GDPR vs DPDP

Understanding Data Privacy Laws — Europe vs India

This document explains the key differences between the European Union's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act 2023 (DPDP Act). It includes a detailed comparison table, a deep dive into transparency requirements, real-world examples, and a final side-by-side transparency breakdown that any ordinary person can understand.

What Are These Two Laws?

GDPR — General Data Protection Regulation (EU, 2018)

GDPR is a privacy law introduced by the European Union in 2018. Although it applies to people located in Europe, its influence is global because companies around the world often serve European users. GDPR is considered the world's most comprehensive privacy framework — it gives individuals significant control over their personal data and places strong legal obligations on any organization that collects or processes it.

DPDP Act — Digital Personal Data Protection Act (India, 2023)

The DPDP Act is India's most significant privacy legislation to date. It aims to regulate how organizations collect, process, store, and use personal data in India. The law introduces several principles familiar to GDPR — including individual rights, organizational responsibilities, and financial penalties for serious failures. Privacy experts view it as a major step forward in aligning India with global standards while addressing local realities.

> *Is India's law as strict as GDPR? Not exactly — GDPR is still generally considered the gold standard. However, the DPDP Act represents a meaningful shift toward stronger privacy protection and greater accountability in India.*

Key Differences — GDPR vs DPDP

The table below compares the two laws across the most important parameters that affect ordinary individuals and organizations.

Parameter	GDPR (EU, 2018)	DPDP Act (India, 2023)
Scope	Covers both digital AND non-digital personal data	Covers digital personal data only
Right to Be Forgotten	Explicitly guaranteed — strong erasure rights in most situations	Limited — not as strongly or clearly defined
Data Localization	No mandatory requirement to store data within EU	Government can restrict cross-border data transfers to certain countries
Consent Language	Must be in clear, understandable language	Must be available in multiple Indian languages — a unique local requirement
Children's Data	Age of consent is 16 in most EU countries	Age of consent is 18 and parental consent is mandatory — stricter here
Penalties	Up to EUR 20 million or 4% of global annual turnover — whichever is higher	Up to INR 250 crore per violation — significant but not tied to global turnover
Regulator	Independent Data Protection Authority in each EU country	Government-appointed Data Protection Board — less independent
Transparency Requirements	Extremely detailed — organizations must explain every use of data clearly	Less exhaustive — fewer mandatory disclosure requirements
Legal Basis	Must clearly state the legal basis for every data collection activity	Not required to specify legal basis
Third-Party Sharing	Must name or clearly categorize every third party data is shared with	Not explicitly required to disclose third-party recipients
Retention Periods	Specific time limits must be stated for how long data is kept	No explicit requirement to state retention periods
Right to Data Portability	Individuals can request their data in a portable, machine-readable format	Not as explicitly defined in the current framework

Real-world example: If Spotify collected your data without proper consent — under GDPR, a European user could demand full deletion of their data and Spotify could face fines tied to its global revenue. Under DPDP, an Indian user has the right to withdraw consent and seek correction, but the enforcement mechanism and regulator's independence are not yet as battle-tested.

Deep Dive — Transparency Requirements

Of all the differences between GDPR and DPDP, transparency requirements are the most practically important for ordinary people. This is where the gap between the two laws is most visible in everyday life.

Transparency means: when a company collects your data, how much are they legally required to tell you about what they are doing with it?

Under GDPR — What a Company MUST Tell You

Under GDPR, when any organization collects your personal data, they are legally required to clearly communicate all of the following:

- **Who is collecting your data**

  Not just the app name. The full legal name of the company, their registered address, and contact details of their Data Protection Officer must be provided.

- **Why they are collecting it — every purpose separately**

  Not vague statements like 'to improve your experience.' They must say specifically: 'we collect your location to show you nearby restaurants' AND 'we collect your browsing history to show you targeted advertisements' — each purpose stated individually.

- **The legal basis for collecting it**

  They must tell you why they are legally allowed to collect it. Is it because you consented? Because they have a contract with you? Because it is legally required? Each basis must be stated clearly.

