · Report & manage breaches · Approve or reject DPIAs · Manage team, API keys & organisation	30 Sept, 05:32 pm	Active	You can't remove your own access
Meera Iyer meera.iyer@acme-retail.example	Privacy Analyst Edit purposes, scans, processors, DPIAs & cookies	Never	Invited Link valid until 7 Oct, 05:32 pm	Resend Cancel invitation
Vikram Rao vikram.rao@acme-retail.example	Viewer View only	Never	Invited Link valid until 7 Oct, 05:32 pm	Resend Cancel invitation

What each role can do

Data Protection Officer
Handle rights requests & grievances
Edit purposes, scans, processors, DPIAs & cookies
Publish notice versions
Report & manage breaches
Approve or reject DPIAs
Manage team, API keys & organisation

Grievance Officer
Handle rights requests & grievances
Report & manage breaches

Privacy Analyst
Edit purposes, scans, processors, DPIAs & cookies

Viewer
View everything, change nothing

Pending invitations show as *Invited* with the link's expiry. **Resend** sends a new link (the old one stops working); **Cancel invitation** withdraws it. Once someone signs in, they show as *Active*.

IF EMAIL ISN'T WORKING YET

Nyvika shows the invitation link on screen instead, so you can pass it on yourself. Send it privately: whoever opens it first can set the password.

Later, change someone's role from the same table, or **Deactivate** them when they leave: they are signed out at once and can't sign in again, and their past actions stay in the audit log. You can't remove your own DPO access, so an organisation always has one.

Nyvika · Guide for Data Fiduciaries

19 / 65

Secure the console

Who: DPO.

Once everyone has been invited, make two-factor mandatory and, if your company has one, connect your identity provider.

Settings
Who your principals can contact, who can use the console, how your systems connect, and the record of everything done here.

Organisation Team **Security** API keys Integrations Processor sync Notifications Audit log

Two-factor authentication Required
Everyone sets up their own authenticator app under your [sign-in security](#). Requiring it stops anyone who hasn't from using the console until they do. People signing in through single sign-on are covered by your identity provider instead.

☒ Require two-factor authentication for everyone in Acme Retail India Pvt. Ltd.
Two-factor is now required. 2 members will be asked to set it up the next time they use the console.

Member	Role	Two-factor
Ananya Sharma ananya@acme-retail.example	Data Protection Officer	On
Meera Iyer meera.iyer@acme-retail.example	Privacy Analyst	Not set up
Vikram Rao vikram.rao@acme-retail.example	Viewer	Not set up

Single sign-on (OpenID Connect) Not set up
Let your team sign in with Microsoft Entra ID, Google Workspace, Okta or any OpenID Connect provider. People are matched to their console account by email, so add them under Team first. Register this redirect URI with your provider: `http://localhost:3000/auth/sso/callback`

Issuer URL

Client ID Client secret

Email domains

Addresses at these domains can use single sign-on, and the provider must confirm one of them.

☐ Require single sign-on for these domains
Passwords stop working for them. The Data Protection Officer can still sign in with a password and two-factor, so a provider outage can't lock you out.

[Set up single sign-on](#)

Settings → **Security**. Who has two-factor, the organisation-wide requirement, and single sign-on.

Require two-factor for everyone

Tick **Require two-factor authentication**. Anyone without it is taken to their sign-in security page and can't use the rest of the console until they set it up. You can only switch this on from a session that itself used two-factor, so you can't lock yourself out.

Single sign-on (OpenID Connect or SAML 2.0)

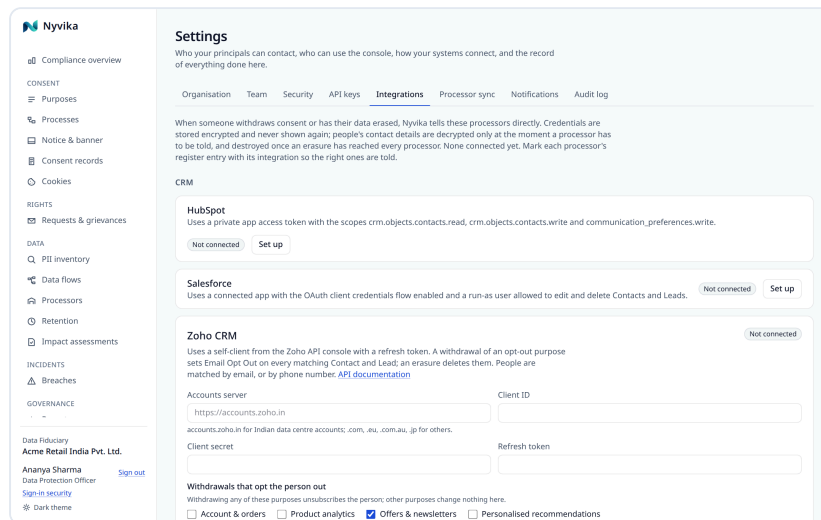
- 1 Choose the protocol your identity provider offers. **OpenID Connect:** register a web application with the redirect URI shown on the page and enter the provider's **issuer URL**, **client ID** and **client secret**. **SAML 2.0:** register a SAML application with the ACS URL and entity ID shown on the page (NameID format: email address), then enter the provider's **sign-on URL** and paste its **signing certificate**.
- 2 Enter your company's **email domains**. Nyvika checks it can reach the provider (or read the certificate) when you save.
- 3 Try it: sign out and choose **Sign in with single sign-on** on the sign-in page.
- 4 Optionally tick **Require single sign-on**: passwords stop working for those domains.

Single sign-on matches people to existing console accounts by email and never creates accounts, so invite people first. Even when it's required, the DPO can still sign in with a password and two-factor, so an outage at your identity provider can't lock you out. If someone loses their phone, **Reset** next to their name clears their two-factor.

Connect your processors

Who: DPO, with the administrators of your CRM, marketing and support tools.

When someone withdraws consent or has their data erased, the law expects your processors to act on it too (s.6(6), s.8(7)(b)). Connected, Nyvika tells each processor directly, within minutes, and keeps a delivery log.



Settings → **Integrations**. Processors are grouped by kind; **Set up** opens a card that lists exactly what access to grant and what Nyvika will do.

Kind	Processors	What Nyvika does
CRM	HubSpot, Salesforce, Zoho CRM, Freshsales	Withdrawal of a marketing purpose opts the person out (unsubscribe, <i>Email Opt Out</i> , <i>Do Not Call</i>); erasure deletes their records.
Engagement platforms	WebEngage, MoEngage, CleverTap	Turns the person's email, SMS, push and WhatsApp opt-ins off; erasure deletes the profile. Tell Nyvika whether your app identifies users by email or phone.
Email marketing	Mailchimp, Brevo, SendGrid	Unsubscribes or suppresses the address; erasure deletes the contact.
WhatsApp	Gupshup, Interakt, WATI	Opts the number out so template messages stop; these providers have no profile deletion, and the log says so.
Support desks	Zendesk, Freshdesk	Nothing on withdrawal (not marketing); erasure permanently deletes the person's user record.
Payment gateways	Razorpay, PayU	No self-service erasure API: Nyvika emails a formal erasure request to the privacy contact you enter and records that it was sent.
Advertising	Google Ads (Customer Match), Meta custom audiences	Removes the person's hashed email or phone from the audience.

Kind	Processors	What Nyvika does
Your own systems	Signed webhook	Posts each withdrawal and erasure, signed with a shared secret, to a URL your developers provide; their reply is the acknowledgement.

Only processors that appear in your **Processors** register with the matching integration are told, so mark each vendor with its integration (Chapter 6). If a system isn't on the list, use the signed webhook or ask Nyvika for a connector.

BUILT IN

- Credentials are stored encrypted and never shown again; only a masked hint.
- To reach the processor, Nyvika keeps each person's email or phone in an encrypted vault, decrypts it only at the moment of sending, and destroys it once an erasure has reached every processor.
- Failed deliveries are retried automatically and listed under **Settings** → **Processor sync** (Chapter 21).

Put Nyvika on your website

Who: DPO creates the key; your web developer adds the code.

The Nyvika widget shows the cookie banner, the itemised notice at sign-up and checkout, and the preference centre. It always shows the current published notice, so publishing a new version needs no code change.

1 • Create a publishable key

- 1 Go to **Settings** → **API keys**. Choose **Publishable**, give it a label such as "Website" and create it.
- 2 Copy the key now: it is shown once. Only a hash is stored; if you lose it, revoke it and create another.

The screenshot shows the Nyvika Settings page. On the left is a sidebar with navigation links: Compliance overview, CONSENT (Purposes, Processes, Notice & banner, Consent records, Cookies), RIGHTS (Requests & grievances), DATA (PII inventory, Data flows, Processors, Retention, Impact assessments), INCIDENTS (Breaches), and GOVERNANCE (Reports). At the bottom of the sidebar, it identifies the user as Ananya Sharma, Data Protection Officer, with links for Sign out and Sign-in security.

The main content area is titled 'Settings' and includes a description: 'Who your principals can contact, who can use the console, how your systems connect, and the record of everything done here.' Below this are tabs for Organisation, Team, Security, API keys (selected), Integrations, Processor sync, Notifications, and Audit log.

Under the 'API keys' tab, there are two sections: 'Publishable' and 'Secret'. The 'Publishable' section explains it's for website widgets and apps, can only read notices and records consent, and is safe in page source. The 'Secret' section explains it's for servers, has full access to consent records and rights requests, and must never be put in a browser or app.

A yellow warning box states: 'Copy this publishable key now. It won't be shown again. Only a hash is stored. If you lose it, revoke it and create a new one.' Below this, a key is displayed: 'nv_pk_live_3d9y45hUTxKZa9kZaUvG7xj xenPNZLM7', with 'Copy' and 'I've stored it' buttons.

Below the warning box is a form to create a new key with 'Type' (set to 'Publishable') and 'Label' (set to 'Mobile app') dropdowns, and a 'Create key' button.

At the bottom is a table listing existing keys:

Label	Key	Type	Created	Status	Actions
Website and Privacy Centre	nv_pk_live_3d9y4...	Publishable	30 Sept, 05:32 pm	Active	Routing Revoke

A new publishable key. Publishable keys are safe in web pages: they can only read the notice, record consent and start a rights request, and only from your own domain. Secret keys are for your servers and must never be put in a browser or app.

2 • Add the widget

Your developer copies the snippets from **Notice & banner** → **Embed code**, which already contain your addresses:

Embed code

Add the widget to your website. It always renders the current published notice, so publishing a new version needs no code change. [See it live on the demo store](#) →

Replace `nv_pk_...` with your full publishable key. Keys are stored hashed and shown only once, when created in Settings → API keys.

1. Install

Before `</body>` on every page. Shows the cookie banner.

Copy

```
<script src="http://localhost:3000/widget/nyvika.js" defer></script>
<script>
  window.addEventListener("load", () => {
    Nyvika.init({ apiUrl: "http://localhost:8000", publishableKey: "nv_pk_...", language: "en" });
    Nyvika.cookieBanner();
  });
</script>
```

2. Capture purpose consent

Renders one Off-by-default switch per purpose.

Copy

```
// Show the purpose notice inside a sign-up or checkout form...
const notice = Nyvika.renderNotice(document.getElementById("consent"));

// ...and record the choices once you know who the person is.
form.addEventListener("submit", () => {
  Nyvika.capture(emailOrPhone, notice.getGranted());
});
```

3. Ask again after a re-consent notice

Call when a known principal signs in.

Copy

```
// On sign-in: if their consent predates a notice that requires re-consent,
// the current notice is shown again and the new choices are recorded.
await Nyvika.ensureConsent(emailOrPhone);
```

4. Preference centre

Lets principals review and withdraw consent.

