

Website privacy report

Example Business (a real site, name hidden) | <https://example-business.example/>

Checked on 10 October 2026 against India's data protection law (the DPDP Act, 2023). 7 pages opened.



The main duties under the Act apply from 13 May 2027. This report shows how ready the site is. It does not say that any law has been broken.

In short

Your website shows a clear pop-up about cookies, and saying no is as easy as saying yes. But as soon as someone arrives, your website saves small tracking files that record where they came from. It keeps doing this after they press "Reject All". Your privacy notice also leaves out some things people need, such as how to change their cookie choice, how to use their rights, who to contact, how quickly you reply and how to complain, and your web developer and whoever writes your privacy notice can fix these.

Where the site stands

Tracking of visitors

Needs attention

Files noting where visitors came from are saved before any choice and kept after refusing.

Privacy notice

Some gaps

Lists the details you collect, but rights, complaints and cookie descriptions are vague or missing.

Asking permission

Needs attention

Refusing is easy, but it does not stop the tracking and cannot be changed later.

Contact and complaints

Some gaps

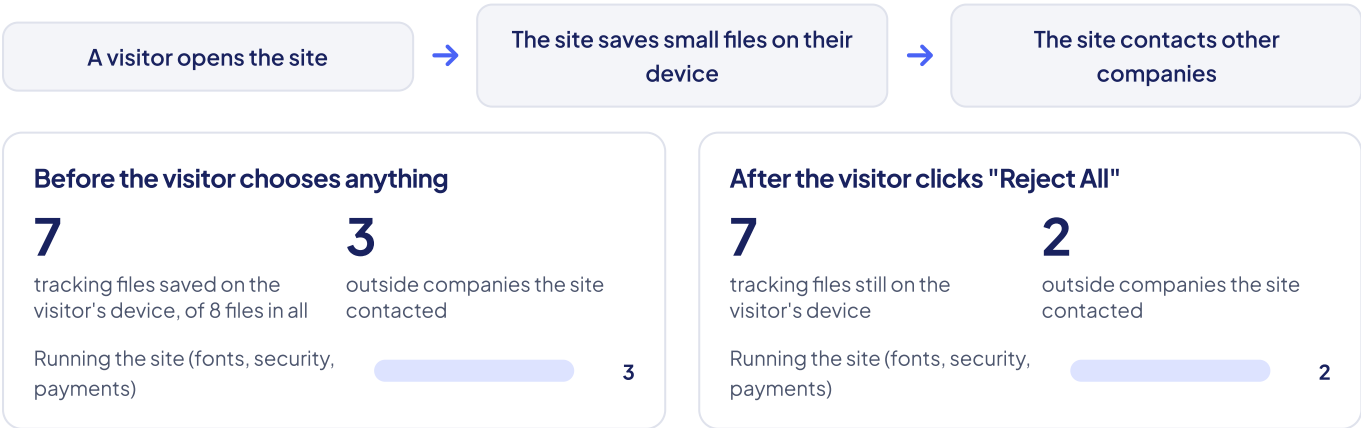
General email and phone are shown, but no privacy contact or reply time.

Children

Looks fine

The site serves businesses, says it is not for under-18s, and asks no age.

What happens when someone visits



Used to track or advertise Used to run the site, or not identified | Counted only if seen in at least 2 of the 3 checks.

What we found, in plain words

Most serious first. The site was checked 3 separate times, and each point below was found in at least two of them. The numbers match the detailed findings in the second part of this report.

- 1**

Your website records where visitors came from before they choose, and keeps doing it after they press "Reject All".

High risk

When someone opens your website, it saves small tracking files, called cookies, that note how they found you, for example from a search or an advert. This happens before they answer the pop-up that asks about cookies, and the files stay after they say no, with one refreshed. So the "Reject All" button does not do what it says, and the online shop that uses these files is not open yet.

Who fixes it: [Your web developer](#)

- 2**

Your website gives visitors no easy way to change their cookie choice later.

