DAILY FLOWERS INDIA PVT. LTD.

Daily Flowers Privacy Policy

Version 1.0.0 Status: Draft Effective: Not yet in force

Applies to: Customers, gift recipients, website and app visitors, and contact persons of business customers

DRAFT — FOR LEGAL REVIEW

Effective date: [EFFECTIVE DATE — TO BE CONFIRMED ON PUBLICATION] · **Version:** 1.0.0

This Privacy Policy explains how Daily Flowers India Pvt. Ltd. handles personal data when you visit the Daily Flowers website or app, create an account, place or receive an order, subscribe, contact us, or deal with us on behalf of a business. It is written to be read on its own, without needing any other document.

In short: we collect the information needed to take, prepare and deliver your orders and to support you; we share it only with those who help us do that; we send marketing only with your consent; we do not sell your personal data; and you can ask us at any time to see, correct or erase your data, withdraw consent, nominate someone to act for you, or complain.

Part 1 — About this Policy

1.1 Who is responsible for your data

Daily Flowers India Pvt. Ltd., a company incorporated under the Companies Act, 2013, having its registered office at [REGISTERED OFFICE ADDRESS] (CIN [CIN]) (**Daily Flowers**, **we**, **us**), decides why and how your personal data is processed on the Platform and is the **Data Fiduciary** for it. "Platform" means https://dailyflow-ersai.com and the Daily Flowers mobile applications.

Contact for any question about this Policy or your personal data:

Role	Contact
Person who answers questions on processing of personal data / Data Protection Officer (if appointed)	[NAME / DESIGNATION / CONTACT — TO BE CONFIRMED]
Grievance Officer	[NAME / DESIGNATION / CONTACT — TO BE CONFIRMED]

DRAFT — FOR LEGAL REVIEW

General privacy mailbox	[PRIVACY EMAIL — TO BE CONFIRMED BY MANAGEMENT], or support@dailyflowersai.com until a dedicated mailbox is set up

1.2 Whose data this Policy covers

This Policy covers: (a) customers who browse, sign in or order; (b) gift recipients whose details a customer gives us; (c) visitors to the Platform; (d) people who contact our support team or send a business enquiry; and (e) contact persons of business customers. Independent sellers, franchise operators, delivery partners, suppliers and job applicants receive separate privacy notices with their agreements.

1.3 The law that applies

We process personal data in accordance with the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which continue to apply until the relevant provisions of the Digital Personal Data Protection Act, 2023 (**DPDP Act**) take effect, and with the DPDP Act and the Digital Personal Data Protection Rules, 2025 (**DPDP Rules**) as their provisions come into force. The DPDP Rules were published on 13 November 2025; the provisions on Consent Managers apply from November 2026 and most other obligations from May 2027. We have written this Policy to the standard of the DPDP Act now, so that you have those rights and protections from today where we can practically provide them.

Part 2 — The personal data we process

We collect only what is needed for the purposes in Part 3. The items marked "required" are needed to provide the service; if you do not provide them, we cannot complete that service.

Category	Items of personal data	Where it comes from	Required or optional
Identity and contact	Your name; mobile number and the date it was verified; email address and whether and how it was verified	You	Mobile number and name required to order; email optional unless needed for invoices

DRAFT — FOR LEGAL REVIEW

Sign-in and security	One-time passcodes (stored only in scrambled form and for a short time); number of sign-in attempts; date and time of sign-in; IP address and browser or device description of your session; records of security events such as repeated failed attempts	Generated when you sign in	Required
Addresses	Delivery addresses, labels (such as "Home" or "Office"), landmark, delivery instructions, pincode and city; map coordinates we derive from the address to plan delivery	You; coordinates derived by us	Required for delivery
Recipients	Name, mobile number and address of the person receiving a gift; optional relationship to you; gift message	You	Required to deliver a gift
Occasions	Occasions you choose to save (such as a birthday or anniversary), the date, the recipient, and whether you want reminders	You	Optional