Copy

```
// Link from your footer or account page: withdrawal must be as easy as consent (s.6(4)).
document.getElementById("privacy-choices").addEventListener("click", () => {
  Nyvika.openPreferenceCentre();
});
```

Embed code, shown here from a test installation; in your console the snippets contain your own Nyvika addresses and key prefix. 1 · the banner on every page; 2 · the notice with one switch per purpose in sign-up and checkout forms; 3 · asking again after a re-consent notice; 4 · a "Privacy choices" link to the preference centre.

To hold back analytics or advertising scripts until the visitor allows them, change their tag to `<script type="text/plain" data-nv-category="ANALYTICS">` (or `FUNCTIONAL`, `ADVERTISING`). The widget runs them only once that category is allowed. Unclassified cookies never load.

3 · Apps, channels and processes

Give each app or system its own publishable key. If you use business processes, open the key's **Routing** to choose its default process, other processes it may ask for, and short labels an app can send instead of codes (for example `signup-screen`).

Process routing · Mobile app

Callers using this key get their default process when they name none. They may name the default or an allowed process; labels let an app ask for a screen by its own name (e.g. checkout) without knowing process codes. Leave everything empty for a key that may use any process.

Default process

App sign-up (APP_SIGNUP)

Also allowed

No other processes yet — add them under Consent → Processes.

Labels

signup-screen

→

App sign-up

Remove

+ Add a label

Save routing

Cancel

Routing for the mobile app's key. The app asks for `signup-screen` and gets the App sign-up purposes, in order.

Your developer then tells the widget where it is running — `Nyvika.init({ ..., channel: "app", ref: "signup-screen" })` — or sends the same fields with API calls. Each consent records its channel and process, and both are part of its tamper-evident entry:

Consent records

Find what one principal agreed to, on which notice version, and the tamper-evident ledger behind it. This is the proof of consent a Data Fiduciary must be able to show (s.6(10)).

Ledger integrity
Recompute every artifact's hash and check each link to the one before it, for every principal. Any edit or deletion in the database shows up here. [Verify entire ledger](#)

Email, phone number or principal ref
 [Look up](#)

The value is hashed server-side with your organisation's key and compared with stored hashes. It is never stored, and each lookup is recorded in the audit log. [Try a demo principal](#)

Principal ref
2d32407d7922
First seen 30 Sept 2026 ✓ Ledger intact - 2 entries

Current consent
Latest decision per purpose.

Product analytics Since 30 Sept, 05:32 pm · notice v1 · en	✓ Granted
Offers & newsletters Since 30 Sept, 05:32 pm · notice v1 · en	✓ Granted

Rights requests
No requests filed.

Consent ledger
Every grant and withdrawal, newest first. Entries are append-only and hash-linked.

Product analytics Granted Notice v1 · en · via web · Mobile app · process APP_SIGNUP hash df30ddc909_8b3c links to previous 3b1175e3f9_3db3	30 Sept, 05:32 pm
Offers & newsletters Granted Notice v1 · en · via web · Mobile app · process APP_SIGNUP hash 3b1175e3f9_3db3 first entry (genesis)	30 Sept, 05:32 pm

Data Fiduciary
Acme Retail India Pvt. Ltd.

Ananya Sharma
Data Protection Officer [Sign out](#)
[Sign-in security](#)

A consent from the app in Consent records: "via web · Mobile app · process APP_SIGNUP", with the ledger intact.

WATCH OUT

Don't give a default process to the key your website or hosted Privacy Centre uses: they would show only that process's purposes. Keep routing on the app keys that need it.

4 · The Privacy Centre

The hosted Privacy Centre is where customers prove who they are with a one-time code and then see and change their consent, and make rights requests (Chapter 14). Link to it from your footer and account pages, and put its address in Settings → Organisation.

TIP · GO LIVE SAFELY

1. Add the widget to a staging copy of your site first. Sign up with a test address and check the consent appears in **Consent records**.
2. Withdraw it from the preference centre and check the withdrawal is recorded too.
3. Then deploy to your live site. The first real consent completes the last step of the setup checklist.

WATCH OUT

A publishable key only works on your organisation's own domain and its subdomains. If the banner doesn't appear on a different domain, that's why — ask Nyvika to add it.

Notifications and retention

Who: DPO.

Two last settings decide who hears from Nyvika, and what happens when data is due for deletion. The defaults are sensible; check they suit you.

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 out](#)
[Sign-in security](#)

Settings

Who your principals can contact, who can use the console, how your systems connect, and the record of everything done here.

Organisation Team Security API keys Integrations Processor sync **Notifications** Audit log

Who hears from Nyvika

- ☒ **Email requesters about their requests**
When a request is received, changes status, gets a message from your team or is completed, the person hears about it — by email, or by SMS if they gave a phone number — in English or Hindi. An erased person's confirmation is sent before their address is destroyed.
- Daily deadline digest for officers**
Each morning (9:00 IST), everyone who handles requests gets their overdue and soon-due requests — assigns their own, the DPO and grievance officers every unassigned one.
Warn 7 days before the deadline

[Save](#)

Sent	Pending	Failed
0	0	0

[All](#) [Failed](#) [Pending](#) [Sent](#) [Every kind](#) [Request updates](#) [Deadline digests](#) [Breach notices](#) [Inactivity warnings](#)

Nothing here yet.

Settings → Notifications.

- **Email requesters about their requests** (on by default): people hear when their request is received, changes status, gets a message from your team or is completed — by email, or SMS if they gave a phone number, in English or Hindi.
- **Daily deadline digest** (9:00 IST): everyone who handles requests gets their overdue and soon-due requests; the DPO and grievance officers also get every unassigned one. Choose how many days' warning, or switch it off.

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 out

Sign-in security

Retention

Personal data is kept only as long as each purpose's retention period promises (s.8(7)) — and, if you turn it on, erased after long inactivity (rule 8). Nyvika finds what is due every morning; your team approves it here.

When a deletion falls due

☒ Ask us first
The DPO or grievance officer approves each deletion below (or keeps the data, with a reason).

☐ Delete automatically
Nyvika carries out due deletions itself every morning and records each one.

Save

Check now

Erase people after long inactivity

Rule 8 and the Third Schedule: large e-commerce, gaming and social platforms erase people who haven't used their account for 3 years, warning them 48 hours before. Anything they do in that time — signing in, a consent choice, a request — cancels it.

Off

Due for deletion (0)

Deleted (0)

Kept (0)

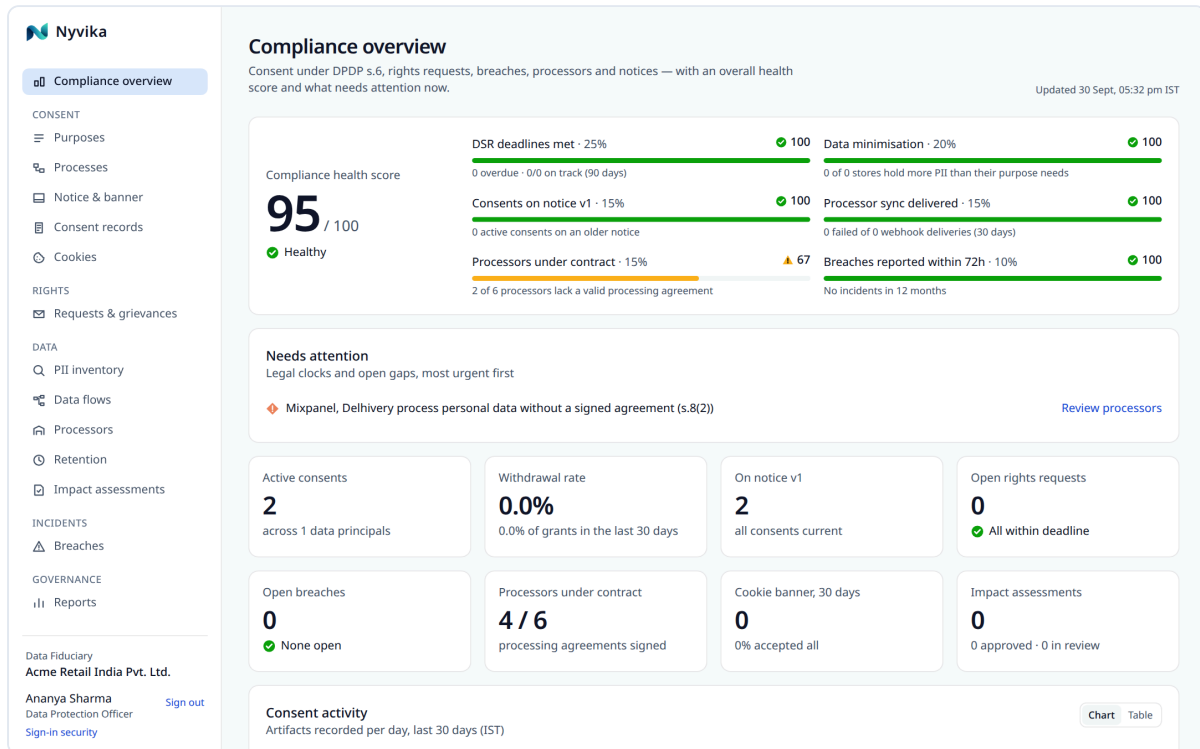
Nothing is due. Nyvika checks every morning; a deletion appears here once someone's consent for a purpose has been withdrawn for longer than that purpose's retention period (or, if turned on, after long inactivity).

Retention settings.

- **When a deletion falls due:** *Ask us first* (recommended to start) puts each deletion in a queue for the DPO or Grievance Officer to approve, or to keep with a reason. *Delete automatically* carries them out every morning and records each one.
- **Erase people after long inactivity:** for large e-commerce, gaming and social platforms under Rule 8 and the Third Schedule — 3 years. People are warned 48 hours before; anything they do in that time cancels it.

You're live

By the end of day one, Acme's checklist shows four of five steps done. The fifth ticks itself off when the website records its first consent.



The overview at the end of day one. The attention list has already found something real: two processors without signed agreements.

Day-one checklist

- ☐ Invitation accepted, two-factor on, recovery codes stored safely
- ☐ Grievance Officer and DPO contacts saved
- ☐ Every purpose added, with data categories, retention and translations
- ☐ Every processor registered, with agreement status
- ☐ Notice v1 published
- ☐ Team invited with the right roles; two-factor required
- ☐ Single sign-on set up (if you use it)
- ☐ Channel wording and business processes set up, and app keys routed (if you use them)
- ☐ Processors connected (CRM, marketing tools, support desk — whichever you use)
- ☐ Publishable key created; widget on a test site, then live
- ☐ Privacy Centre linked from your website
- ☐ Notification and retention settings reviewed

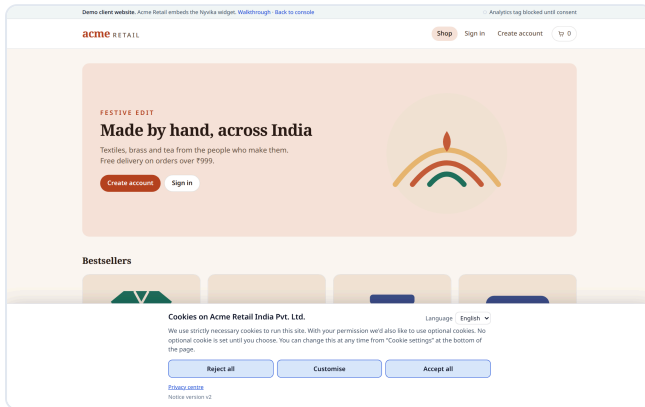
PART II

Every day: running compliance

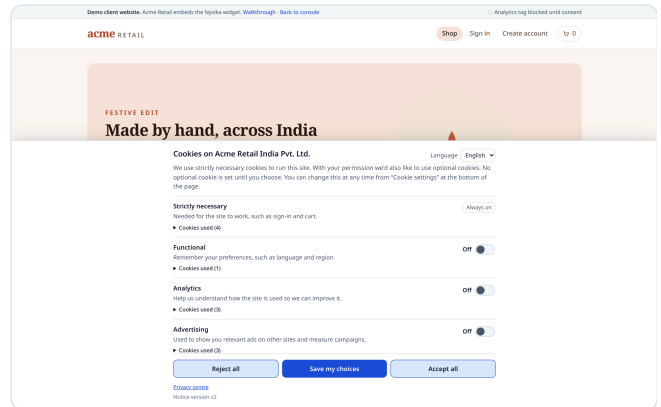
Months have passed. Thousands of Acme's customers have consented through the website, some have changed their minds, a few have asked for their data or complained, and one weekend a breach started a 72-hour clock. This part shows how each of those is handled, screen by screen.