Medium risk

Once a visitor answers the pop-up that asks about cookies, it disappears and there is no button to bring it back. Your privacy notice only tells people to change their browser settings. Changing their mind should be as easy as the first click.

Who fixes it: [Your web developer, with whoever writes your privacy notice](#)

- 3**

Your privacy notice does not tell people exactly how to ask to see, correct or delete their details.

Medium risk

Your notice says people "may" have rights and should use your "official communication channels", but it does not say which email or form to use. It also does not mention raising a complaint with you or naming someone to act for them.

Who fixes it: [Whoever writes your privacy notice](#)

- 4**

Your privacy notice does not tell people they can complain to the government's Data Protection Board.

Medium risk

If someone is unhappy with how you handle their details, they can take it to the Data Protection Board of India. Your notice does not mention this, and a sentence or two would cover it.

Who fixes it: [Whoever writes your privacy notice](#)

- 5**

Your website does not name anyone to answer privacy questions or say how quickly complaints will be answered.

Medium risk

Your contact page lists a general email and phone number, which helps. But your privacy notice only says to use "the contact details provided on our website" and to expect a reply "as promptly as reasonably possible". It should say who handles privacy questions and give a set time for answering complaints.

Who fixes it: [You, with whoever writes your privacy notice](#)

- 6**

Your privacy notice and cookie pop-up do not describe the tracking your website actually does.

Medium risk

The pop-up says cookies are used for personalised adverts, which we did not see happen, and your privacy notice does not mention adverts at all. Neither one says that your website records where each visitor came from. People should be able to read one clear, accurate list of what is collected and why.

Who fixes it: [Whoever writes your privacy notice, with your web developer](#)

7 Your website's enquiry form asks for more details than are needed to answer a question.

Medium risk

The "Get Started" form on every page marks name, email, company, phone and location as required, and the location box asks for a street address. For a first enquiry, a name and an email or phone number are usually enough, and fewer details means less to look after.

Whether this is required depends on how the law treats details a person gives voluntarily.

Who fixes it: You, with your web developer

Depends on the legal basis

8 Your privacy notice does not name the other companies your website uses.

Low risk

Every visit loads lettering from Google and Cloudflare, so those companies see each visitor's internet address. Your notice only mentions "trusted" providers without naming them. Naming them is good practice rather than a strict rule.

Who fixes it: Whoever writes your privacy notice, with your web developer

9 Your privacy notice is only in English.

Low risk

The law lets people read the notice in English or in one of India's listed languages. How many languages a business must offer is not settled yet, so this is a minor point.

Who fixes it: Whoever writes your privacy notice

What the site does well

- ✓ The pop-up about cookies appears straight away, and "Reject All" is as easy to press as "Accept All".
- ✓ No advertising or social media trackers were seen, either before or after a visitor refused.
- ✓ Every page we opened uses a secure connection.
- ✓ Your privacy notice is linked on every page and lists the kinds of details you collect.

What we could not see

- ? Whether your enquiry forms send details securely. They probably do, but your developer should confirm it.
- ? What your website does after a visitor presses "Accept All", and what the "Customise" option offers.
- ? The free online calculator, your product sign-in areas and the shop, which is not open yet.
- ? Our checks disagreed on whether your notice explains clearly enough why each detail is used. A person should look.

What no website check can show

This report looks only at what a visitor can see. These matter just as much, and need a look inside the business.

- Whether the business has a plan for a data leak, and would tell the Board and the people affected in time.
- The contracts with outside companies that handle personal data for the business.
- How personal data is stored, protected and backed up inside the business.
- Whether data is really erased when it is no longer needed.
- How the business answers a person who asks to see, correct or erase their data.
- What staff do with personal data in email, chat apps and AI tools.

"Depends on the legal basis": Whether this is required depends on how the law treats details a person gives voluntarily. That question is not settled in this report.

About penalties. The main duties under the Digital Personal Data Protection Act, 2023 apply from 13 May 2027. The Act allows the Data Protection Board to impose penalties, up to Rs 250 crore for the most serious failures. This report cannot tell you whether a penalty would apply to your site: the Board decides each case on its facts.