DRAFT — FOR LEGAL REVIEW

Orders and subscriptions	Products, sellers, prices, discounts and offers applied, delivery date and slot, order status, subscription schedule, skips and pauses, invoices, and your GSTIN and business name if you give them	You and our systems	Required
Payments	Payment status, amount, payment method type, transaction and refund references and, where shown to us by the payment aggregator, the last digits of a card and the issuing bank. We do not receive your full card number, card security code, UPI PIN or net-banking password	Payment aggregator	Required
Delivery records	Delivery code confirmation, time of delivery, delivery attempts and reasons for failure, photograph of the handover, signature or site acknowledgement where used, and the delivery partner assigned	Delivery partner and our systems	Required

DRAFT — FOR LEGAL REVIEW

Support and complaints	Messages, calls and emails you send us, complaint details, photographs or videos you provide as evidence, and our responses	You	Optional, but needed to resolve a complaint
Feedback and reviews	Ratings, comments, tags and reviews	You	Optional
Communication preferences and consents	Your marketing choices, and for each consent: whether given or withdrawn, when, and through which channel; records of messages sent to you (channel, address, content and delivery status)	You and our systems	Required to honour your choices
Usage and device information	Pages or screens viewed and actions such as viewing a product or starting checkout, with the page address and time; IP address; browser type; approximate area derived from the pincode you enter	Automatically when you use the Platform	Collected automatically — see Part 7
Serviceability and enquiries	Pincode and, if you choose to give it, your mobile number when you check whether we deliver to an area we do not yet serve; business enquiry details	You	Optional

DRAFT — FOR LEGAL REVIEW

Business customer contacts	Name, designation, work email and telephone of people who manage a business account	You or your employer	Required for business accounts

Sensitive information. We do not ask for information about health, sexual orientation, biometrics or other sensitive categories. Customers sign in with a one-time passcode, so we do not hold customer passwords. Where we need bank account details to pay a refund that cannot be returned to the original payment method, we collect them only with your consent and only for that refund.

Part 3 — Why we use your data, and on what basis

We use personal data only for the purposes below. Where we rely on your **consent**, you may withdraw it at any time (Part 4). Where you have **voluntarily provided** data for a specified purpose and not objected to its use, the DPDP Act permits us to use it for that purpose without separate consent (section 7(a)). Some processing is needed to **comply with law** or a lawful order, or to **establish, exercise or defend legal claims** or **prevent and detect fraud and offences**, as the DPDP Act permits.

Purpose	Data used	Basis
Create and secure your account; verify your mobile number and email; keep you signed in	Identity and contact; sign-in and security	Voluntarily provided for this purpose; security safeguards required by law
Take, confirm and invoice orders; operate subscriptions; process payments and refunds	Identity; orders; payments; addresses	Voluntarily provided for this purpose; tax and accounting law
Prepare and deliver orders, including gifts; verify delivery by delivery code, photograph or signature; handle failed deliveries	Addresses; recipients; orders; delivery records	Voluntarily provided for this purpose (see Part 6 for recipient data)

DRAFT — FOR LEGAL REVIEW

Send transactional messages — pass-codes, confirmations, delivery updates and codes, payment, refund and com-plaint updates	Contact details; orders	Voluntarily provided for this purpose
Answer questions, investigate com-plaints, provide replacements and re-funds	Support records; orders; delivery records; photographs	Voluntarily provided for this purpose; consumer protection law
Send occasion reminders you asked for	Occasions; recipients; contact details	Consent
Send marketing messages and offers	Contact details; order history; prefer-ences	Consent (never pre-ticked)
Recommend products and personalise what you see based on your past orders on the Platform	Orders; preferences; usage	Consent, where required; you can switch personalisation off in your account set-tings [TO BE CONFIRMED BY MAN-AGEMENT]
Understand how the Platform is used and improve it	Usage and device information, mostly in aggregated form	Voluntarily provided / consent where re-quired — see Part 7
Prevent fraud, abuse of offers or refunds, spam and attacks; protect our customers, staff and partners	Sign-in and security; usage; orders; pay-ments	Prevention and detection of fraud and of-fences; security safeguards required by law
Meet legal, tax, audit and regulatory du-ties; respond to lawful requests of courts and authorities	Records needed for the duty	Compliance with law and lawful orders
Establish, exercise or defend legal claims	Records relevant to the claim	Enforcement of legal rights and claims
Manage business accounts, credit and invoicing	Business contact details; orders; pay-ments	Voluntarily provided for this purpose; contract with the business

