CHANNELFORCE · DATA PROTECTION

Your leads are yours

Brokers ask us a fair question: **"if my leads sit on your system, who can see my customers' phone numbers?"** Here is the straight answer — what the software prevents, what we commit to, and what any hosted software provider can technically reach.

1. No other brokerage can ever see your data

This is not a setting or a screen filter — it is enforced by the database itself. Every table carries a **row-level security policy** that compares the requester's brokerage to the row's brokerage. A query for another firm's leads returns nothing, no matter how it is asked.

What that means in practice: a competing brokerage on Channelforce cannot see your leads, your customers, your bookings or your brokerage rates — even if they knew your company name, guessed a record ID, or tried to call the API directly. The wall is in the database, so the app, the mobile browser and any future integration all inherit it.

2. Your own team only sees what you allow

ROLE	LEADS THEY CAN OPEN	BROKERAGE FIGURES
Salesperson	Only leads assigned to them	**Hidden by default**
Pre-Sales / Telecaller	Their team's leads + unassigned	**Hidden by default**
Team Leader	Their team	Your choice
Zonal / City Head	Their zone or city	Your choice
Sales Head / Admin	All	**Yes**

Brokerage amounts, slabs and collections are masked **in the database** for roles that should not see them — not merely hidden on screen. A salesperson's export, their browser and any API call all return the same: nothing.

3. What the Channelforce team can and cannot see

We think you deserve a precise answer rather than a comfortable one.

Inside the product, we cannot see your leads. Our own logins are ordinary brokerage accounts and are bound by exactly the same database rules as everyone else. The one cross-brokerage view that exists for operating the service shows **only counts** — brokerage name, number of users, number of leads, and when the last lead arrived. It carries no customer names, no phone numbers, no notes, no money.

The honest caveat, true of every hosted software provider. Channelforce runs on a database that we operate. As the operator, our administrators hold the credentials needed to run backups, fix faults and apply updates — and those credentials can technically read stored records. This is equally true of every CRM, accounting package and email service your business already uses. What protects you is not a claim of impossibility; it is what we commit to, and what we do not do.

4. What we commit to

- **We never use your data for our own purposes.** Your leads are not analysed for our benefit, not shared with other brokerages, not used to train anything, and never sold. Ever.
- **We do not go looking.** Administrative access to production data is used only to keep the service running or to fix something you have asked us to fix.
- **We do not contact your customers.** Under any circumstance.
- **Your data leaves whenever you want it to.** One click exports every record your brokerage owns as CSV — leads, activities, bookings, payments. No notice period, no request to us, no “contact sales to leave”.
- **Deletion on request.** Ask, and your brokerage's data is removed from the live system.

5. How your customers' details are handled

- Traffic between your browser and Channelforce is encrypted (TLS); stored data is encrypted at rest by our infrastructure providers.
- Passwords are never stored in readable form — only as salted hashes, which cannot be reversed.
- Your brokerage is the **data controller** for your customers' details; Channelforce processes them on your instructions. If a customer asks you to correct or delete their record, you can do it yourself, and we will help if you need us to.
- Lead sources (Meta, Google, your website) deliver to **your** private webhook, keyed to your brokerage alone.

Want this in writing for your records? We will sign a data-processing agreement covering everything on this page. Write to **founder@channelforce.co.in**.