



Data Security & Privacy Policy

Definitions

- **Anonymization-** The process of either encrypting or removing personal data from a database, so that the individuals whom the data describe remain anonymous. This is done for the purpose of protecting individuals' private activities while maintaining the integrity of the data gathered and shared.
- **Behavioral Advertising-** The act of tracking users' online activities and then delivering ads or recommendations based upon the tracked activities.
- **Biometric Data-** Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data.
- **Consent-** Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **Cookies-** A small text file stored on a user machine that may later be retrieved by a web server from the machine. Cookies allow web servers to keep track of the end user's browser activities, and connect individual web requests into a session.
- **Data Enrichment-** A process used to enhance, refine or otherwise improve existing data.
- **Data Retention-** The policies and processes used within Dabur for determining the time period for archiving and storing of personal data.
- **Data Processing-** Any operation or set of operations which is performed on personal data, such as collecting, recording, organizing, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, dissemination or otherwise making the data available, aligning or combining data, or blocking, erasing or destroying data. Not limited to automatic means.
- **Direct Marketing-** A form of advertising in which companies provide physical marketing materials to consumers to communicate information about a product or service.
- **Encryption-** The method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key
- **Genetic Data-** Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.



- **Health Data-** Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
- **IP Address-** A unique address that identifies a device on the Internet or a local network and which allows a system to be recognized by other systems connected via the Internet protocol.
- **Online Behavioral Advertising-** Websites or online advertising services that engage in the tracking or analysis of, e.g., search terms, browser or user profiles, preferences, demographics, online activity, offline activity, location data, and offer advertising based on that tracking.
- **Personal Data-** Any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly, in particular, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
- **Personal Data Breach-** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **Privacy and Data Protection-** The collection of laws and regulation that applies to the collection, usage, storage, protection and other processing of personal data. This includes data protection, privacy, banking secrecy, electronic communications and confidentiality laws and regulations, and any other applicable laws or regulations to the extent they relate to privacy of personal data.
- **Processor-** A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- **Recipient-** A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third-party or not. However, public authorities which may receive personal data in the framework of an inquiry in accordance with India Law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.



- **Representative-** Natural or legal person established in the India law.
- **Special Categories of Personal Data-** Special categories of personal data, include: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data (for uniquely identifying an individual) and of data concerning health, sex life or sexual orientation.
- **Third-Party-** A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

Privacy Notice - Dabur

Welcome to Dabur India Ltd website. The information that we collect and store during normal use of the site is used to monitor use of the site and to help its further development. Our goal is to protect your privacy and the information that you submit to us through the Internet.

A number of pages in this website give you the option to submit personal information to the Company. All such communications are not confidential. Any application, request or enquiry you make, may be passed or made available to Group affiliates.

By accessing this web site, you indicate your acceptance of this Privacy Policy.

Dabur is committed to update our users promptly in the event of any changes to our privacy policy or any occurrence of a data breach. Notifications will be provided through appropriate channels to ensure transparency and timely communication.

Dabur privacy policy applies comprehensively to all aspects of our company's operations, encompassing all entities, subsidiaries, and affiliates under our control. This ensures uniformity and consistency in the protection of user data across our entire organizational framework.

This privacy Notice applies to the vendors as well, if they are collecting their personal data on behalf of Dabur.

Data Collection

Any personal data provided to or collected by Dabur is controlled by Dabur India Limited.

This Privacy Notice applies to personal data collected by Dabur in connection with the services and products we offer. References to "Dabur" in this Notice means Dabur India Limited and any company directly or indirectly owned and/or controlled by Dabur India Limited that you are interacting with or have a business relationship with.



This Privacy Notice also applies to Dabur's marketing content, including offers and advertisements for Dabur products and services, which we send to you on third-party websites, platforms and applications based on your site usage information.

- We may collect personal data basis Information you give us and Information we collect when you contact us, visit our sites etc.
- Personal data means any information that can be used to identify directly or indirectly a specific individual.