DRAFT — FOR LEGAL REVIEW

Automated decisions. We use automated rules to detect suspected fraud or misuse (for example, too many passcode requests from one network). Any decision to close an account or refuse a refund because of such a flag is reviewed by a person, and you may ask us to explain it.

No sale of personal data. We do not sell or rent your personal data, and we do not share it with third parties for their own marketing.

Part 4 — Consent and how to withdraw it

When we ask for consent, we explain what it is for, ask you to give it by a clear action (such as ticking an unticked box), and record when and through which channel you gave it. Consent to marketing is never a condition of buying.

You can withdraw consent at any time, as easily as you gave it:

- in your account under communication preferences;
- by using the unsubscribe link in any marketing email or replying "STOP" to a marketing message where offered; or
- by writing to [PRIVACY EMAIL — TO BE CONFIRMED BY MANAGEMENT] or support@dailyflowersai.com.

Withdrawal does not affect processing that took place before it, and does not stop the transactional messages and processing needed to complete orders you have already placed or to meet our legal duties. After withdrawal we stop the processing that relied on consent within a reasonable time, and ask our service providers to do the same.

Consent Managers. From the date the Consent Manager provisions of the DPDP Act apply, you may also give, manage, review and withdraw your consent to us through a Consent Manager registered with the Data Protection Board of India, once we are connected to one. We will publish the details here when that is available. [CONSENT MANAGER INTEGRATION — TO BE CONFIRMED BY MANAGEMENT]

Part 5 — Who we share your data with

We share personal data only with the categories of recipient below, only as much as each needs, and only for the purpose stated. Service providers who process data on our behalf (**Data Processors**) act on our instructions

DRAFT — FOR LEGAL REVIEW

under written contracts that require reasonable security safeguards, confidentiality and deletion or return of data when the service ends.

Recipient	What they receive	Why	Role
Independent sellers (flower partners, food and bakery sellers, gift sellers) whose products you order	Recipient name, delivery address and mobile number; order details and gift message; your name where needed for the invoice or packing slip	To prepare, pack, ship and invoice your order and resolve complaints	Separate business responsible for its own use; bound by our seller agreements to use the data only for your order
Daily Flowers network fulfilment partners and franchise operators	Order details, recipient name, address, mobile number and gift message	To prepare and deliver Daily Flowers orders on our behalf	Data Processor
Delivery partners and courier or logistics companies	Recipient name, mobile number, address, landmark, delivery slot, package description and value	To deliver and track your order and confirm delivery	Data Processor for deliveries we arrange
Payment aggregator (currently Razorpay) and banks	Order amount, reference, and the contact details needed to process the payment or refund	To collect payments, process refunds and prevent payment fraud	Regulated by the Reserve Bank of India; processes payment data under its own legal obligations and our instructions
Messaging and email providers (SMS, WhatsApp, email)	Your mobile number or email and the content of the message	To deliver passcodes, order updates and, with consent, marketing	Data Processor
Cloud hosting, data storage, security and bot-protection providers	All categories stored on or passing through the Platform	To host and secure the Platform	Data Processor