What your customers see

It helps to know the other side of the screen. Everything here is the widget and the Privacy Centre on your website, in the customer's language.



The cookie banner. *Reject all* is as easy as *Accept all*; nothing optional loads before a choice.



Customise: one switch per category, off by default.

Demo client website. Acme Retail embeds the Nyvika widget. Walkthrough · Back to console

Analytics tag blocked until consent · cookies allowed: necessary only

acme RETAIL Shop Sign in Create account 0

Create your account

Track orders, save addresses and check out faster.

Full name

Email or mobile number

Password

Demo only: the password is never sent or stored.

Create account

Already shopping with us? [Sign in](#)

Rendered by the Nyvika widget (Nyvika.renderNotice):

Language: English

Acme Retail India Pvt. Ltd. processes your personal data only for the purposes below, each with your separate consent. Nothing is switched on until you choose.

Account & orders On

To create and run your account, process payments and deliver your orders.

Data used: Name, Email, Phone, Address, Date of birth, UPI ID, PAN, Bank account, IP address · **Kept for:** 1095 days

Shared with: Salesforce, Zendesk, Razorpay, Delhivery

Product analytics Off

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

Offers & newsletters On

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, Salesforce

Tax & legal records No consent needed

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:** 2920 days

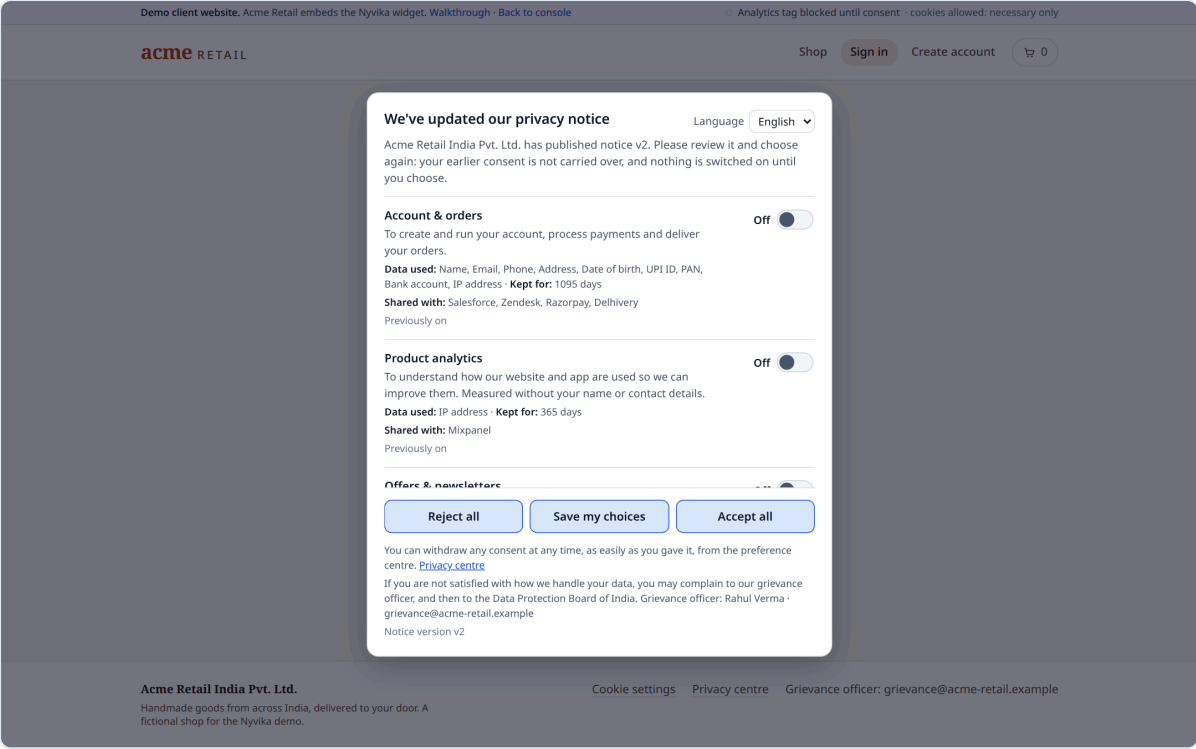
Shared with: Not shared with third parties

We process this under a legitimate use permitted by law (DPDP s.7). It's listed so you know about it.

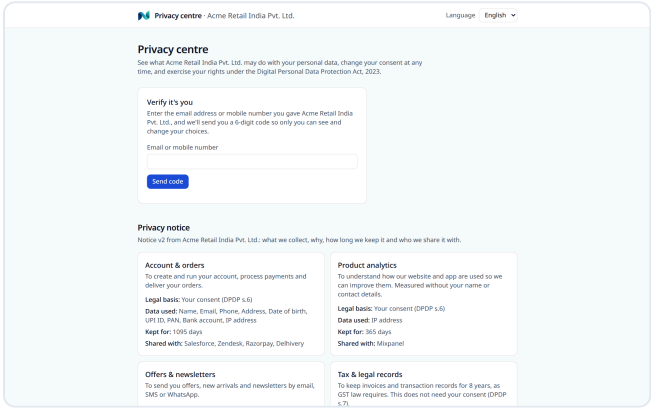
You can withdraw any consent at any time, as easily as you gave it, from the preference centre. [Privacy centre](#)

If you are not satisfied with how we handle your data, you may complain to our privacy.

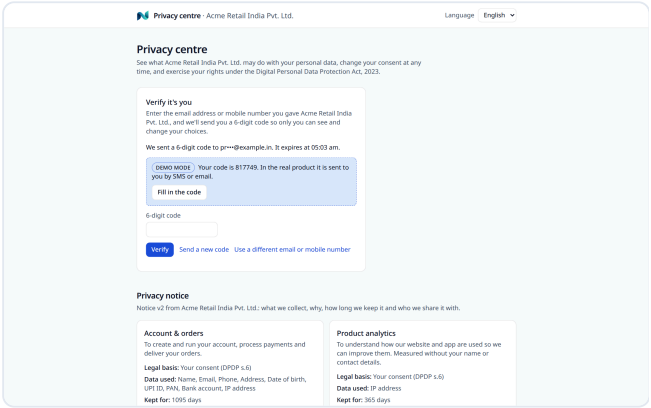
The notice at sign-up: every purpose with its own switch, the data it uses, how long it's kept and who it's shared with; legitimate uses are disclosed without a switch. Language can be changed right there.



After a notice change that requires re-consent, returning customers see what changed and choose again.



The Privacy Centre: customers enter the email or mobile number they gave you...



...and prove it's theirs with a 6-digit code sent by email or SMS. (The demo shows the code on screen.)

Privacy centre
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 63e34635d5a0

My consents My requests Make a request Privacy notice

Our privacy notice has changed
This gives 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 create and run your account, process payments and deliver your orders.
Data used: Name, Email, Phone, Address, Date of birth, UPI ID, PAN, Bank account, IP address. **Kept for:** 1095 days
Shared with: Salesforce, Zendesk, Shipping, 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: Mapbox
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: Mailchimp, Salesforce
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. No consent needed

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:** 2620 days
Shared with: Your shared with third parties

Privacy centre powered by Nyvika

Their choices: switch any purpose off; withdrawal is one click, as easy as consenting.

Privacy centre
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 63e34635d5a0

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 use it for and who we've shared it with (s.15).
Correct my data
Correct, complete or update personal data that is wrong or out of date (s.12).
Erase my data
Delete your personal data, unless a law requires us to keep it (s.12).

Nominate someone
Report someone who's got access to their rights for you, if you dare or can't act yourself (s.16).
Raise a grievance
Complain about how we have handled your personal data (s.13).

Nominate someone
Nominee's full name Relationship to you Nominee's email or phone number
Anything else? (optional)
Submit request

Their rights: access, correction, erasure, nomination or a grievance, tracked with a ticket number.

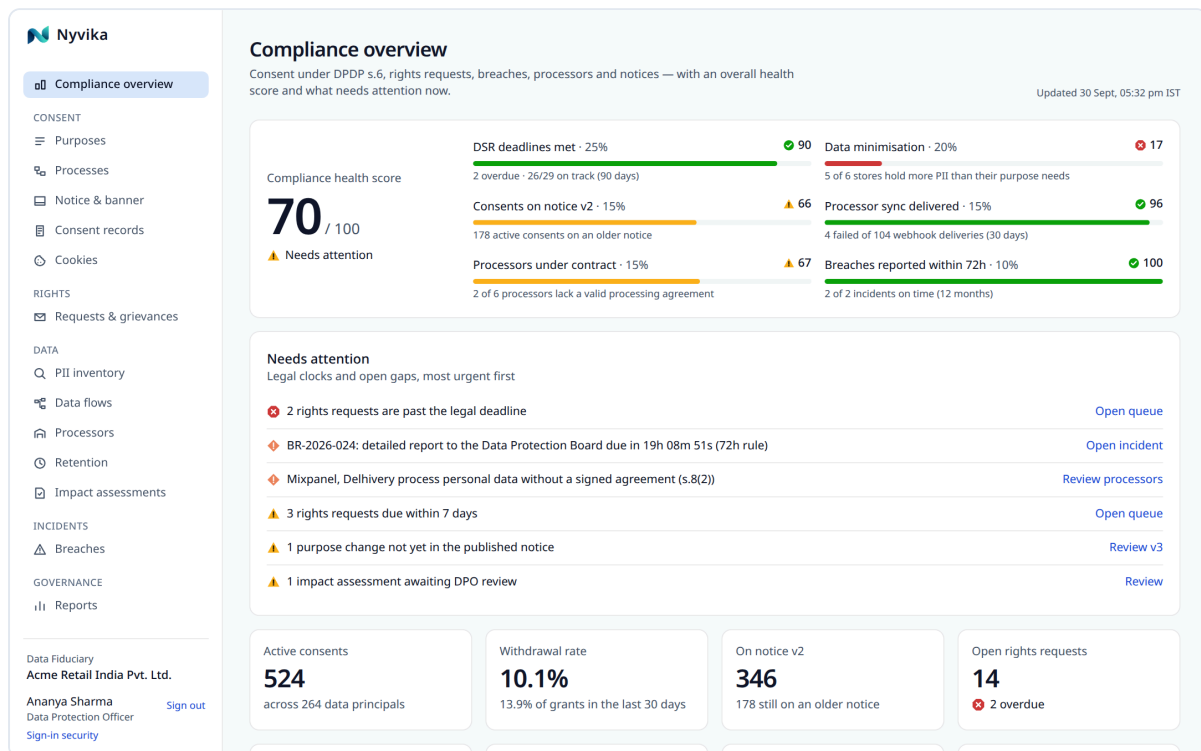
BUILT IN

- Codes are single-use, expire after 10 minutes and allow 5 attempts; at most 3 codes are sent per 10 minutes.
- A request made after signing in with a code arrives already marked *identity verified*.
- Nyvika stores people's identifiers only as keyed hashes. Readable contact details exist only in the encrypted vault used to reach processors and to send updates.