Gap assessment from public pages only. Not legal advice. It reports what was seen on public pages on the day of the check and does not say whether the site meets the law.

For the person making the fixes

The exact details behind each finding: what was observed, where, and what to change.

Findings in detail

1. Sourcebuster `sbjs_*` cookies set before consent and kept/renewed after "Reject All"

C2, C4, T1 | found in 3 of 3 checks

High risk

Observed	On first load of <code>https://example-business.example/</code> , before any choice, the site set <code>sbjs_migrations</code> , <code>sbjs_current_add</code> , <code>sbjs_first_add</code> , <code>sbjs_current</code> , <code>sbjs_first</code> , <code>sbjs_udata</code> and <code>sbjs_session</code> on <code>.example-business.example</code> (Sourcebuster, records where the visitor came from; used by WooCommerce order attribution). After clicking "Reject All" and reloading, <code>sbjs_session</code> (30 minutes) was set or renewed and the other six <code>sbjs_*</code> cookies were left in place. No outside company received this data. The store page <code>https://example-business.example/product/product-a/</code> says it is "launching soon", so no orders are being attributed. Recorded in all 3 checks.
Where	<code>https://example-business.example/</code> (all pages); <code>screenshots/01-page.jpg</code> , <code>screenshots/after-refusing.jpg</code>
Why it matters	Recording traffic source is tracking that no legitimate use covers, so it needs consent before it starts (C2). It carries on after an explicit refusal, so the banner's choice does not match what the site does (C4, T1). Tracking that continues after refusing is rated high.
What to do	Turn off WooCommerce Order Attribution (WooCommerce > Settings > Advanced > Features) while the store is not live, or have CookieYes block the Sourcebuster script until the analytics/advertisement category is accepted, and delete existing <code>sbjs_*</code> cookies when a visitor rejects.

2. No persistent control to reopen cookie preferences; notice points only to browser settings

C4, N4 | found in 3 of 3 checks

Medium risk

Observed	After "Reject All" the banner was not shown again and no revisit or preferences button is visible (<code>screenshots/after-refusing.jpg</code>). Footer links are only Terms of Use, Privacy Policy, Refund and Returns Policy. Privacy notice section 3: "You may disable cookies through your browser settings, although doing so may affect certain features of the website."
Where	<code>https://example-business.example/</code> (<code>screenshots/after-refusing.jpg</code>); <code>https://example-business.example/privacy-policy/</code>
Why it matters	Withdrawing consent must be as easy as giving it (s6(4)), and the notice must give the means of withdrawing (s5(1)(ii), r3(c)(i)). Browser settings are not the site's own means and are not comparable to a one-click banner.
What to do	Enable the CookieYes revisit-consent button (or add a "Cookie settings" footer link that reopens the banner) and refer to it in section 3 of the privacy notice.

3. Notice gives no concrete means to exercise rights, raise a grievance or nominate

N5 | found in 3 of 3 checks

Medium risk

Observed	Section 8 "Your Rights": "Depending on applicable laws, you may have the right to request access to, correction of, updating, or deletion of your personal information. You may also request information regarding how your data is processed by contacting us through our official communication channels." No email, form or steps are given, and grievance redressal and nomination are not mentioned.
Where	https://example-business.example/privacy-policy/
Why it matters	r14(1)(a) requires the site to prominently publish the means to request access, correction and erasure, to raise a grievance and to nominate (Act s11 to s14). r3(c)(ii) requires the consent notice to describe them too.
What to do	Rewrite section 8 to list each right (access, correction, erasure, grievance, nomination) and give one specific channel, such as a privacy@example-business.example address or a request form, with what to include in a request.

4. Notice omits how to complain to the Data Protection Board

N6 | found in 3 of 3 checks

Medium risk

Observed	Sections 1 to 11 of the privacy notice contain no reference to the Data Protection Board of India or any outside complaint route.
Where	https://example-business.example/privacy-policy/
Why it matters	s5(1)(iii) and r3(c)(iii) require the notice accompanying a consent request (here the cookie banner) to describe how to complain to the Board.
What to do	Add a sentence to section 8 saying that a person may complain to the Data Protection Board of India after using Example Business's own grievance process, with a link to the Board's website.