DRAFT — FOR LEGAL REVIEW

Mapping and address services	Address text and pincode only — never your name or mobile number	To locate delivery addresses and plan routes	Data Processor
Analytics and business-reporting services, including the CFO and AROS finance and operations services of Snxw-Fairies Innovations Pvt. Ltd.	Aggregated sales, finance and operations figures. Individual consumer names, mobile numbers and addresses are not sent. Business customers' names may appear in invoice and receivable records	To produce accounts, reports and operational analysis for Daily Flowers	Data Processor acting only on our documented instructions
Artificial-intelligence services used to summarise business reports	Aggregated business figures, with personal data removed before sending	To help management read reports	Data Processor; not permitted to use the data to train its models
Professional advisers, auditors and insurers	Records relevant to their engagement	Legal, audit, tax and insurance purposes	Bound by professional confidentiality
Government, courts, regulators and law-enforcement authorities	Data they lawfully require	To comply with law, a court order or a lawful request	Independent authority
A buyer of, or successor to, our business	Records relating to the transferred business	Merger, acquisition or restructuring, subject to this Policy	New Data Fiduciary, bound to honour this Policy

On request, we will give you the names of the Data Fiduciaries and Data Processors with whom your personal data has been shared, and a description of what was shared (Part 11).

Part 6 — Gift recipients and children

6.1 Recipients

DRAFT — FOR LEGAL REVIEW

When you send a gift, you give us the recipient's name, mobile number and address. We use these only to prepare and deliver the gift, to send the recipient delivery updates and the delivery code, and to handle any delivery problem or complaint. We do not send marketing to a recipient unless the recipient separately becomes our customer and consents. A recipient may contact us at any time to ask what we hold about them, to correct it, or to ask us to erase it once the delivery and any related complaint or legal retention period have ended. By giving us a recipient's details you confirm that you are entitled to do so for the purpose of the delivery.

6.2 Children

Our Platform is meant for adults. We do not knowingly allow anyone under eighteen to create an account or place orders. If we need to process a child's personal data other than as a gift recipient, we will first obtain verifiable consent from a parent or lawful guardian in the manner the DPDP Rules require, by checking that the person giving consent is an identifiable adult through reliable identity and age details or an authorised virtual token. We do not track or monitor the behaviour of children, or direct targeted advertising at them. When a gift is addressed to a child, we use the child's name and delivery details only to deliver the gift. If you believe we hold a child's data without proper consent, please contact us and we will act promptly.

Part 7 — Cookies, local storage and analytics

We keep tracking to a minimum and do not use third-party advertising cookies or trackers.

Technology	What it does	Can you refuse it?
Sign-in cookie	A strictly necessary cookie that keeps you signed in securely. It is not readable by scripts on the page and expires after a limited period or when you sign out	No — the Platform cannot keep you signed in without it
Cart and preference storage in your browser	Stores your cart contents, gift message draft and whether you dismissed our cookie notice, on your own device	You can clear it through your browser; your cart will be emptied

DRAFT — FOR LEGAL REVIEW

First-party activity measurement	Records actions such as viewing a product or starting checkout, with the page address, time and IP address, to understand how the Platform is used and to stop abuse. It does not use a third-party analytics tool	[TO BE CONFIRMED BY MANAGEMENT — opt-out setting]
Cookieless web analytics (Cloudflare Web Analytics)	Counts page visits and performance in aggregate without placing cookies	It does not identify you personally
Bot protection on public forms	A security check on the business enquiry and serviceability forms that distinguishes people from automated programs	Required to submit those forms
Sign in with Google (staff pages only)	Used only on staff sign-in pages, not by customers	Not applicable to customers

If we introduce any non-essential cookie or tracker in future, we will ask for your consent before it is used and update this Policy.

Part 8 — How long we keep your data

We keep personal data only for as long as it is needed for the purpose for which it was collected, or for longer where the law requires. When that period ends, we erase the data or irreversibly de-identify it, and instruct our Data Processors to do the same.