Your morning: the overview

Who: everyone; the DPO owns it.

Start the day with **Needs attention**: every legal clock that is running and every open gap, most urgent first. Each item links to where it's fixed.



A normal Monday at Acme: overdue requests, a Board report due, processors without agreements, an unpublished purpose change and a DPIA waiting for review.

The health score

One number from 0 to 100 summarises six measures. Use it for trends and board reporting; use the attention list for today's work.

Measure	Weight	What moves it
Rights deadlines met	25%	Requests in the last 90 days closed on time, or still inside their window
Data minimisation	20%	Systems holding no more personal data than their purposes need
Consents on the current notice	15%	Share of active consents given on the latest notice version
Processor sync delivered	15%	Withdrawal and erasure instructions delivered, last 30 days
Processors under contract	15%	Active processors with a signed, unexpired agreement
Breaches reported within 72 hours	10%	Incidents in the last 12 months reported to the Board in time

80 or more reads *Healthy*; 60–79 *Needs attention*; 40–59 *At risk*; below 40 *Critical*.

Rights requests and grievances

Who: Grievance Officer and DPO.

Every request from the Privacy Centre, the widget or your own channels lands in one queue, with a ticket number and a deadline clock that starts when it's filed.

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 ab8ddb5Scae8	ID verified	Privacy portal	Rahul Verma	In progress	26 Aug 2026	Overdue by 4d 22h 51m 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 51m Day 30 of 30
NV-2026-000179 Erasure · DPDP s.12(3) Principal b398b91ec740	ID not verified	Email	Unassigned	Pending	2 Sept 2026	2d 01h 08m 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 08m Day 25 of 30
NV-2026-000181 Access · DPDP s.11 Principal ac3f9218d206	ID verified	Privacy portal	Unassigned	Pending	5 Sept 2026	5d 01h 08m Day 24 of 30
NV-2026-000183 Erasure · DPDP s.12(3) Principal bca50e604749	ID verified	Privacy portal	Ananya Sharma	In progress	11 Sept 2026	11d 01h 08m Day 18 of 30
NV-2026-000184 Access · DPDP s.11	ID verified	Privacy portal	Unassigned	Pending	15 Sept 2026	15d 01h 08m

Requests & grievances. Filter by status, type and assignee. Each row shows how much of the window is used; red means overdue.

Request	The law	What you do in Nyvika
Access	s.11	Export a summary of the person's data, consents and who it was shared with
Correction	s.12	Correct the data in your systems, then fulfil with a note of what changed
Erasure	s.12(3)	Execute erasure: withdraws every consent, redacts the evidence trail and instructs every processor
Nomination	s.14	The nominee's details arrive with the request; check them and fulfil it, so the nominee can act for the person on death or incapacity
Grievance	s.13 · Rule 14(3)	Investigate and respond; must be redressed within 90 days

Working a request

- 1 Open the request and **assign** it (to yourself or a colleague).
- 2 Check **identity**. Requests made after a Privacy Centre code are verified already; otherwise record how you verified (for example, a call-back to the registered mobile). Export and erasure are refused until identity is verified.

- 3 Move it to **In progress**. Use **On hold** if you are waiting on the person — the clock keeps running.
- 4 Add **notes**: internal ones for the team, or messages the person sees in the Privacy Centre (and is told about by email or SMS).
- 5 Do the work: export, execute erasure, or correct. Access and erasure requests can only be fulfilled by actually doing them.
- 6 Close it as **Fulfilled** with a resolution note, or **Rejected** with a reason the person can take to the Board. Closed requests can't be reopened; a new request is filed instead.

- 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 out](#)
[Sign-in security](#)

Requests & grievances

NV-2026-000177
In progress
ID verified

Erasure request · DPDP s.12(3)
Erase personal data unless retention is required by law

Time to legal deadline
Overdue by 4d 22h 51m
Day 30 of 30

Deadline
25 Sept 2026
from the date of filing

Filed
26 Aug, 06:41 pm
via privacy portal

Assignee
Rahul Verma

Requester
Data Principal ab8ddb5cae8 — a keyed hash, never the raw email or phone

Identity
Identity verified by one-time passcode.

Request details
No free-text details — a standard erasure request.

Current consents

Account & orders	Granted since 20 Sept 2026
Offers & newsletters	Granted since 20 Sept 2026

Other requests from this principal
None — this is their first request.

Workflow
Assign an owner, move the request and fulfil it.

Assignee
Rahul Verma

Move this request
Put on hold Reject

Erasure requests are fulfilled by the action below, so the right is actually carried out rather than just marked done.

Right to erasure · s.12(3)
Executes the erasure across the consent ledger and every downstream processor, then closes the request.

Execute erasure

Add to the timeline

Internal note Message to the principal

Note (staff only)
Checked the order system; the DOB field is editable by support.

Add note

Timeline

Every action on this request, oldest first. Messages marked visible appear in the principal's portal.

✓ Timeline intact — 18 events verified against the hash chain

● Request filed Visible to principal
Request NV-2026-000177 received via portal. We will respond within 30 days.
Data Principal (Data Principal) · 26 Aug, 06:41 pm · #df0c89e6c5

● Identity verified Visible to principal
Identity verified by one-time passcode.
Nyvika (System) · 26 Aug, 06:43 pm · #d84da099da

● Assignment
Assigned to Rahul Verma
Ananya Sharma (Staff) · 27 Aug, 01:53 am · #4ae4c354f5

● Status changed Pending → In progress Visible to principal
Status changed to In progress.
Rahul Verma (Staff) · 27 Aug, 06:41 pm · #653f5768a4

● Internal note
Stage 1 check 1790690770763
Rahul Verma (Staff) · 29 Sept, 07:36 pm · #791ea67525

● Internal note
Stage 1 check 1790691293000
Rahul Verma (Staff) · 29 Sept, 07:44 pm · #b0951c0b68

● Internal note
Stage 1 check 1790691316494
Rahul Verma (Staff) · 29 Sept, 07:45 pm · #39eb03e7e0

● Internal note
Stage 1 check 1790691749634
Rahul Verma (Staff) · 29 Sept, 07:52 pm · #25e222c945

● Internal note
Stage 1 check 1790691827327
Rahul Verma (Staff) · 29 Sept, 07:53 pm · #f2ec735f7e

● Internal note
Stage 1 check 1790691923001
Rahul Verma (Staff) · 29 Sept, 07:55 pm · #9a7bccf886

● Internal note
Stage 1 check 1790692310864
Rahul Verma (Staff) · 29 Sept, 08:01 pm · #733daece8d

● Internal note
Stage 1 check 1790693001095
Rahul Verma (Staff) · 29 Sept, 08:13 pm · #f68950fea1

● Internal note
Stage 1 check 1790693633266
Rahul Verma (Staff) · 29 Sept, 08:23 pm · #0ceed6ccaf

● Internal note
Stage 1 check 1790694704579
Rahul Verma (Staff) · 29 Sept, 08:41 pm · #bbbd81ab4f

● Internal note
Stage 1 check 1790695724598
Rahul Verma (Staff) · 29 Sept, 08:58 pm · #ff32dee4ee

● Internal note
Stage 1 check 1790699006894
Rahul Verma (Staff) · 29 Sept, 09:53 pm · #02196a5320

● Internal note
Stage 1 check 1790745905303
Rahul Verma (Staff) · 30 Sept, 10:55 am · #d0aa9c56f4

● Internal note
Stage 1 check 1790746602352
Rahul Verma (Staff) · 30 Sept, 11:06 am · #959cb96bd6

A request. The requester panel (identity, current consents, other requests), the workflow with the fields each move needs, notes, and a tamper-evident timeline.

DEADLINES

Nyvika's default window for rights requests is 30 days, which your organisation can change; grievances must be redressed within 90 days (Rule 14(3)). The daily digest warns assignees before the deadline (Chapter 12).

Proving consent

Who: everyone can look; every lookup is logged.

When a customer says "I never agreed to that", **Consent records** answers in one screen: which purposes, on which notice version, in which language, through which channel, and when.

Consent records. Type the person's email or phone; it is compared as a hash and never stored. Each entry is chained to the one before, so any tampering is visible; *Verify entire ledger* checks every customer's chain.

Where your apps send them, each entry also shows the **channel** (such as Mobile app or IVR) and the **business process** the consent was given in — so you can show exactly which wording the person saw (Chapter 11).

DPDP · S.6(10)

Where consent is the basis for processing, the Data Fiduciary must prove that notice was given and consent obtained. This screen, and the ledger proof report (Chapter 26), is that proof.

Changing your notice

Who: Privacy Analyst or DPO edits purposes; the DPO publishes.

Business changes: a new purpose, a new processor, longer retention. Edit the register as usual; nothing reaches customers until you publish a new notice version.

- 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](#)

Notice & banner

The privacy notice principals see before they consent (DPDP s.5): what data, for which purpose, how to withdraw and how to complain. Edits to purposes become a draft; publishing makes it the new version.

Current version **Re-consent required**

v2
 Added Hindi, disclosed tax-record retention (s.7) and published grievance officer & DPO contacts
 Published 8 Sept, 06:41 pm by Ananya Sharma · 4 purposes · English, Hindi

Consents on older versions
178
 active consents given before v2; these principals are asked again on their next visit

Pending changes

What the purpose register and organisation settings would change compared with v2.

- New purpose: Personalised recommendations

Publish v3

Change summary

e.g. Added personalised recommendations as a new optional purpose

Kept with the version as the record of why the notice changed.

Require re-consent

☐ Principals whose consent predates v3 are asked again on their next visit. Use it when a change affects what they agreed to (new data, new processors, a changed purpose). 178 active consents were given on older versions.

Publish v3...

Live preview

Try the banner exactly as a principal would. Nothing is recorded from the preview.

Current v2
 Draft v3
 Bottom bar
 Centred modal
 English

https://acme-retail.example/

Your privacy choices

Acme Retail India Pvt. Ltd. processes your personal data only for the purposes below, each with your separate consent. Nothing is switched on until you choose.

Language English

Account & orders
Off

To create and run your account, process payments and deliver your orders.
 Data used: Name, Email, Phone, Address, Date of birth, UPI ID, PAN, Bank account, IP address · Kept for: 1095 days
 Shared with: Salesforce, Zendesk, Razorpay, Delhivery

Product analytics
Off

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

Offers & newsletters
Off

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, Salesforce

Reject all

Save my choices

Accept all

You can withdraw any consent at any time, as easily as you gave it, from the preference centre.
 If you are not satisfied with how we handle your data, you may complain to our grievance officer, and then to the Data Protection Board of India. Rahul Verma · grievance@acme-retail.example
 Notice version v2

What gets sent

Make a choice on the banner to see the API call the widget would make.

- The identifier (email or phone) is hashed with a tenant key on arrival; the raw value is never stored.
- Legitimate-use purposes are never sent: they need no consent (s.7).

Embed code

Add the widget to your website. It always renders the current published notice, so publishing a new version needs no code change. [See it live on the demo store →](#)

Uses this workspace's demo publishable key. Publishable keys can only capture consent and read the notice, so they are safe in page source.

1. Install

Before </body> on every page. Shows the cookie banner.