5. No designated privacy/grievance contact and no published grievance response period

G1, G2 | found in 3 of 3 checks

Medium risk

Observed	Privacy notice section 11: "please contact us using the contact details provided on our website. We will respond to your enquiry as promptly as reasonably possible." https://example-business.example/contacts/ lists hello@example-business.example , +91 00000 00000 and a [city] address as general business contacts. No privacy contact, DPO, grievance procedure or response period appears on any page opened.
Where	https://example-business.example/privacy-policy/ ; https://example-business.example/contacts/
Why it matters	s8(9) and r9 require prominent publication of the business contact of a person able to answer questions about personal data. s8(10), s13 and r14(3) require a grievance system and a published response period of no more than 90 days.
What to do	Add a "Privacy contact and grievances" section to the notice naming a role and a dedicated email (e.g. privacy@example-business.example), a short grievance procedure and a response period of no more than 90 days (e.g. 30 days).

6. Cookie descriptions in banner and notice do not match each other or the cookies observed

N1, N2, T1 | found in 2 of 3 checks

Medium risk

Observed	Banner: "We use cookies to enhance your browsing experience, serve personalised ads or content, and analyse our traffic." Notice section 3: "Our website may use cookies and similar technologies to improve your browsing experience, remember your preferences, and analyze website performance." No advertising cookies or ad-network requests were recorded. The notice names no cookies and does not mention the traffic-source <code>sbjs_*</code> cookies or <code>cookieyes-consent</code> .
Where	https://example-business.example/privacy-policy/ ; screenshots/01-page.jpg
Why it matters	The notice must give an itemised description of the data and specific purposes (s5(1)(i), r3(b)) and be a fair account that matches what the site does (T1).
What to do	Run the CookieYes cookie scan, publish the resulting cookie list (name, provider, purpose, duration, category) in section 3 of the notice, including <code>sbjs_*</code> if kept, and remove "serve personalised ads" from the banner unless advertising tools are actually added.

7. Enquiry form marks company, phone and street-address location as mandatory

Depends on the legal basis | C3 | found in 3 of 3 checks

Medium risk

Observed	The "Get Started" pop-up form on every page opened has <code>name-1</code> (Name *), <code>email-1</code> (Email *), <code>name-2</code> (Company Name *), <code>phone-1</code> (Contact *), <code>address-1-street_address</code> (Location *) and <code>textarea-1</code> (Message). Every field except the message is starred as mandatory (one check notes they are not marked <code>required</code> in the HTML).
Where	https://example-business.example/ and every other page opened, via the "Get Started" pop-up
Why it matters	Personal data asked for should be limited to what the purpose needs (s6(1)), here replying to an enquiry. A street address is unlikely to be needed.
What to do	Keep name and email mandatory, make <code>name-2</code> and <code>phone-1</code> optional, and replace <code>address-1-street_address</code> with an optional city/country field.

8. Outside service providers receiving data not named in the notice

S1 | found in 3 of 3 checks

Low risk

Observed

Notice section 5: "Information may be shared only with trusted third-party service providers who assist in operating our website or delivering our services". None are named. Before any choice the browser contacted `fonts.googleapis.com`, `fonts.gstatic.com` (Google Fonts) and `cdnjs.cloudflare.com` (Cloudflare, Font Awesome). After "Reject All", `fonts.googleapis.com` and `fonts.gstatic.com` were still contacted. CookieYes runs the banner (`cookieyes-consent`).

Where

`https://example-business.example/privacy-policy/`

Why it matters

Good practice only: s11(1)(b) gives a right to learn, on request, who data has been shared with. Naming providers up front makes this easier.

What to do

List the providers by name and purpose in section 5 (Google Fonts, Cloudflare, CookieYes, hosting and form/email tools), or self-host the fonts and Font Awesome so no outside request is made.