Record	Retention period
Account and profile data	While your account is active, and for [PERIOD — TO BE CONFIRMED BY MANAGEMENT] after your last activity or account closure

DRAFT — FOR LEGAL REVIEW

Order, invoice and payment records	For the period required by tax and company law — including the period under section 36 of the Central Goods and Services Tax Act, 2017 (72 months from the due date of the annual return for the year) and eight financial years for books of account under section 128(5) of the Companies Act, 2013 — or longer if a dispute is pending
Delivery records including handover photographs	[PERIOD — TO BE CONFIRMED BY MANAGEMENT], and in any case not less than one year from the delivery as the DPDP Rules require
Complaints and support records	[PERIOD — TO BE CONFIRMED BY MANAGEMENT] after the complaint is closed, or until any proceeding is finally decided
Marketing consents and withdrawal records	For as long as the consent is relied on and for [PERIOD — TO BE CONFIRMED BY MANAGEMENT] afterwards, to prove our compliance
Security logs, sign-in records and processing logs	At least one year from the processing, as the DPDP Rules require, and at least 180 days as CERT-In directions require
Passcodes	Minutes; a passcode expires shortly after it is issued and cannot be reused
Audit trail of actions on the Platform	[PERIOD — TO BE CONFIRMED BY MANAGEMENT]; personal identifiers in the audit trail are de-identified when the period for the underlying record ends
Saved recipients and occasions	Until you delete them or close your account
Serviceability requests from areas we do not serve	[PERIOD — TO BE CONFIRMED BY MANAGEMENT]

If you do not use your account for the period after which we would otherwise erase your data, we will tell you at least forty-eight hours before erasure, so that you can sign in or contact us if you want us to keep it.

DRAFT — FOR LEGAL REVIEW

Part 9 — Where your data is stored and transferred

Our Platform and our main customer records are hosted in India. Some of our service providers — such as messaging, email, mapping and artificial-intelligence service providers — may process data on servers outside India. Where that happens, we transfer only the data the provider needs, under contracts that require protection at least equal to that required by Indian law, and we will not transfer personal data to any country or territory that the Central Government has restricted under section 16 of the DPDP Act, or in breach of any requirement specified under the DPDP Rules. Payment data is stored in India by our payment aggregator as required by the Reserve Bank of India.

Part 10 — How we protect your data

10.1 Security safeguards

We take reasonable security safeguards to prevent personal data breaches, including:

- encryption of data in transit and of stored secrets such as provider keys, and storing passcodes only in scrambled form;
- access controls based on job role, with additional confirmation for sensitive actions, and masking of personal data for staff who do not need to see it;
- logs of access to personal data, with monitoring and review to detect and investigate unauthorised access;
- limits on repeated sign-in and passcode requests to prevent account takeover and misuse;
- backups and recovery arrangements so that the service can continue if data is lost or unavailable;
- written security and confidentiality obligations on every Data Processor; and
- security reviews of new features before release.

We follow a documented information security programme that includes the managerial, technical, operational and physical controls required under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ([SECURITY STANDARD OR CERTIFICATION — TO BE CONFIRMED BY MANAGEMENT]). No system is completely secure, but we work continuously to keep your data safe.

10.2 If there is a personal data breach

DRAFT — FOR LEGAL REVIEW

If a personal data breach affects you, we will tell you without delay, in clear language, through your account or the contact details you have registered with us: what happened and when, the likely consequences for you, what we have done and are doing to reduce the risk, what you can do to protect yourself, and whom to contact. We will also report the breach to the Data Protection Board of India without delay and give it a detailed report within seventy-two hours of becoming aware of it (or any longer period the Board allows), and report cyber incidents to CERT-In within the time its directions require.

Part 11 — Your rights

11.1 Rights you have

Right	What it means
Access	Obtain a summary of the personal data we hold about you and the processing we carry out, and the identities of the Data Fiduciaries and Data Processors we have shared it with, with a description of what was shared
Correction, completion and updating	Have inaccurate or misleading data corrected, incomplete data completed, and out-of-date data updated. Many details can be changed directly in your account
Erasure	Have your personal data erased when it is no longer needed for the purpose for which it was collected, unless we must keep it to comply with the law (for example, tax invoices) — in which case we will tell you what we keep and why, and restrict its use to that legal purpose
Withdraw consent	Withdraw any consent you have given, as described in Part 4
Grievance redressal	Have a complaint about our handling of your personal data dealt with by our Grievance Officer