Copy

```
<script src="http://localhost:3000/widget/nyvika.js" defer></script>
<script>
  window.addEventListener("load", () => {
    Nyvika.init({ apiUrl: "http://localhost:8000", publishableKey: "nv_pk_test_demo_acme_publishable_key_000000", language: "en" });
    Nyvika.cookieBanner();
  });
</script>
```

2. Capture purpose consent

Renders one Off-by-default switch per purpose.

Copy

```
// Show the purpose notice inside a sign-up or checkout form...
const notice = Nyvika.renderNotice(document.getElementById("consent"));

// ...and record the choices once you know who the person is.
form.addEventListener("submit", () => {
  Nyvika.capture(emailOrPhone, notice.getGranted());
});
```

3. Ask again after a re-consent notice

Call when a known principal signs in.

Copy

```
// On sign-in: if their consent predates a notice that requires re-consent,
// the current notice is shown again and the new choices are recorded.
await Nyvika.ensureConsent(emailOrPhone);
```

4. Preference centre

Lets principals review and withdraw consent.

Copy

```
// Link from your footer or account page: withdrawal must be as easy as consent (s.6(4)).
document.getElementById("privacy-choices").addEventListener("click", () => {
  Nyvika.openPreferenceCentre();
});
```

Version history

Published versions are frozen. Each consent record points to one, so this is the evidence of what principals saw.

> v2 Current Re-consent required	8 Sept, 06:41 pm · Ananya Sharma · 4 purposes · English, Hindi
Added Hindi, disclosed tax-record retention (s.7) and published grievance officer & DPO contacts	
> v1	31 Jul, 06:41 pm · Ananya Sharma · 3 purposes · English
Initial notice	

A change waiting to be published. Acme has added a personalisation purpose. The page lists exactly what differs from the current version and how many active consents were given on older versions.

- 1 Review the pending changes and the preview in each language.
- 2 Write the change summary. Decide on re-consent: required when the change affects what people agreed to.
- 3 Publish. Customers with older consents are asked again on their next visit (Chapter 14); the overview tracks how many consents are still on older versions.

Breaches: the 72-hour clock

Who: Grievance Officer and DPO.

Report a suspected breach as soon as you know. The moment you record when it was detected, Nyvika starts the Rule 7 clock and lays out every step in order.



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 out

Sign-in security

Personal data breaches

Every breach must be intimated to the Data Protection Board and each affected Data Principal without delay, with a detailed report to the Board within 72 hours of becoming aware of it (DPDP s.8(6), Rule 7).

Report a breach

Open incidents

1

investigating, contained or resolved

Board reports due < 24h

1

72-hour clock running out

Overdue Board reports

0

past 72 hours, not yet filed

Closed this year

1

all Rule 7 steps completed

Incident	Severity	Status	Detected	72h Board report	Notifications
BR-2026-024 Credential-stuffing attack on customer accounts ~380 principals affected	Medium	Investigating	28 Sept, 12:41 pm	19h 08m 46s	Board intimated Report filed Principals notified
BR-2026-023 Public read access on the user-uploads bucket ~1,240 principals affected	High	Closed	1 Jun, 06:41 pm	Reported in 41h	Board intimated Report filed Principals notified

The breach register, with each incident's clock and status.

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 out

Sign-in security

Breaches

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

Medium

Investigating

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

19h 08m 06s

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

EmailPhoneAddress

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

Nyvika · Guide for Data Fiduciaries

41 / 65

Report to the Data Protection Board

Rule 7(2) — built from this incident. Fill the bracketed gaps before filing.

 Copy

REPORT OF PERSONAL DATA BREACH

To: The Data Protection Board of India
Under: Section 8(6) of the Digital Personal Data Protection Act, 2023, read with Rule 7(2) of the Digital Personal Data Protection Rules, 2025
From: Acme Retail India Pvt. Ltd. (acme-retail.example), Data Fiduciary
Incident reference: BR-2026-024
Date of this report: 30 September 2026 at 05:33 pm IST
Internal severity assessment: Medium

1. Description of the breach
Credential-stuffing attack on customer accounts
Login attempts using leaked passwords from another site succeeded on a number of customer accounts; attackers viewed saved addresses and phone numbers.

Notice to affected Data Principals

Rule 7(1) — plain language, sent to each affected principal.

 Copy

English

हिंदी

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

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

We became aware of it on 28 September 2026 at 12:41 pm IST.

What data was involved
Email, Phone, Address

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

priya.sharma@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
Login attempts using leaked passwords from another site succeeded on a number of customer accounts; attackers viewed saved addresses and phone numbers.
We became aware of it on 28 September 2026 at 12:41 pm IST.

What data was involved
Email, Phone, Address

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

⚠ Fill in the draft's gaps before sending:

- English: [Describe the steps taken to stop the breach]

Check who this reaches

Timeline

Everything recorded on this incident, newest first. Also written to the audit log.

Add note

Forensics confirmed no payment data was accessed.

Add note

- Forced password reset queued for 380 affected accounts**
Ananya Sharma · 29 Sept, 08:41 am
- Initial intimation sent to the Data Protection Board**
Ananya Sharma · 28 Sept, 03:41 pm
- Incident reported**
Rahul Verma · 28 Sept, 12:41 pm

An incident. The Board-report clock, the response checklist with timestamps, what happened, affected systems and data, cause and remediation, drafts of the Board report and the customer notice, and the timeline.

- 1 **Contain** the breach and mark it contained.
- 2 **Intimate the Board** without delay with what you know so far.
- 3 **File the detailed report** with the Board within 72 hours. Nyvika drafts it from the incident's facts; gaps are left as placeholders rather than invented.
- 4 **Notify affected people** without delay: Nyvika sends the breach notice by email or SMS to everyone it can reach, in their language. Before you send, it shows how many people will get it, and by which channel.
- 5 **Resolve** once remediation is recorded, then **close** — possible only when the Board report is filed and people are notified.

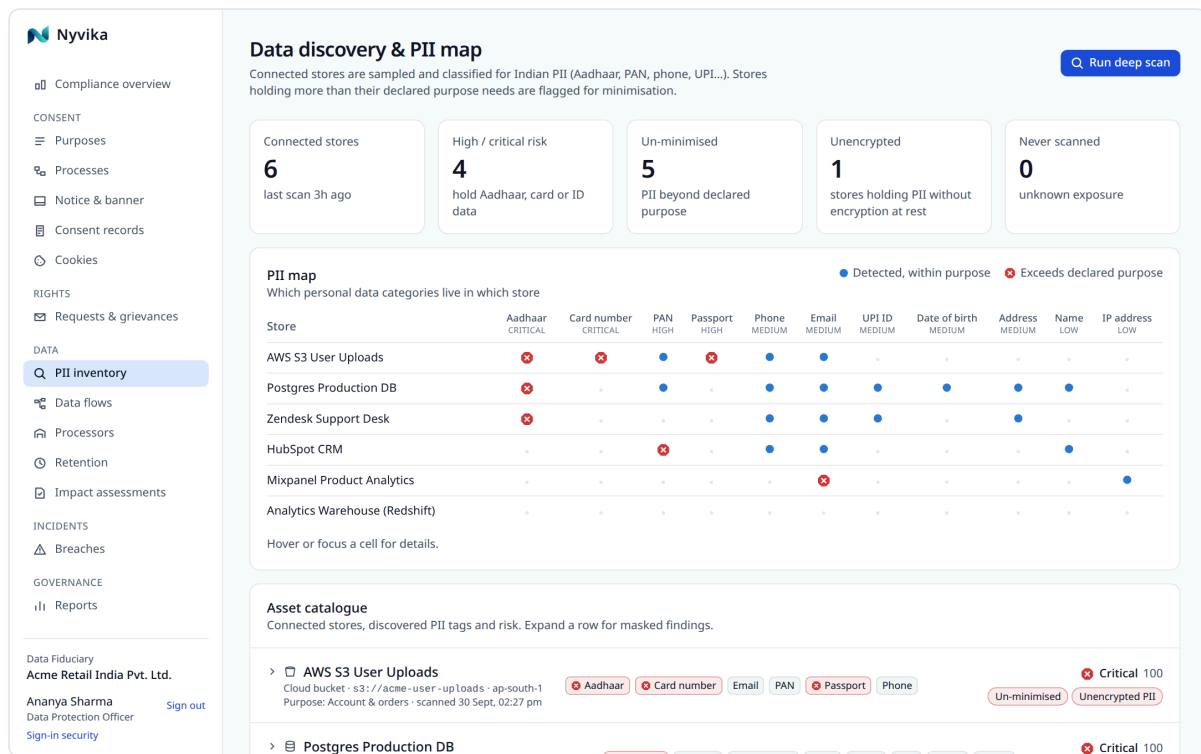
DPDP · S.8(6) · RULE 7

On becoming aware of a personal data breach, the fiduciary must intimate the Board and each affected person without delay, and file a detailed report with the Board within 72 hours covering what happened, its extent and likely impact, mitigation, the cause, remediation and the notices sent.

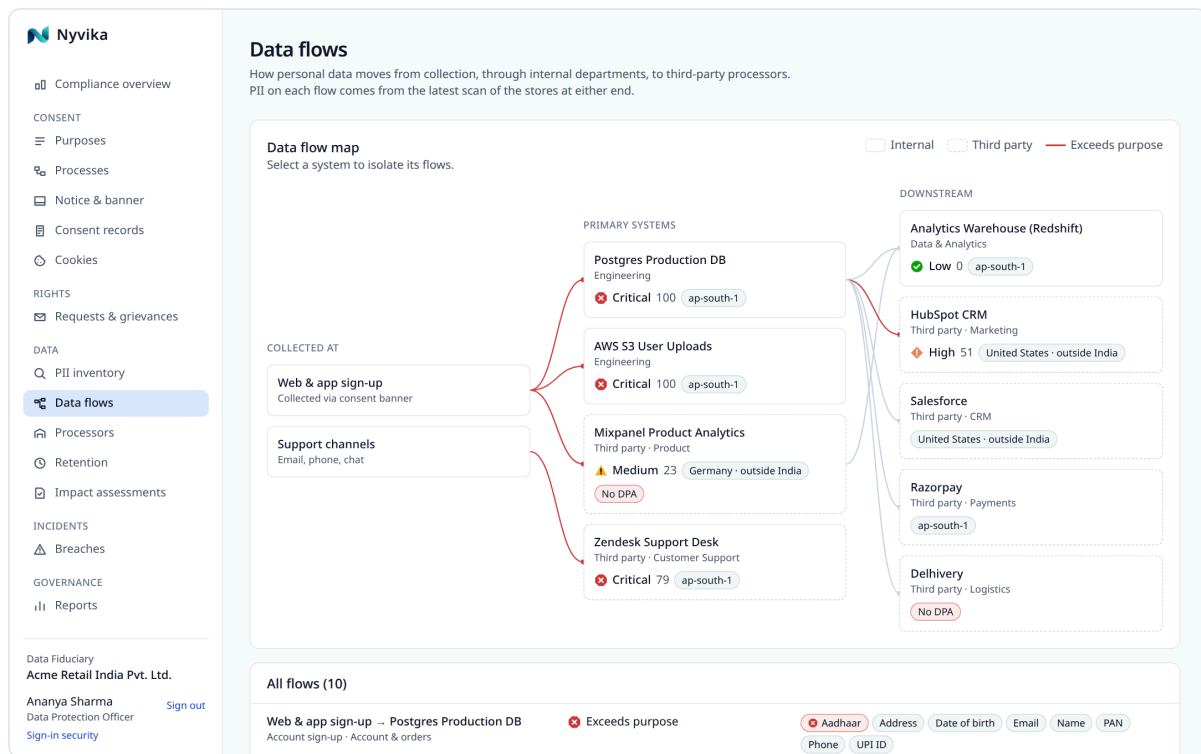
Where your data lives

Who: Privacy Analyst or DPO.