- **How long they will keep it**

  They cannot keep your data forever without telling you. They must state: 'we keep your purchase history for 3 years' or 'we keep your location data for 90 days.' Specific periods, not vague promises.

- **Who they are sharing it with**

  Every third party must be disclosed. If they share your data with Google Analytics, Facebook Pixel, an email marketing company, or a payment processor — each one must be named or clearly categorized.

- **Whether your data leaves the country**

  If your data is being sent to servers in the US, Singapore, or anywhere outside the EU — they must tell you and explain what protections are in place to safeguard it.

- **All eight of your rights — listed clearly**

  They must explicitly inform you that you have the right to access your data, correct it, delete it, restrict its use, object to it being processed, port it to another service, and withdraw consent at any time.

- **How to complain to the regulator**

  They must name the specific government data protection authority you can approach if you feel your rights have been violated — not just tell you 'contact us.'

Real-world GDPR example: When you sign up for Spotify in Europe, before completing registration you receive a privacy notice stating — Spotify AB is collecting your data, here is exactly why, here is who we share it with including advertising and analytics partners, here is how long we keep each type of data, here are your eight rights, and here is how to contact the Swedish data protection authority if you have a complaint. All of this in plain, readable language — not buried in legal text.

Under DPDP — What a Company Must Tell You

India's DPDP Act requires companies to communicate the following at the baseline level:

- What personal data is being collected.
- The purpose of collection — in general terms.
- How to withdraw consent.
- How to make a complaint to the Data Protection Board.

Real-world DPDP example: When you sign up for an Indian fintech app, they must tell you they are collecting your name, phone number, and financial data to process your loan application, and that you can withdraw consent or complain to the Data Protection Board. But they are not legally required — under the same level of specificity as GDPR — to name the third-party companies they share your data with, state how long they keep it, or declare the legal basis for collection beyond your consent.

The Restaurant Menu Analogy

Think of it like a restaurant menu.

GDPR is like a menu that lists every ingredient in every dish, the calorie count, the allergens, where the ingredients were sourced from, and how the dish was prepared.

DPDP is like a menu that lists the name of the dish and the main ingredients — but does not tell you everything that went into it, where it came from, or how long it has been sitting in the kitchen.

> *Both menus are better than no menu at all. But if you have a serious allergy — or in data terms, if you are seriously concerned about your privacy — the GDPR menu gives you significantly more to work with.*

What This Means for Ordinary People

- **Under GDPR, you can ask a company: 'Who exactly did you share my data with?'**

  They are legally required to tell you specifically. Under DPDP, this obligation does not yet exist at the same level of detail.

- **Under GDPR, you can ask: 'How long are you keeping my medical records?'**

  They must give you a specific answer. Under DPDP, no equivalent requirement exists to disclose retention periods.

- **Under GDPR, you can ask: 'Why are you legally allowed to have my data?'**

  They must state the legal basis — consent, contract, or legal obligation. Under DPDP, they are not required to state a legal basis beyond your consent.

- **Under GDPR, you are informed of all eight of your rights upfront.**

  Under DPDP, your key rights are mentioned but not presented with the same completeness or clarity required by GDPR.

Transparency Requirements — Side by Side

The table below answers the questions an ordinary person might ask when handing over their personal data — and whether each law requires companies to answer them.

Question You Might Ask	GDPR	DPDP Act
Who exactly is collecting my data?	Yes — full legal name and registered address required	Yes — but less specific detail required

Question You Might Ask	GDPR	DPDP Act
Why exactly are you collecting each piece of my data?	Yes — every purpose must be listed separately and specifically	Yes — but a general purpose statement is acceptable
Which specific companies are you sharing my data with?	Yes — must name them or clearly define the category	Not explicitly required under the current framework
How long will you keep my data?	Yes — specific retention periods must be stated	Not explicitly required
Is my data going outside the country?	Yes — must disclose and explain what protections are in place	Government can restrict transfers but detailed disclosure rules are less defined
What is your legal basis for collecting this?	Yes — must clearly state which legal basis applies	Not required to specify a legal basis
What are all my rights?	Yes — all eight rights must be listed clearly and explained	Partial — key rights mentioned but not comprehensively listed
Who do I complain to if my rights are violated?	Yes — specific authority named with contact details	Yes — Data Protection Board mentioned
Can I get a copy of all data you hold about me?	Yes — right of access is explicitly guaranteed and detailed	Yes — right to access exists but procedures are less defined
Can I ask you to delete my data?	Yes — strong Right to Erasure with specific conditions	Limited — erasure rights exist but are not as clearly defined

