

PRIVACY AMBASSADOR IN ACTION

Department-Wise
Implementation
Guide



MARKETING & SALES DEPARTMENT

**Drivers of Data and
Customer Engagement**

The Marketing & Sales Department is responsible for collecting and using personal data to communicate with customers and prospects across marketing and sales activities.

According to the DPDP framework, they are required to ensure compliance with data protection requirements by relying on valid and purpose-specific consent, providing transparent notices, respecting user choices across channels, and enabling responsible targeting and outreach practices.

DPDP FRAMEWORK APPLICATION AREAS



Messaging
Platforms



SMS and Voice
Communications



Targeted Advertising
and Profiling



Email
Marketing



CRM and Lead
Management Systems



Campaign
Analytics



Customer Retention
and Reactivation Campaigns

Data Processing

Requires validating consent scope for each campaign, including profiling, segmentation, and targeted advertising by ceasing communications, across all channels after withdrawal of consent.

Data Storage

Requires retaining marketing processing logs and related traffic data for at least one year, including after account deletion or erasure, unless a longer period is legally required.

Data Collection

Requires collecting customer and prospect personal data only where supported by valid, active, and purpose-specific consent, including consent obtained by clearly specifying the end use of collected data.

Data Erasure

Requires periodical cleansing of databases to remove inactive, expired, or non-consented records. Provide at least 48 hours' advance notice to users before erasing personal data.

KEY ACTIONS



Confirm that marketing agencies, platforms, and technology vendors operate under valid written contracts for engaging Data Processor.



Provide clear and accessible opt-out mechanisms in all forms of communication and mention Data Principal rights and grievance mechanisms.



Obtain verifiable parental or lawful guardian consent before processing a child's personal data, using due diligence mechanisms such as digital identity tools or authorised virtual tokens.



Coordinate regularly with legal and compliance teams to ensure marketing activities remain aligned with DPDP guidelines and applicable sector-specific norms.



Align marketing tools, automation platforms, and vendors with the organisation's personal data breach and incident response framework.



Identify and flag campaigns involving children or high-risk audiences at the planning stage and apply enhanced safeguards, including prohibition of tracking and disabling behavioural monitoring of children or targeted ads, unless a lawful exemption is documented.

SUPPORTED BY



CRED



IIFL
FINANCE



Kempegowda
INTERNATIONAL
AIRPORT
BENGALURU



PRIVASAPIEN
Evolution for the Privacy & AI Era



Protectt.ai



Providence



PNB



QRC
Quality • Trust • Compliance
be assured. be secured



SQ1
nextgen cybersecurity



target



ZS



Follow us on social media channels for Data Privacy Day 2026 awareness content!