9. Notice available in English only

N7 | found in 3 of 3 checks

Low risk

Observed

No language selector on the notice, the banner or any page opened; all text is English.

Where

`https://example-business.example/privacy-policy/`

Why it matters

s5(3) and s6(3) give the option to access the notice in English or an Eighth Schedule language. How many languages a site must offer is not settled.

What to do

Publish a Hindi (and if relevant Marathi) version of the privacy notice, linked from the top of the English page.

Seen in one check only

Not confirmed, so not counted as findings. Listed so nothing is left out.

- ? No privacy contact and no privacy notice link inside the CookieYes banner (C8).
- ? No privacy note or notice link beside the enquiry and contact forms; the only link is in the page footer (C5).
- ? No published identifier (e.g. registered email or account ID) to give when making a request, although Terms of Use section 4 refers to login credentials and Product A has client portals (N8).

What could not be checked

Nothing here is a finding either way.

- ? Form transport: the evidence flags the forms on all 7 pages opened as sent without a secure connection, but each form has an empty `action`, which submits to the current https page. The field names (`name-1`, `email-1`) suggest a Forminator AJAX submit. Not reported as an X1 finding. Confirm in the browser network tab that submissions go to an https endpoint; if any use http, that is a high X1 issue.
- ? The CookieYes "Customise" layer was not opened, so whether categories are pre-ticked (C1) was not checked.

- ? "Accept All" was not tested, so the tools behind the banner's "serve personalised ads" wording and which scripts CookieYes controls were not observed.
- ? The "Use the calculator" calculator on <https://example-business.example/solutions-product-b/> was not filled in, and the product portals and logins (Product A, Product B, Sizoru) were not accessed. The store <https://example-business.example/product/product-a/> is not live, so there was no checkout to check.
- ? The checks disagreed on whether notice section 2 states purposes specifically enough. One check said its general list (e.g. "Send important updates and notifications") is not linked to each data item (N1/N2); another counted the notice's list of data and purposes as done well. A person needs to review it.
- ? KI: outside scope. The site sells financial services to businesses, notice section 9 says services are "not intended for individuals under the age of 18", and no age or date-of-birth field was seen.

What was recorded

From the browser's own record during the visit, without accepting anything, filling in a form or logging in.

Personal data asked for

- ? "Get Started" pop-up form on every page opened (e.g. <https://example-business.example/#popup>): name-1 Name *, email-1 Email *, name-2 Company Name *, phone-1 Contact *, address-1-street_address Location *, textarea-1 Message.
- ? Contact form on <https://example-business.example/contacts/>: name-1 Full Name, email-1 E-Mail, phone-1 Phone, text-1 Subject, textarea-1 Your Message.
- ? Site search on <https://example-business.example/>: s search text.

Secure connection (https)

A form on this page is sent without a secure connection: <https://example-business.example/>
 A form on this page is sent without a secure connection: <https://example-business.example/contacts/>
 A form on this page is sent without a secure connection: <https://example-business.example/faq/>
 A form on this page is sent without a secure connection: <https://example-business.example/privacy-policy/>
 A form on this page is sent without a secure connection: <https://example-business.example/product/product-a/>
 A form on this page is sent without a secure connection: <https://example-business.example/solutions-product-b/>
 A form on this page is sent without a secure connection: <https://example-business.example/terms-of-use/>

Cookies set before any choice

Cookie	What it is	Kept for	First seen on	Checks
cookieyes-consent	CookieYes (records the consent choice)	365 days	/	3 of 3
sbjs_current	Sourcebuster (records where the visitor came from; used by WooCommerce order attribution)	this visit only	/	3 of 3
sbjs_current_add	Sourcebuster (records where the visitor came from; used by WooCommerce order attribution)	this visit only	/	3 of 3
sbjs_first	Sourcebuster (records where the visitor came from; used by WooCommerce order attribution)	this visit only	/	3 of 3
sbjs_first_add	Sourcebuster (records where the visitor came from; used by WooCommerce order attribution)	this visit only	/	3 of 3

