# Tired of Spam Calls? How the DPDP Rules, 2025 Put You Back in Control. The Daily Nuisance We All Know

Thought Leadership • November 15, 2025

*'First published on Enterprise IT World'*

*By: Subroto Kumar Panda*

**If you are using a phone, chances are you've been bombarded by calls like these:**

- "Sir, would you like to transfer your car loan to another bank?"
- "Sir/Ma'am, we have an amazing health insurance plan for you!"
- "Invest in property today for guaranteed returns!"

These calls often come at the worst times—during meetings, family dinners, or even while you're driving. For years, despite TRAI's "Do Not Disturb" (DND) registry and RBI guidelines, these telemarketing calls continued unchecked. Why? Because enforcement was weak, loopholes were exploited, and your personal data was treated like a free-for-all.

We've all been there. You're in the middle of a meeting, and your phone buzzes. You pick it up, and it's an agent offering to help you transfer your car loan. An hour later, another call comes in, this time from an insurance provider with a "limited-time offer," followed by someone offering a loan against your property.

This constant digital intrusion persisted despite nascent frameworks like TRAI's "**Do Not Disturb**" (**DND**) registry and various RBI guidelines. The reason for this failure was simple: the old system lacked **legal teeth**, enforcement was inconsistent, and the very concept of "consent" was a legal fiction, often buried in 50-page terms of service agreements.

With the DPDP Rules, that entire framework is now obsolete. The rules re-architect the relationship between the individual (the "Data Principal") and the corporation (the "Data Fiduciary"), shifting the balance of power decisively back to the citizen.

**Pillar 1: The Demise of "Implied" Consent (Rule 3)**

The single greatest weapon against the telemarketing industry is the new, robust definition of **consent**. The era of "**hidden consent**" is over.

**Under Rule 3**, any Data Fiduciary (the bank, the insurance company, the real estate firm) processing your personal data must provide a clear and specific notice *before* collection. This notice is legally mandated to be:

1. **Clear, Simple, and Independent:** The request for consent must be presented in "clear, simple and plain language" and must be "understandable independently" of any other information. This explicitly outlaws bundling consent for telemarketing within a primary service contract.
2. **Itemised and Specific:** The notice must provide an "itemised description" of the personal data to be collected (e.g., "Your Phone Number, Your Email"). Crucially, it must also state the "specified purpose".
3. **Purpose Limitation:** If the purpose stated is "Processing a car loan application," that data *cannot* be legally used for a cross-promotional "health insurance" call. To use it for a new purpose, the company must seek *new, specific consent*.

**This change is seismic**. A bank can no longer share your data with its insurance or real estate partners just because you opened an account. That "consent" would be void under the new law.

**Pillar 2: The Enforceable "Right to Withdraw" (The Kill-Switch)**

This is perhaps the most powerful tool granted to citizens. The rules formalise your right to withdraw consent at any time.

The legal standard is "comparable ease".

The rules state that the ease of withdrawing consent *must be comparable* to the ease with which it was given. This means if a user "consented" with a single click on an app, the Data Fiduciary cannot legally require them to "call a helpline" or "send a written request" to opt out. They must provide a one-click withdrawal mechanism.

For every telemarketer, this creates an immediate legal obligation. The moment you state your withdrawal, their legal basis for processing your data (i.e., making the call) evaporates.

**Pillar 3: The New Enforcement and Adjudication Regime**

Where the DND registry failed due to a lack of consequences, the DPDP framework succeeds by creating a powerful, two-tiered enforcement structure.

**1. Internal Accountability: Grievance Redressal (Rule 14)**

Every Data Fiduciary must establish an effective **grievance redressal system**. When a user lodges a complaint (for instance, "I withdrew my consent, but your agents are still calling"), the company is legally bound to respond and resolve the issue within a "reasonable period not exceeding ninety

days".

**2. External Adjudication: The Data Protection Board (DPB)**

If the company fails to resolve the grievance, citizens can now escalate the complaint to the **Data Protection Board of India**. This is the new, quasi-judicial body with the power to investigate, adjudicate, and—most importantly—impose significant financial penalties on non-compliant Data Fiduciaries.

This is the "teeth" that was always missing. The Board transforms your complaint from a mere data point into a potential legal and financial liability for the offending company.

**Your New Legal Action Plan Against Unwanted Calls**

Effective today, every individual has a clear, four-step legal recourse when receiving an unwanted call :

1. **Challenge the Legal Basis:** Ask the caller to identify their Data Fiduciary and state the legal basis for the call. Demand they provide a copy of the specific, itemised notice where you gave consent for this exact purpose (e.g., "for property loan marketing").
2. **Execute Your Right to Withdraw:** Inform the caller, "I am, under my rights granted by the DPDP Rules, formally withdrawing all consent for my personal data to be processed for this purpose, effective immediately".
3. **Initiate Grievance Redressal:** If the calls persist, file a formal complaint with the company's Grievance Officer (whose details must be publicly available). This begins the 90-day resolution clock under Rule 14.
4. **File for Adjudication:** If the company ignores the complaint or fails to provide a satisfactory resolution, file a formal complaint with the Data Protection Board of India for adjudication and penalties.

**The Structural Future: The Rise of the "Consent Manager" (Rule 4)**

Finally, the rules lay the groundwork for a long-term technological solution: the **Consent Manager**.

This is a new class of entity, a registered "personal agent" that acts as a digital intermediary on your behalf. Think of it as a unified privacy dashboard for your entire digital life.

Through a registered Consent Manager, you will be able to:

"give, manage, review and withdraw" all your data consents for every company from a single, trusted platform.

Want to stop all insurance-related offers? You will simply flip a switch in your Consent Manager, which will then have the legal authority to communicate your withdrawal to all relevant Data Fiduciaries on your behalf.

**Conclusion: The New Burden of Proof**

The DPDP Rules, 2025, fundamentally alter India's data landscape. **They replace digital anarchy with digital sovereignty.** For the telemarketing industry, the business model of purchasing and exploiting ambiguous data lists is now defunct.

The burden of proof has shifted. It is no longer your job to prove you *didn't* consent; it is their job to prove, with clear and specific evidence, that you *did*.