PII inventory shows which personal data each of your systems holds and flags anything beyond what its purposes need. **Data flows** shows where data goes.



PII inventory. Systems down the side, data categories across; red means data held beyond the system's purpose. Aadhaar, card and account numbers are recognised with their checksums and context, and findings are stored masked.



Data flows. Collection points, your systems, and internal and third-party recipients. Flows outside India and to processors without agreements are flagged.

Connecting a real data store

A store can be registered with or without a connection. Without one it still counts in data flows and breach impact; with read-only credentials, a scan samples it for Indian personal data. Ten kinds of store can be connected: PostgreSQL, MySQL and MongoDB databases; Amazon S3 (and S3-compatible) and Azure Blob storage; Google Drive and SharePoint or OneDrive folders; BigQuery and Snowflake warehouses; and the contacts in a CRM you have already connected under Settings → Integrations. Credentials are encrypted on arrival and never shown again. A scan reads a bounded sample (at most 200 tables, 20 rows each, 500 objects, 64 KB per document), keeps only the masked findings, and never copies your data.

If you already run a discovery or data-security tool, **Import inventory** takes its findings as CSV or JSON instead, so you don't pay for a second scanner.

How to: connect a Google Drive folder

Nyvika can't sign in to Google as you. Instead you create a *service account*, which is a robot account Google provides, share the folder with it as a viewer, and give Nyvika the robot's key file. The whole job takes about ten minutes.

Part A: create the service account (in Google Cloud, once per organisation)

- 1 Go to **console.cloud.google.com** and sign in with your Google Workspace account. In the project drop-down at the top, choose **New Project**, name it *nyvika*, create it and select it.
- 2 In the search box type *Google Drive API*, open it and select **Enable**. Without this step Google refuses the connection later.
- 3 Left menu → **APIs & Services** → **Credentials** → **+ Create credentials** → **Service account**. Name it *nyvika-discovery*, select **Create and continue**, then **Done**; no roles are needed.

- 4 Open the new service account and note its email address, which ends in `.iam.gserviceaccount.com`.
- 5 On its **Keys** tab: **Add key** → **Create new key** → **JSON** → **Create**. A file downloads. It is the robot's password: keep it private and never paste it anywhere but the Nyvika form.

Part B: share the folder (in Google Drive, per folder)

- 1 Right-click the folder → **Share**. Paste the service account's email, set it to **Viewer**, untick *Notify people*, and share.
- 2 Open the folder and copy the id from the address bar: everything after `/folders/` in `drive.google.com/drive/folders/...`. For a shared drive, use the drive's id the same way.

Part C: add the store in Nyvika (PII inventory → Add data store)

- 1 **Kind of store:** Google Drive. **Name:** what your team calls the folder; it appears in the inventory, in breach reports and in the record of processing.
- 2 **Locator:** paste the folder id after the `gdrive://` prefix.
- 3 **Declared purpose:** the purpose this folder serves. This is what the scan checks against: any category of data found that the purpose doesn't need is flagged for minimisation.
- 4 **Encrypted at rest:** attest it. Google encrypts Drive at rest.
- 5 **Service account key:** open the downloaded file in a text editor and paste its entire contents, braces included.
- 6 Select **Add store**, then **Run deep scan**. Within a minute the store shows what it found.

The screenshot shows the Nyvika web interface. On the left is a sidebar with navigation links: Compliance overview, CONSENT (Purposes, Processes, Notice & banner, Consent records, Cookies), RIGHTS (Requests & grievances), DATA (PII inventory, Data flows, Processors, Retention, Impact assessments), INCIDENTS (Breaches), and GOVERNANCE (Reports, Settings). The main panel is titled 'Data discovery & PII map' and shows a summary of scan results: 1 Connected store (last scan just now), 1 High / critical risk (hold Aadhaar, card or ID data), 1 Un-minimised (PII beyond declared purpose), 0 Unencrypted stores, and 0 Never scanned stores. Below this is a 'PII map' table showing detected data categories (PAN, Phone, Email) for the 'Nyvika test folder'. The 'PAN' column is red, indicating it exceeds the declared purpose. An 'Asset catalogue' section shows a detailed view of the 'Nyvika test folder' with its location, category, signal, confidence, and masked sample. A table below lists specific findings: a phone number (95% confidence), an email address (95% confidence), and a PAN (85% confidence).

Location	Category	Signal	Confidence	Masked sample
drive/1cAF1A84g5m3U_e49R1X0s1PgFn12PCZ/Team Members	Phone	Content match	95%	XXXXXXXX4287
drive/1cAF1A84g5m3U_e49R1X0s1PgFn12PCZ/Team Members	Email	Content match	95%	a***@gmail.com
drive/1cAF1A84g5m3U_e49R1X0s1PgFn12PCZ/Team Members	PAN	Content match	85%	A*****SC

A Google Drive folder after its first scan. A sheet in the folder held a phone number, an email address and a PAN, each stored masked with its confidence. The folder's declared purpose (enquiries) doesn't need a PAN, so the store is flagged *un-minimised* and the PAN marked red: either that column goes, or there is a real purpose for it that belongs on the register.

TRY IT ON A TEST FOLDER FIRST

Make a folder with one Google Sheet of made-up rows (a name, a phone number, an email, a PAN) and connect that before a real one. You'll see exactly what a finding looks like, and the red PAN marker shows how minimisation flags work, in a minute.

LIMITS

A store reads the files directly inside the folder, not its subfolders; add each subfolder as its own store. Google Sheets and Docs are read as text, plus small CSV, text and JSON files; PDFs, images and scans are not. Scans are started from the console, not scheduled. If key creation is greyed out in Google Cloud, your Workspace has a policy blocking service-account keys and an administrator must allow it.

Processors, over time

Who: Privacy Analyst or DPO.

Keep the register current: agreements expire, reviews lapse, vendors change. The register warns about agreements expiring within 30 days.

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)

Register
Highest risk first. Offboarded processors are listed at the bottom. [+ Add processor](#)

Processor · sync	Location	Purposes	Data received	Processing agreement	Security review	Risk
Mixpanel Product analytics Analytics Manual sync	Germany eu-central-1 → Cross-border	Product analytics	IP address Email	⚠ Awaiting signature	⚠ In progress	🔴 High 58 why Edit
Delhivery Last-mile delivery Logistics Manual sync	India	Account & orders	Name Phone Address	❌ No agreement	⚠ Not started	🔴 High 54 why Edit
Razorpay Payment gateway Payments Manual sync	India ap-south-1	Account & orders	Name Email Phone UPI ID ❌ Card number	⚠ Signed expires in 29 days (29 Oct 2026)	✅ Passed	🔴 High 50 why Edit
Salesforce Customer relationship management CRM	United States → Cross-border	Account & orders Offers & newsletters	Name Email Phone Address	⚠ Signed expires in 20 days (19 Oct 2026)	✅ Passed	🟡 Medium 30 why Edit

The processor register a few months in.

When a new agreement is signed, open the processor, set it to *Signed* with its dates, and save: the attention item clears and the health score rises. When you stop using a processor, offboard it rather than deleting it, so the history stays.

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 out

Sign-in security

Settings

Who your principals can contact, who can use the console, how your systems connect, and the record of everything done here.

OrganisationTeamSecurityAPI keysIntegrationsProcessor syncNotificationsAudit log

When a principal withdraws consent or has their data erased, each processor that received it must stop processing and erase it too (s.8(7)). Nyvika pushes these changes to HubSpot and Salesforce and retries failures with backoff. Showing the latest 100. [Connect processors](#) · [Turn integrations on or off](#)

Delivered

96

Pending

0

Failed

4

processors may still hold the data

All

Failed

Pending

Delivered

Event	Processor	Status	Attempts	Created	Last error	Actions
consent.withdrawn	Salesforce	Delivered 30 Sept, 12:06 pm	2	30 Sept, 12:06 pm	—	No action
consent.withdrawn	Salesforce	Delivered 30 Sept, 11:47 am	1	30 Sept, 11:47 am	—	No action
principal.erasure_requested	Salesforce	Delivered 30 Sept, 11:07 am	1	30 Sept, 11:07 am	—	No action
principal.erasure_requested	HubSpot	Delivered 30 Sept, 11:07 am	1	30 Sept, 11:07 am	—	No action
consent.withdrawn	Salesforce	Delivered 30 Sept, 11:06 am	1	30 Sept, 11:06 am	—	No action
consent.withdrawn	HubSpot	Delivered 30 Sept, 11:06 am	2	30 Sept, 11:06 am	—	No action
consent.withdrawn	HubSpot	Delivered 30 Sept, 10:55 am	1	30 Sept, 10:55 am	—	No action

Settings → Processor sync: every withdrawal and erasure instruction sent to your connected processors, with its status and attempts. Failed ones are retried automatically; you can retry by hand once you've fixed the cause.

Nyvika · Guide for Data Fiduciaries

49 / 65

Impact assessments

Who: Privacy Analyst writes; the DPO approves.

Before launching something that processes personal data in a new way — profiling, a new tracking tool, a large new dataset — write a DPIA. Twelve questions score the risk as you answer.

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 out

Sign-in security

Data protection impact assessments

Assess high-risk processing before it starts. DPDP s.10(2)(c) makes periodic DPIAs mandatory for Significant Data Fiduciaries; for everyone else they are good practice whenever processing is new, large-scale or sensitive.

Assessments
3
1 in progress

Awaiting review
1
decided by the DPO

Approved
1

High or critical risk
0
based on answers so far

Assessments
Most recently updated first. Open one to answer, submit or review it.

Assessment	Status	Risk	Answered	Owner	Reviewer	Updated
Customer support call recording Record support calls for quality and dispute resolution.	Draft	Low 8	3/12	Meera Iyer	—	29 Sept, 06:41 pm
Loyalty programme with UPI cashback Points and cashback credited to a linked UPI ID for repeat purchases.	Approved	Medium 19	12/12	Meera Iyer	Ananya Sharma	29 Sept, 06:41 pm
Personalised recommendations engine Recommend products from browsing and purchase history in the...	In review	Medium 32	12/12	Meera Iyer	Awaiting DPO	29 Sept, 06:41 pm

Impact assessments and their status.

Nyvika · Guide for Data Fiduciaries

50 / 65

Safeguards

Reasonable security safeguards (s.8(5)).

S1 Is the data encrypted at rest and in transit?

☐ Yes
☒ No
☐ Not applicable
⬆ Raises risk +10

S2 Is access restricted by role and logged?

☒ Yes
☐ No
☐ Not applicable

Sharing

Transfers outside India (s.16) and processor contracts (s.8(2)).

X1 Is personal data transferred outside India?

☐ Yes
☒ No
☐ Not applicable

X2 Do all processors involved have a signed processing agreement?

☒ Yes
☐ No
☐ Not applicable

Mitigations

How each flagged risk is reduced or accepted. Required before submitting.

Opt-in only (separate consent), 12-month retention on browsing events, no sensitive categories used as signals, warehouse encryption to be enabled before launch.

An assessment: linked purposes, systems and processors, answers, the live risk meter, mitigations and the DPO's review.

- 1 Create the assessment, link the purposes, systems and processors involved, and answer all twelve questions.
- 2 Write the mitigations and submit. The assessment is locked while in review.
- 3 The DPO approves it, or rejects it with a note; a rejected assessment goes back to draft. Authors can't approve their own.