This definition includes personal data collected by direct marketing campaigns, sweepstakes and competitions and online through our websites, applications and branded pages

Certain categories of personal data, such as health data, financial data, biometrics, race, ethnicity, religion, health, sexuality or biometric data are classified as "special categories of data" or "Sensitive Personal Information" and benefit from additional protection.

We limit the circumstances where we collect and process these special categories of data.

Dabur sometimes collects data related to your health, etc., to send you tailored ads and relevant promotions. Dabur only collects and uses this personal data where you have provided us with your consent to do so. In some instances, you may have requested services or products that do not directly involve the collection of any special categories of data but may imply or suggest your health or other special categories of data.

Dabur pledges to gather user data through lawful and transparent means, ensuring explicit consent from the data subject where necessary. Our data collection practices are designed to adhere to applicable laws and regulations, and we strive to provide clear information regarding the purposes and methods of data collection.

Dabur is committed to empower customers to exercise control over their data through various options, including opt-out, granting opt-in consent, requesting data transfers, corrections, and deletion as per the applicable regulations including but not limited to DPDP Act. These options are readily accessible and reflect our dedication to fostering trust and respect for individual privacy preferences.



Usage of Data collection

We collect, process and disclose your personal data only for specific and limited purposes.

We also create profiles of visitors by analyzing the information provided by them while online surfing, searching and buying our products/ services or otherwise while interacting with our brand communications by building segments.

We collect, process and disclose your personal data for the following purposes:

- To process your payments, if you purchase our products/services, to provide you with your order status, deal with your enquiries and requests, and assess and handle any complaints;
- To process and answer your inquiries or to contact you to answer your questions and/or requests;
- To develop and improve our products, services, communication methods and the functionality of our websites;
- For the purposes of competitions or promotions that you have entered;
- To communicate information to you and to manage your registration and/or subscription to our newsletter or other communications;
- To manage our everyday business needs regarding your participation in our contests, sweepstakes or promotional activities or request;
- To authenticate the identity of individuals contacting us by telephone, electronic means or otherwise;
- For internal training and quality assurance purposes;
- To understand and assess the interests, wants, and changing needs of consumers, to improve our website, our current products and services, and/or developing new products and services; and
- To provide personalized products, communications and targeted advertising as well as product recommendations to you.



Dabur uses your personal data to build profiles. We create profiles by analyzing the information about your online surfing, searching and buying behavior and your interactions with our brand communications by building segments and by placing your personal data in one or more segments. These segments are used by Dabur to personalize the website and our communications to you and to display relevant offers and advertisements from the Dabur brands on the Dabur sites, and via third-party websites. The segments can also be used for third-party campaigns on the Dabur sites. Dabur profiles your data where you have provided consent for us to do so.

You can withdraw your consent to prevent your personal data being used this way at any time using the manage cookies section of our Cookie Notice or unsubscribing to the use of your email address if you have logged into one of our websites or signed up to any marketing newsletters.

Dabur collects data, with your consent, from:

- Our websites about what you view and the way you interact with our content;
- Our digital display advertising that we serve to you on social platforms and other publisher's websites; and
- Forms you fill in online and send to us about what your interests are.
- We also track the products you buy when you click on one of our display adverts and go on to purchase something from a selection of our retail partners.
- If you have asked to receive emails or SMS communications from us, we track whether you open, read or click on the content to see what you are interested in so that we can give you more content that we think you are more likely to enjoy.
- Based on this profile information, we may also give you advertising that we think you will like and want to see as you view content from us or from our network of publishers that we advertise with. Sometimes, with your consent, we may use your current location to serve advertising to you that is to do with promotions or events that are happening nearby that we think you might be interested in.
- We may also use information you have provided to selected third-parties and consented to be shared, like your age, gender, life stage, lifestyle and wider interests to identify people who we think will have similar interests to you and who we believe will be interested in similar advertising.



Our commitment extends to collecting and processing user data only for the specified purposes outlined in our privacy policy. We do not engage in data processing activities beyond the scope of what is necessary to fulfill these purposes, ensuring that user data is used responsibly and ethically.