DRAFT — FOR LEGAL REVIEW

Nomination	Nominate one or more individuals to exercise your rights if you die or become unable to exercise them because of unsoundness of mind or infirmity of body
Complaint to the Data Protection Board	Complain to the Data Protection Board of India after using our grievance process

11.2 How to exercise your rights

Send your request through [ACCOUNT PRIVACY SETTINGS / REQUEST FORM — TO BE CONFIRMED BY MANAGEMENT] or by email to [PRIVACY EMAIL — TO BE CONFIRMED BY MANAGEMENT] (or support@dailyflowersai.com), from or quoting your **registered mobile number** and, where relevant, your **order number**. To protect you, we will verify your identity — usually by a one-time passcode sent to your registered mobile number — before acting. A nominee must provide proof of identity, the nomination and, where applicable, proof of death or incapacity. To register a nominee, use [NOMINATION FORM — TO BE CONFIRMED BY MANAGEMENT].

We do not charge for handling a request. We will acknowledge your request promptly and respond within one month of receipt and, in any case, within the period required by law (which, under the DPDP Rules, may not exceed ninety days). If we cannot fully meet a request, we will explain why and tell you how to escalate it.

11.3 Your duties

The DPDP Act asks you, when exercising these rights, to comply with applicable law, not to impersonate anyone, not to suppress material information, not to file false or frivolous complaints, and to give only verifiably authentic information when asking for correction or erasure.

Part 12 — Grievance Officer and complaints

If you have a concern about how we handle your personal data, contact our Grievance Officer:

Item	Detail
Name	[NAME — TO BE CONFIRMED]
Designation	[DESIGNATION — TO BE CONFIRMED]

DRAFT — FOR LEGAL REVIEW

Email	[GRIEVANCE EMAIL — TO BE CONFIRMED]
Telephone	[GRIEVANCE TELEPHONE — TO BE CONFIRMED]
Address	Daily Flowers India Pvt. Ltd., [REGISTERED OFFICE ADDRESS]

We will acknowledge your grievance within forty-eight hours and resolve it within one month of receipt. If you are not satisfied with our response, or we do not respond within the period required by law, you may complain to the Data Protection Board of India through its online portal ([DATA PROTECTION BOARD COMPLAINT PORTAL URL — TO BE CONFIRMED]). The DPDP Act requires you to use our grievance process first. Our Grievance Redressal Policy describes all complaint routes.

Part 13 — Marketing and your choices

We send marketing by SMS, WhatsApp, email or app notification only with your consent, and respect the preferences you register with your telecom provider. We do not treat an order placed by telephone or WhatsApp as consent to marketing unless you give that consent through an explicit written or digital action. You can change your choices at any time (Part 4).

Part 14 — Links and third-party services

The Platform may link to websites or services of others, such as a payment page, a courier's tracking page or a seller's website. Those services have their own privacy policies, and we are not responsible for how they handle your data once you leave the Platform. The payment page is operated by our payment aggregator under its own privacy policy.

Part 15 — Changes to this Policy

We will update this Policy when our processing or the law changes. We will publish each version, with its version number and effective date, in the Legal & Agreements Centre at https://dailyflowersai.com/legal and keep earlier

DRAFT — FOR LEGAL REVIEW

versions available there. If a change is material — for example, a new purpose that needs your consent — we will tell you in advance and, where required, ask for your consent before the new processing begins.

Schedule 1 — Items to be confirmed by management before publication

No.	Item	Part	Status
1	Registered office address and CIN	1.1	[TO BE CONFIRMED BY MANAGEMENT]
2	Person answering processing questions / Data Protection Officer	1.1	[NAME / DESIGNATION / CONTACT — TO BE CONFIRMED]
3	Grievance Officer	1.1, 12	[NAME / DESIGNATION / CONTACT — TO BE CONFIRMED]
4	Dedicated privacy mailbox and request form	1.1, 4, 11	[TO BE CONFIRMED BY MANAGEMENT]
5	Personalisation setting and opt-out for activity measurement	3, 7	[TO BE CONFIRMED BY MANAGEMENT]
6	Consent Manager integration	4	[TO BE CONFIRMED BY MANAGEMENT]
7	Retention periods	8	[TO BE CONFIRMED BY MANAGEMENT]
8	Current list of Data Processors and their processing locations	5, 9	[TO BE CONFIRMED BY MANAGEMENT]