What To Do If Your Data Rights Are Violated

A violation of your data rights happens when an organization does any of the following without your knowledge or consent:

- Collects your data without your consent — signing you up for marketing emails without you agreeing, or collecting your location data when you never permitted it.

- Uses your data for a purpose you never agreed to — you gave your email for a delivery notification and they sold it to an insurance company.
- Refuses to delete your data when you ask — the company ignores or stalls your deletion request indefinitely.
- Shares your data with third parties without telling you — your health app shares your medical information with advertisers without disclosing this anywhere.
- Stores your data insecurely leading to a breach — poor security practices result in your personal information being leaked or stolen.
- Denies you access to your own data — you ask a company what data they hold about you and they refuse to respond.
- Does not respond to your complaints — you raise a grievance with the company and they ignore it completely.

Step 1 — Complain Directly to the Organization

This is the same under both laws and always the first step. Every organization that collects data must have a grievance or complaint mechanism. Write to them formally — email is sufficient — stating what your complaint is, what right you believe was violated, and what you want them to do about it.

- **Under GDPR** — the organization must respond within one month. If the request is complex they can extend to three months but must tell you why.
- **Under DPDP** — the organization must have a grievance officer and respond within a reasonable timeframe. The specific deadline is left to rules the government is still finalizing — a significant weakness of the current framework.

Step 2 — Escalate to the Regulator

If the organization does not respond or responds inadequately, this is where the two laws diverge most significantly.

Under GDPR:

You complain to your country's Independent Data Protection Authority (DPA) — a fully independent body whose entire job is data privacy and nothing else. It is not a telecom regulator that also handles data. It exists solely to protect your data rights. The complaint is free of charge, fully online, and the DPA is legally obligated to investigate. They can demand documents from the company, interview staff, conduct audits, and impose fines — all without needing court approval.

Under DPDP:

You complain to the Data Protection Board of India. The complaint process is intended to be digital — an online portal. However, the Board is government-appointed rather than independent, which raises questions about how aggressively it will act against powerful corporations or government entities. As of

2026, the rules governing complaint timelines and processes are still being finalized.

Step 3 — Legal Action

- **Under GDPR** — You can take the organization to court independently of the DPA complaint without waiting. You can also authorize a nonprofit or consumer rights organization to take legal action on your behalf. Class action complaints — where many affected individuals complain together — are explicitly supported and have resulted in massive fines against companies like Meta and Google.
- **Under DPDP** — Direct court action on data privacy grounds is not as straightforwardly available. The primary route remains through the Data Protection Board. Appeals from the Board's decisions go to TDSAT and then to High Courts. There is no explicit provision for consumer organizations to file complaints on behalf of groups of affected individuals the way GDPR allows.

Step 4 — Penalties the Violator Faces

- **Under GDPR** — Fines of up to EUR 20 million or 4% of global annual turnover — whichever is higher. This is what makes GDPR genuinely feared by large corporations. 4% of Google's global revenue is billions of dollars. Companies actually change their behaviour because the financial risk is existential.
- **Under DPDP** — Fines of up to INR 250 crore per violation. Significant for Indian companies — but not linked to global turnover, meaning a multinational that makes thousands of crores in India faces a capped penalty that may not meaningfully deter them.