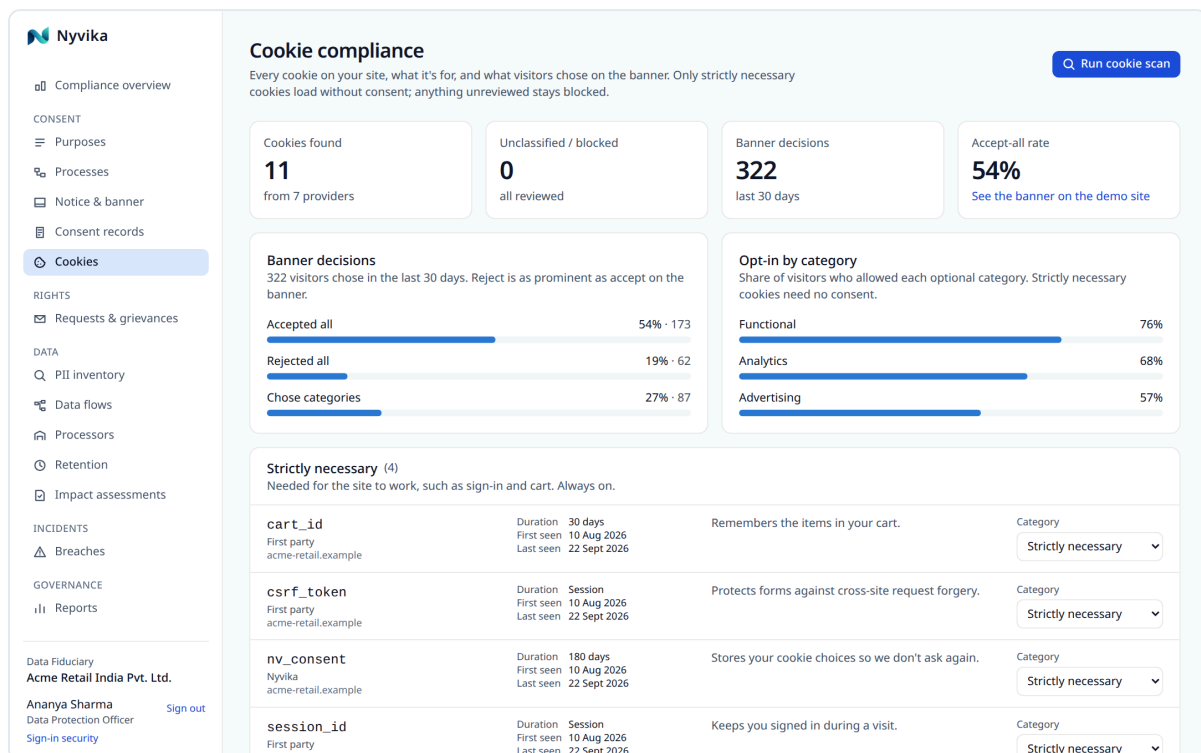
DPDP · S.10 · RULE 13

Significant Data Fiduciaries must carry out periodic DPIAs and audits. For everyone else, a DPIA is good practice and the best evidence that privacy was considered before launch.

Cookies

Who: Privacy Analyst or DPO.

The cookie inventory lists every cookie on your site and its category, with how visitors are choosing. New cookies found by a scan are *Unclassified* and never load until you classify them.



Cookie compliance. Banner decisions, opt-in rate per category, and the inventory with a category selector per cookie.

Run a scan monthly, and after any website release. Classify each new cookie as necessary, functional, analytics or advertising; visitors who allowed that category get it from their next visit.

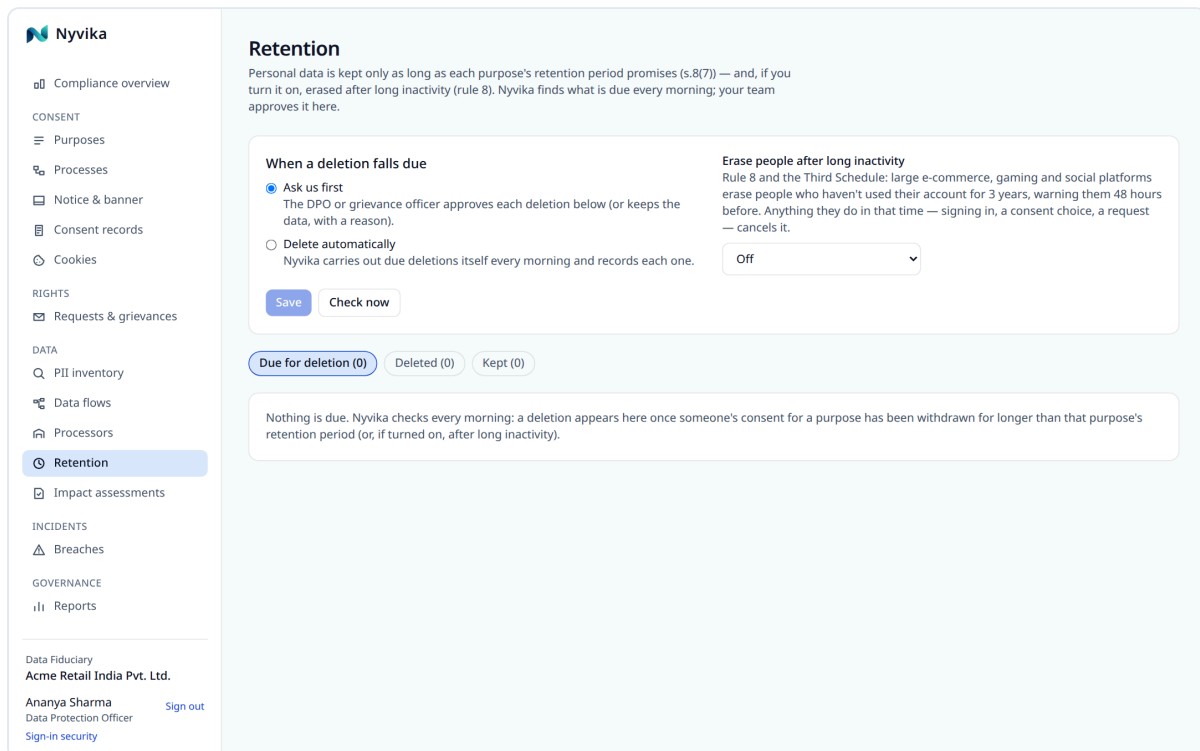
IN THIS VERSION

The cookie crawler is simulated; a real crawl of your site is on the roadmap. Add and classify cookies you know about in the meantime.

Retention and deletion

Who: Grievance Officer and DPO approve; DPO sets the rules.

Every morning Nyvika works out whose data has outlived its purpose: consent withdrawn longer ago than the purpose's retention period, or (if switched on) long inactivity. With *Ask us first*, each deletion waits here for a decision.



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 out](#)
[Sign-in security](#)

Retention

Personal data is kept only as long as each purpose's retention period promises (s.8(7)) — and, if you turn it on, erased after long inactivity (rule 8). Nyvika finds what is due every morning; your team approves it here.

When a deletion falls due

☒ **Ask us first**
The DPO or grievance officer approves each deletion below (or keeps the data, with a reason).

☐ **Delete automatically**
Nyvika carries out due deletions itself every morning and records each one.

[Save](#) [Check now](#)

Erase people after long inactivity
Rule 8 and the Third Schedule: large e-commerce, gaming and social platforms erase people who haven't used their account for 3 years, warning them 48 hours before. Anything they do in that time — signing in, a consent choice, a request — cancels it.

Off ▼

[Due for deletion \(0\)](#) [Deleted \(0\)](#) [Kept \(0\)](#)

Nothing is due. Nyvika checks every morning: a deletion appears here once someone's consent for a purpose has been withdrawn for longer than that purpose's retention period (or, if turned on, after long inactivity).

Retention. Nothing is due today at Acme; when something is, each item says exactly what will happen before you approve it.

- **Approve** to carry out the deletion: processors holding the data only for expired purposes are told to erase it, and once nothing about the person is needed, their encrypted contact details are destroyed and the evidence trail redacted.
- **Keep** with a reason, such as a legal hold; it isn't proposed again.
- Inactivity erasures warn the person 48 hours ahead; anything they do in that time cancels it.

Nyvika also clears its own short-lived records: sign-in code records after 30 days, notification texts after a year (breach notices are kept as proof), and cookie-banner decisions after 13 months.

Notifications

Who: everyone can see; the DPO manages settings.

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 out](#)
[Sign-in security](#)

Settings

Who your principals can contact, who can use the console, how your systems connect, and the record of everything done here.

Organisation Team Security API keys Integrations Processor sync **Notifications** Audit log

Who hears from Nyvika

- ☒ **Email requesters about their requests**
When a request is received, changes status, gets a message from your team or is completed, the person hears about it — by email, or by SMS if they gave a phone number — in English or Hindi. An erased person's confirmation is sent before their address is destroyed.
- Daily deadline digest for officers**
Each morning (9:00 IST), everyone who handles requests gets their overdue and soon-due requests — assignees their own, the DPO and grievance officers every unassigned one.
Warn 7 days before the deadline ▼

[Save](#)

Sent	Pending	Failed
0	0	0

[All](#)
[Failed](#)
[Pending](#)
[Sent](#)
[Every kind](#)
[Request updates](#)
[Deadline digests](#)
[Breach notices](#)
[Inactivity warnings](#)

Nothing here yet.

Settings → **Notifications:** every email and SMS Nyvika sent or is sending — request updates, deadline digests, breach notices and inactivity warnings. Recipients are described, never shown.

Check the **Failed** filter weekly. A failure usually means a bounced address or an SMS template problem; fix the cause and retry. Someone who wasn't told about their request may not know it was completed.

Reports and the audit log

Who: everyone; exports are logged.

When an auditor, the board or the Data Protection Board asks, the answer is a download.

Audit-ready reports
Export the records an auditor, the Data Protection Board or a customer's due-diligence team will ask for. Every export is generated live and recorded in the audit log.

- Record of processing activities**
Every purpose with its lawful basis, data categories, retention, systems, processors and cross-border transfers.
Who asks: Auditors and the Board; the starting point for any compliance review.
[Download CSV](#) [JSON](#) [Preview](#)
- Consent summary**
Current consent state per purpose and the notice version it was given on.
Who asks: Management and marketing, to see who can lawfully be contacted.
[Download CSV](#) [JSON](#) [Preview](#)
- Consent ledger**
Every consent artifact with its hash-chain links (most recent 20,000).
Who asks: Auditors testing that consent evidence is complete and untampered.
[Download CSV](#) [JSON](#) [Preview](#)
- Ledger integrity proof**
A fresh recomputation of every principal's consent hash chain, with any breaks.
Who asks: Auditors and the Board, as proof of consent under s.6(10).
[Download CSV](#) [JSON](#) [Preview](#)
- Rights request register**
Access, correction, erasure, nomination and grievance requests with SLA outcome.
Who asks: The Board when investigating a complaint; internal audit.
[Download CSV](#) [JSON](#) [Preview](#)
- Personal data breach register**
Incidents with detection, containment, Board and principal notification timestamps.
Who asks: The Data Protection Board (Rule 7) and cyber-insurance.
[Download CSV](#) [JSON](#) [Preview](#)
- Processor register**
Third parties that receive personal data, their contracts, security reviews and risk.
Who asks: Customers' vendor due diligence and auditors checking s.8(2) contracts.
[Download CSV](#) [JSON](#) [Preview](#)
- Cookie register**
Cookies and trackers found on the website and how each is classified.
Who asks: Marketing and web teams; customers' privacy questionnaires.
[Download CSV](#) [JSON](#) [Preview](#)
- Console audit log**
Who did what in the console, most recent 5,000 events.
Who asks: Internal audit and security reviews.
[Download CSV](#) [JSON](#) [Preview](#)

Choose Preview on a report to see its first rows here.