Data Shared With

As part of the Dabur group your personal data use within the Dabur Group and with selected third-parties in the following circumstances:

Third-party service providers- In order to carry out your requests, respond to your inquiries, fulfil your orders, honor coupons, provide you with samples, enable you to participate in sweepstakes or make various other features, services and materials available to you through our websites we share your personal data with third-party service providers that perform functions on our behalf, such as companies that: host or operate Dabur's websites and Apps process payments, analyze data, provide customer service, postal or delivery services, and sponsors or other third-parties that participate in or administer our promotions. They have access to personal data needed to perform their functions but may not use it for other purposes. Further, third-party service provider/ vendor must process this personal data in accordance with this Privacy Notice and as permitted by applicable data protection laws and regulations.

Other third-parties- Your personal data will also be used by us or shared with our sponsors, advertisers, advertising networks, advertising servers, social media networks, and analytics companies or other third-parties in connection with marketing, promotional, data enrichment (to find out more about our privacy key terms follow the link) and other offers, as well as product information.

Business transfer- Your personal data will be used by us or shared with the Dabur Group, primarily for business and operational purposes. As Dabur Group continues to develop the business, it may sell or purchase assets, subsidiaries or business units. In such transactions, your personal data generally is one of the transferred business assets but remains subject to the promises made in any pre-existing Privacy Notice (unless, of course, you consent otherwise). If another entity acquires us, our businesses or substantially all or part of our assets, or assets related to Dabur's websites, your personal data will be disclosed to such entity as part of the due diligence process and will be transferred to such entity as one of the transferred assets. Also, if any bankruptcy or reorganization proceeding is brought by or against us, all such personal data will be considered an asset of ours and as such it is possible they will be sold or transferred to third-parties.



Legal disclosure- We may transfer and disclose your personal data to third-parties:

- To comply with a legal obligation;
- When we believe in good faith that an applicable law requires it;
- At the request of governmental authorities conducting an investigation;
- To verify or enforce our "Terms of Use" or other applicable policies;
- To detect and protect against fraud, or any technical or security vulnerabilities;
- To respond to an emergency; or otherwise
- To protect the rights, property, safety, or security of third-parties, visitors to Dabur's websites, Dabur or the public.

Dabur requires third parties with whom we share user data to adhere to the same stringent privacy standards upheld by our company. Any sharing of data is done in accordance with our privacy policy and contractual agreements that mandate compliance with our data protection principles.

Protection of Data

Dabur takes the security of your personal data very seriously. We take every effort to protect your personal data from misuse, interference, loss, unauthorized access, modification or disclosure.

Access to your personal data is only permitted among our employees and agents on a need-to-know basis and subject to strict contractual confidentiality obligations when processed by third-parties.

Dabur does not retain personal information beyond the period necessary to fulfil the purpose for which it was collected, unless retention is required under applicable law or for audit and compliance purposes. In all such cases, Dabur ensures the continued confidentiality and protection of such information.

Your data may also be retained so that we can continue to improve your experience with us and to ensure that you receive any loyalty rewards which are due to you.



We retain the identifiable data we collect directly for targeting purposes for as little time as possible, after which we employ measures to permanently delete it.

We will actively review the personal data we hold and delete it securely, or in some cases anonymize it, when there is no longer a legal, business or consumer need for it to be retained.

Dabur is dedicated to upholding the highest standards of data protection. Our policies and procedures are continuously reviewed and updated to align with leading industry standards and regulatory requirements to safeguard the privacy and security of user data.

A steering committee, consisting of CFO, CHRO, CIO, Company Secretary and Risk Management Committee, has been established to supervise operations related to cyber security and data privacy.

Rights on Data

Your rights in relation to your personal data how it is processed. You can exercise these rights at any point. We have provided an overview of these rights below together with what this entails for you. You can exercise your rights by sending an email or submitting a request through the "Contact Us" form on our websites.

Where we process your personal data, you have a number of rights over how the data is processed and can exercise these rights at any point.