DRAFT — FOR LEGAL REVIEW

9	Security standard or certification	10	[TO BE CONFIRMED BY MANAGEMENT]
10	Nomination form	11	[TO BE CONFIRMED BY MANAGEMENT]
11	Data Protection Board complaint portal URL	12	[TO BE CONFIRMED]

Annexure — Legal basis and review notes

Statutes and rules relied on

Instrument	Provision	Used for
Digital Personal Data Protection Act, 2023	ss.2, 4–9, 11–17, 27; s.44(2)	Notice, consent, legitimate uses, safeguards, breach, erasure, children, rights, grievance, nomination, duties, cross-border transfer, Board, repeal of IT Act s.43A
Digital Personal Data Protection Rules, 2025 (G.S.R. 846(E), 13 November 2025)	rr.1, 3, 4, 6, 7, 8, 9, 10, 14, 15; Third and Seventh Schedules	Commencement, notice content, Consent Managers, security safeguards, breach intimation (72-hour Board report), retention (one-year minimum; 48-hour pre-erasure notice), contact publication, verifiable parental consent, rights and 90-day grievance ceiling, transfers
DPDP Act commencement notification (G.S.R. 843(E), 13 November 2025)	—	Phased commencement; s.44(2) from 13 May 2027

DRAFT — FOR LEGAL REVIEW

Information Technology Act, 2000	ss.43A, 72A, 70B	Reasonable security practices (until repealed), disclosure in breach of contract, CERT-In
IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011	rr.3–8, 5(9)	Privacy policy, consent for sensitive data, grievance officer (one month), disclosure and transfer, security practices
CERT-In Directions under s.70B(6), 28 April 2022	—	Six-hour incident reporting; 180-day log retention in India
Consumer Protection (E-Commerce) Rules, 2020	r.4(9)	Explicit, affirmative consent (no pre-ticked boxes)
Guidelines for Prevention and Regulation of Dark Patterns, 2023	—	Consent and preference interfaces
Central Goods and Services Tax Act, 2017; Companies Act, 2013	s.36; s.128(5)	Record retention
RBI Master Direction on Payment Aggregators, 2025; RBI data localisation directions	—	Card-data storage restrictions; payment data stored in India

DRAFT — FOR LEGAL REVIEW

Open review points

1. **Commencement (legal requirement).** Confirm dates; decide whether to keep Part 1.3's statement that DPDP-standard rights are offered before May 2027.
2. **Lawful basis mapping (interpretive).** Part 3 — each non-consent purpose must fit section 7 or section 17.
3. **Recipient data (open question).** Part 6.1.
4. **Related-party processors (recommended protection).** Part 5 — CFO/AROS services of SnxwFairies Innovations Pvt. Ltd.; written data processing agreement and instruction-only processing.
5. **Cross-border transfers (business assumption to correct).** Part 9 — correct the published "India-based infrastructure" statement.

6. **Audit-trail retention (legal requirement).** Part 8 — replace "kept indefinitely".
7. **Significant Data Fiduciary (interpretive).** Daily Flowers is not expected to be notified as a Significant Data Fiduciary or to fall within the Third Schedule e-commerce class (two crore or more registered users); re-assess as the user base grows.
8. **Activity measurement (open question).** Part 7 — IP address stored with first-party activity events; decide whether this rests on consent with an opt-out or on security grounds with a short retention period.
9. **Verbal marketing consent (business decision).** Part 13 reflects the recommendation in open decision OD-072 that marketing consent requires a digital or written opt-in; management to confirm.
10. **PII export controls (business decision).** OD-058 — internal policy on who may export customer data, to support the safeguards in Part 10.

DRAFT — FOR LEGAL REVIEW