Reports as CSV (opens safely in Excel) or JSON, with a preview.

Report	Contains	Typically for
Record of processing	Every purpose: basis, data, retention, systems, processors, transfers outside India, active consents	Auditors, the Board
Consent ledger	Every consent entry with its hash-chain links	Proving consent
Consent summary	Current state by purpose and notice version	Management
Rights request register	Every request with channel, identity, assignee, dates and SLA outcome	Auditors, the Board
Breach register	Detection, containment and notification times; 72-hour compliance	The Board
Processor register	Contracts, reviews and risk per processor	Procurement, auditors
Cookie register	Every cookie and its category	Web and marketing teams
Console audit log	Who did what, when	Internal audit
Ledger integrity proof	Recomputation of every customer's consent chain	Evidence of no tampering

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

Settings

Who your principals can contact, who can use the console, how your systems connect, and the record of everything done here.

OrganisationTeamSecurityAPI keysIntegrationsProcessor syncNotificationsAudit log

Every change made in the console or through the API, with who made it. Entries can't be edited or deleted from the console. Showing the latest 200; export the full log from [Reports](#).

AllNoticesPurposesRights requestsBreachesPrincipal lookupsReport exportsAPI keysTeamOrganisationProcessors

DPIAsCookiesSign-ins

Time	Who	Action	Summary
30 Sept, 05:32 pm	Ananya Sharma	session.login	Ananya Sharma signed in
30 Sept, 05:31 pm	Ananya Sharma	session.login	Ananya Sharma signed in
30 Sept, 05:31 pm	Ananya Sharma	session.login	Ananya Sharma signed in
30 Sept, 05:30 pm	Ananya Sharma	session.login	Ananya Sharma signed in
30 Sept, 04:08 pm	Ananya Sharma	session.login	Ananya Sharma signed in
30 Sept, 04:02 pm	Ananya Sharma	principal.looked_up	Viewed consent record of principal 63e34635d5a0
30 Sept, 04:02 pm	Ananya Sharma	session.login	Ananya Sharma signed in
30 Sept, 03:11 pm	Ananya Sharma	session.login	Ananya Sharma signed in
30 Sept, 03:10 pm	Ananya Sharma	session.login	Ananya Sharma signed in
30 Sept, 03:10 pm	Ananya Sharma	session.login	Ananya Sharma signed in
30 Sept, 03:09 pm	Ananya Sharma	session.login	Ananya Sharma signed in
30 Sept, 02:56 pm	Ananya Sharma	session.login	Ananya Sharma signed in
30 Sept, 02:51 pm	Vikram Rao	session.login	Vikram Rao signed in

Settings → Audit log. Every change, sign-in, lookup and export, with who and when; filter by area.

PART III

Reference

What the law asks and where Nyvika answers it, every deadline in one place, routines for the privacy team, roles, troubleshooting and a glossary.

The law, mapped to Nyvika

The obligations of a Data Fiduciary under the DPDP Act, 2023 and the DPDP Rules, 2025, and where each is handled.

Provision	Obligation	In Nyvika
s.4, s.7	Process only for a lawful purpose, with consent or for a legitimate use	Purposes with a legal basis (Ch. 5)
s.5 · Rule 3	Give an itemised notice with every consent request, in English or an Eighth Schedule language	Notice & banner, widget, translations, channel wording (Ch. 5, 7, 11)
s.6(1)	Consent free, specific, informed, unconditional and unambiguous, per purpose	One switch per purpose, off by default (Ch. 5, 14)
s.6(4)	Withdrawing consent as easy as giving it	Preference centre, Privacy Centre (Ch. 11, 14)
s.6(6), s.8(7)(b)	Processors stop processing on withdrawal and erase on erasure	Processor connectors and sync log (Ch. 10, 21)
s.6(10)	Prove notice was given and consent obtained	Consent records, tamper-evident ledger, ledger proof (Ch. 17, 26)
s.8(2)	Engage processors only under a valid contract	Processor register with agreement status (Ch. 6, 21)
s.8(5)	Reasonable security safeguards	Two-factor, single sign-on, roles, audit log, encryption (Ch. 2, 9)
s.8(6) · Rule 7	Intimate the Board and affected people of a breach; detailed report within 72 hours	Breach register, checklist, drafts, breach notices (Ch. 19)
s.8(7) · Rule 8	Erase data when the purpose is served or consent withdrawn; erase after inactivity for listed platforms, with 48 hours' warning	Retention queue and settings (Ch. 12, 24)
s.8(9), s.8(10) · Rule 9	Publish contact details; run a grievance mechanism	Organisation contacts, grievances (Ch. 4, 16)
s.10 · Rule 13	Significant Data Fiduciaries: DPO, DPIA, audits	DPIAs, reports, audit log (Ch. 22, 26)
s.11–s.14	Rights to access, correction and erasure, grievance redressal and nomination	Requests & grievances (Ch. 16)
s.16	Transfers outside India, except to restricted countries	Processor and system locations, data flows (Ch. 6, 20)

Provisions are summarised. Confirm with your counsel which apply to your organisation, especially if you are notified as a Significant Data Fiduciary.

Every deadline and clock

Clock	Length	Starts	What happens
Rights request	30 days (default, configurable)	When the request is filed	Countdown on the queue; digest warnings; overdue on the overview
Grievance	90 days (Rule 14(3))	When the grievance is filed	As above
Breach report to the Board	72 hours (Rule 7(2)(b))	When the breach is detected	Live clock on the incident and the overview
Inactivity warning	48 hours before erasure (Rule 8)	When the erasure is approved or due	Warning by email or SMS; any activity cancels it
Inactivity period	3 years for listed platforms (Third Schedule)	Last activity	Proposed for erasure
Purpose retention	Set per purpose	When consent is withdrawn	Proposed for deletion
Deadline digest	Daily, 9:00 IST	—	Email to officers with due and overdue requests
Retention check	Daily, 9:30 IST	—	New deletions queued (or carried out, if automatic)
Privacy Centre code	10 minutes, 5 attempts	When sent	Expires
Console session	8 hours	Sign-in	Sign in again
Invitation link	7 days, single use	When sent	Resend from Settings → Team
Password reset link	1 hour, single use	When requested	Request another
Processor agreements	Warned 30 days before expiry	—	Shown on the processor register

Routines for the privacy team

Every day

- ☐ Overview: work the **Needs attention** list from the top
- ☐ Requests: new requests assigned; nothing waiting on identity
- ☐ Any open breach: next step on its checklist
- ☐ Retention: approve or keep what's due

Every week

- ☐ Notifications: nothing in **Failed**
- ☐ Processor sync: no failed deliveries
- ☐ Requests on hold: still waiting for a reason

Every month

- ☐ Cookie scan; classify anything new
- ☐ Processors: agreements expiring soon; new vendors registered
- ☐ Health score trend reported to management
- ☐ Team: leavers deactivated, roles still right

Every quarter or year

- ☐ Purposes: still accurate; retention periods still right
- ☐ Notice: re-read in every language
- ☐ DPIAs for anything new or changed
- ☐ Export the record of processing and rights register for audit
- ☐ Verify the entire consent ledger

Roles and permissions

Can...	DPO	Grievance Officer	Privacy Analyst	Viewer
See everything	✓	✓	✓	✓
Handle rights requests and grievances	✓	✓		
Report and manage breaches	✓	✓		
Approve retention deletions	✓	✓		
Edit purposes and draft the notice; discovery, processors, DPIAs, cookies	✓		✓	
Publish a notice version	✓			
Approve or reject a DPIA	✓			
Team, security, API keys, integrations and organisation settings	✓			

Everyone manages their own password and two-factor under **Sign-in security**.

Troubleshooting

Problem	What to do
My invitation link says it can't be used	It has expired (7 days) or was already used. Ask your DPO to resend it from Settings → Team.
The invitation email never arrived	Check spam. Your DPO can resend it; if email isn't working, Nyvika shows the link on screen for the DPO to pass on privately.
I forgot my password	Use Forgot password? on the sign-in page. If your company uses single sign-on, sign in that way instead — there's no password to reset.
I lost my phone	Sign in with a recovery code, then set two-factor up again. No codes left? Ask the DPO to reset your two-factor.
"Your organisation requires two-factor authentication"	Set it up on the page you're taken to (Chapter 2); the rest of the console opens once it's on.
"Your organisation signs in with single sign-on"	Use Sign in with single sign-on on the sign-in page.
I can see a screen but not change it	Your role doesn't include that action (see Roles). Settings shows a note saying so.
A page shows only some of our purposes	Its key has a default process (Settings → API keys → Routing), or the page asks for a process. Remove the default from website and Privacy Centre keys.
An app gets "Unknown reference" or "isn't allowed to use process"	The label isn't set up on that app's key, or the process isn't its default or one of its allowed processes. Check the key's Routing.
The banner doesn't appear on our website	Check the script is on the page, the key is a <i>publishable</i> key that hasn't been revoked, and the site is on your organisation's domain or a subdomain.
A consent from our site isn't in Consent records	Search by the exact email or phone used. Check that the site calls <code>Nyvika.capture</code> when the form is submitted.
A processor shows "failed"	Open the integration and select Test connection ; the error says what's wrong (often an expired token or a missing permission). Then retry from Processor sync.
Notifications show "failed"	Usually a bounced address or an SMS template issue. Fix it, then retry the notification.
The health score dropped	The score card shows each of its six measures and what lowered it; the attention list names the specific item to fix.

What's still simulated

This version of Nyvika is complete for consent, notices, rights, breaches, processors, discovery, retention and the console. What remains simulated or unverified:

- **The cookie crawler** reports a fixed set of cookies rather than crawling your site in a browser. Cookies you declare or add are real; unknown ones stay blocked until classified.
- **Connectors are tested against stand-ins** of each vendor's published API. Google Drive has also been run against a live Google account; the other data-store and processor connectors meet a real account for the first time during your onboarding, with your own sandbox or trial credentials.

Email, SMS, WhatsApp, processors and data stores are real once your organisation's accounts are connected.

Glossary

Data Fiduciary	The organisation that decides why and how personal data is processed — you.
Data Principal	The person the data is about: your customer, user or visitor.
Data Processor	A company that processes personal data on your behalf, such as your CRM or delivery partner.
Significant Data Fiduciary	A fiduciary the government notifies as such because of the volume or sensitivity of its processing; it has extra obligations (s.10).
Data Protection Board	The authority that receives breach reports and hears complaints under the Act.
Purpose	One specific reason for processing personal data. Consent is given and withdrawn per purpose.
Channel	Where a notice is given: website, app, IVR, kiosk, call centre or paper. A purpose can have wording for a specific channel.
Business process	One journey that asks for consent (such as app sign-up), with its purposes in order. Consents record the process they were given in.
Routing	A key's default process, allowed processes and labels, set under Settings → API keys.
Legitimate use	Processing allowed without consent under s.7, such as legal obligations. Disclosed, but without a consent switch.
Notice version	A published, numbered snapshot of your notice. Each consent records the version and language it was given on.
Re-consent	Asking people again after a notice change that affects what they agreed to.
Consent ledger	The chain of consent records for each person, linked so any alteration is detectable.
Rights request (DSR)	A request to access, correct or erase data, nominate someone, or raise a grievance.
DPIA	Data protection impact assessment: a structured look at the risks of a processing activity before it starts.
Publishable key	A key for your website; it can only show the notice, record consent and start rights requests, and only from your domain.
Secret key	A key for your servers with full access. Never put it in a web page or app.
Privacy Centre	The page where customers verify with a code and manage their consent and requests.
Two-factor authentication	Signing in with your password plus a code from an app on your phone.
Single sign-on	Signing in with your company account through your identity provider.