<code>sbjs_migrations</code>	Sourcebuster (records where the visitor came from; used by WooCommerce order attribution)	this visit only	/	3 of 3
<code>sbjs_session</code>	Sourcebuster (records where the visitor came from; used by WooCommerce order attribution)	30 minutes	/	3 of 3
<code>sbjs_udata</code>	Sourcebuster (records where the visitor came from; used by WooCommerce order attribution)	this visit only	/	3 of 3

Outside addresses contacted before any choice

Outside address contacted	What it is	Requests	Checks
cdnjs.cloudflare.com	Cloudflare (security and delivery)	4	3 of 3
fonts.googleapis.com	Google services (fonts, maps, Firebase)	15	3 of 3
fonts.gstatic.com	Google static files (fonts, reCAPTCHA)	23	3 of 3

After clicking "Reject All"

Fresh visit to <https://example-business.example/> : clicked "Reject All", then reloaded with cookies kept (screenshots/after-refusing.jpg); same result in all 3 checks. The banner was not shown again and no revisit-consent control is visible. `sbjs_session` (Sourcebuster / WooCommerce order attribution, 30 minutes) was set or renewed. `sbjs_migrations`, `sbjs_current_add`, `sbjs_first_add`, `sbjs_current`, `sbjs_first` and `sbjs_udata` were left in place, and `cookieyes-consent` (365 days) stored the choice. Outside requests after refusing went only to fonts.googleapis.com (3, stylesheet) and fonts.gstatic.com (3, font), which are Google Fonts. No advertising, analytics or session-recording services were contacted before or after the choice.

Cookies set or renewed after refusing

Cookie	What it is	Kept for	Checks
<code>sbjs_session</code>	Sourcebuster (records where the visitor came from; used by WooCommerce order attribution)	30 minutes	3 of 3

Cookies from before the choice, left in place

Cookie	What it is	Kept for	Checks
<code>cookieyes-consent</code>	CookieYes (records the consent choice)	365 days	3 of 3
<code>sbjs_current</code>	Sourcebuster (records where the visitor came from; used by WooCommerce order attribution)	this visit only	3 of 3
<code>sbjs_current_add</code>	Sourcebuster (records where the visitor came from; used by WooCommerce order attribution)	this visit only	3 of 3
<code>sbjs_first</code>	Sourcebuster (records where the visitor came from; used by WooCommerce order attribution)	this visit only	3 of 3
<code>sbjs_first_add</code>	Sourcebuster (records where the visitor came from; used by WooCommerce order attribution)	this visit only	3 of 3
<code>sbjs_migrations</code>	Sourcebuster (records where the visitor came from; used by WooCommerce order attribution)	this visit only	3 of 3
<code>sbjs_udata</code>	Sourcebuster (records where the visitor came from; used by WooCommerce order attribution)	this visit only	3 of 3

Outside addresses contacted after refusing

Outside address contacted	What it is	Requests	Checks
fonts.googleapis.com	Google services (fonts, maps, Firebase)	3	3 of 3
fonts.gstatic.com	Google static files (fonts, reCAPTCHA)	3	3 of 3

How this was done

An automated visit to public pages only, as an ordinary visitor, in Chrome on a computer in India. The site was checked 3 separate times, each from a clean browser. A finding is reported only if at least two checks made it, and a cookie or outside address is counted only if at least two checks recorded it; the tables show the number for each. The findings are measured against a checklist of points from the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025; the codes beside each finding (such as N4 or C2) refer to that checklist. Checklist status: DRAFT of 10 October 2026. Citations read against the gazette copies of the Act and Rules in the legal folder. The points marked Interpretation, and the reading of the legal basis, still need review by Rushabh and a privacy lawyer.

Pages opened: <https://example-business.example/>, <https://example-business.example/privacy-policy/>, <https://example-business.example/contacts/>, <https://example-business.example/terms-of-use/>, <https://example-business.example/product/product-a/>, <https://example-business.example/solutions-product-b/>, <https://example-business.example/faq/>