What a User Can Do — GDPR vs DPDP

Action	Under GDPR	Under DPDP Act
First step	Complain directly to the organization	Complain directly to the organization
Organization response deadline	Legally must respond within 1 month	No fixed statutory deadline — rules still pending
Escalation authority	Independent Data Protection Authority — fully independent of government	Data Protection Board of India — government-appointed
Filing a complaint	Free, online, legally obligated to investigate	Digital process — full mechanism still being finalized
Regulator's powers	Can audit, demand documents, interview staff, impose fines independently	Powers defined but independence is limited

Action	Under GDPR	Under DPDP Act
Direct court action	Yes — independently of regulator complaint	Limited — primary route is through the Board first
Group / class action	Explicitly supported — nonprofits can act on your behalf	No explicit provision for group complaints
Maximum penalty	EUR 20M or 4% of global turnover — whichever is higher	Up to INR 250 crore per violation — capped
Right to compensation	Individuals can claim financial compensation for damages	Compensation mechanism not clearly defined yet
Appeal process	Court system with clear, well-established pathway	TDSAT then High Court — longer and less direct
Single point of complaint?	Yes — always the DPA, regardless of sector or violator	No — depends on who violated your rights and which sector
Awareness & accessibility	Well established — citizens know their rights and how to use them	Still nascent — most Indians unaware of how to use these rights

The Fragmented Complaint Landscape in India

One of the most critical weaknesses of the DPDP Act as it stands in 2026 is that there is no single point of complaint redressal. Where you go depends entirely on who violated your rights and what type of data was involved.

If This Happens...	You Currently Go To...
Bank misused your data	RBI Banking Ombudsman
Telecom company shared your number	TRAI
E-commerce platform leaked your details	Consumer Forum
Hospital leaked your medical records	No clear authority yet
A random app sold your data	Data Protection Board — not yet fully operational
A government body misused your Aadhaar	Nowhere clearly defined
Social media platform violated your privacy	Data Protection Board — not yet functional in practice

Under GDPR the answer is always the same regardless of who violated your rights or what sector they operate in — one complaint, one authority, one clear process. In India you first have to figure out which sector the violator belongs to, then which regulator covers that sector, then whether that regulator even has jurisdiction over data privacy specifically — and then navigate a complaint process that may or may not have a defined timeline.

> *For an ordinary person — a farmer, a student, a homemaker, a small business owner — this fragmentation is effectively the same as having no recourse at all. Most people will simply give up before they even file a complaint.*

Practical Steps an Indian User Can Take Right Now

While the Data Protection Board becomes fully operational, here is what you can actually do today:

- **Raise a formal written complaint with the company first**

  Email creates a paper trail and many companies will respond to avoid regulatory exposure. Keep all records of your communication.

- **Complain to TRAI**

  If the violation involves telecom data or unsolicited calls — TRAI's Do Not Disturb registry and complaint mechanism is functional today.

- **Complain to RBI's Banking Ombudsman**

  If the violation involves a bank or financial institution misusing your financial data.

- **File a consumer complaint**

  With the National Consumer Disputes Redressal Commission — data misuse can in some cases be argued as a deficiency of service.

- **Consult a lawyer**

  If the violation is serious — especially in cases of identity theft, financial fraud from data misuse, or large-scale unauthorized sharing of sensitive information.

> *The gap between having rights and being able to enforce them is the most important unresolved challenge of India's data privacy landscape in 2026. The Data Protection Board, once fully operational, is supposed to become that single point of redressal. Until it is live, staffed, independent, and publicly accessible — the fragmentation remains the single biggest gap between what the DPDP Act promises and what it actually delivers for ordinary Indians.*

The Bigger Picture

The gap between GDPR and DPDP is not because India does not care about privacy. GDPR was built over decades of legal evolution and a deeply rooted consumer rights culture in Europe. India's DPDP Act is version 1.0 — a genuine and important first step. The expectation across the legal and policy community is that it will become more detailed, more specific, and more enforceable as implementation matures and case law develops over time.

India is one of the world's largest digital markets. As more services move online — banking, healthcare, education, entertainment — the importance of privacy will only grow. For individuals, privacy is becoming a basic digital skill. For businesses, it is becoming a legal and ethical responsibility.

> *The most important thing to remember: your personal data is not just information. It is an extension of your identity. Understanding how it is collected, used, and protected is one of the most important forms of digital literacy in the 21st century.*