These rights will include:

- Request access to data held by the company.
- Request their data to be transferred to other service providers.
- Request their data to be corrected.
- Request their data to be deleted.

Risk Assessment and Audit

- In line with Dabur internal control framework, we perform periodic risk assessment to determine the company's exposure to data privacy breaches.
- Based on the risk profile identified necessary steps for its mitigation shall be taken. The risk assessment process shall be undertaken once every three years or earlier in case of a major change in factors impacting the risk e.g. nature of operation, new regulation, etc. Independent audit of data privacy controls would be conducted at least once in three years.



Responsible AI Principles

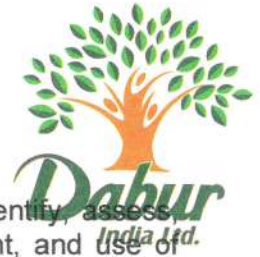
At Dabur, we are committed to the responsible development, deployment, and use of Artificial Intelligence (AI). Our AI practices are guided by the following principles:

- Respecting data privacy in the use and/or development of AI by protecting personal data throughout the AI lifecycle and complying with applicable data protection and privacy laws.
- Avoiding potential bias in the use and/or development of AI by promoting fairness, using representative data, and regularly assessing AI systems to reduce unintended bias.
- Keeping humans “in the loop” for critical decisions and allowing human intervention by ensuring appropriate human oversight and the ability to review or override AI-generated outcomes where necessary.
- Protecting the cybersecurity of systems in the use and/or development of AI through appropriate security controls, secure development practices, continuous monitoring, and incident response measures.
- Ensuring transparency of AI systems and explainability of AI generated results/decisions by clearly communicating the use of AI, its capabilities, limitations, and providing appropriate explanations for significant AI-generated outcomes.
- Establishing clear accountability for outcomes produced by AI models/tools by assigning governance responsibilities and maintaining oversight of AI systems throughout their lifecycle.
- Defining clear boundaries for what the AI can and cannot do by implementing safeguards that ensure AI systems operate only within their intended purpose and approved scope.
- Requiring own and third-party AI data centers/models to have a low ecological footprint, where feasible, by encouraging energy-efficient infrastructure and environmentally sustainable AI practices.
- Not using/deploying AI systems that engage in manipulative behavior, exploitation of vulnerabilities, social scoring, or unauthorized biometric surveillance, and ensuring compliance with applicable legal, ethical, and regulatory requirements.

Emerging Technologies Principles

At Dabur, we recognize the opportunities that emerging technologies offer while acknowledging the risks and ethical considerations associated with their adoption. We are committed to the responsible use of emerging technologies through the following principles:

- Acknowledging the risks and ethical considerations associated with the adoption and use of emerging technologies, including their potential impact on individuals, society, security, privacy, and the environment.
- Avoiding highly controversial or unethical practices by ensuring emerging technologies are used responsibly, ethically, and in compliance with applicable laws, regulations, and organizational values.



- Implementing appropriate controls and risk management measures to identify, assess, monitor, and mitigate risks associated with the development, deployment, and use of emerging technologies.
- Promoting transparency by reporting on the use of emerging technologies, where appropriate, to provide stakeholders with information on governance, responsible adoption, and risk management practices.

Roles and Responsibilities

Dabur defines individual information security responsibilities across its workforce, including employees, contractors, and third parties, and reinforces compliance through onboarding, training, and contractual obligations.

- **Internal workforce responsibilities:**
Information security responsibilities at Dabur are distributed across multiple levels, including senior leadership, information security and privacy teams, operational units, and all employees. Leadership provides strategic oversight and governance, while dedicated security and privacy teams manage risk assessment, implementation of controls, monitoring, compliance, and incident response. Every employee is responsible for adhering to established data protection policies, following access and usage guidelines, and promptly reporting any suspected security or privacy incidents.
- **Third-party data security and privacy requirements:**
External partners, service providers, and vendors are required to comply with Dabur's data security and privacy standards. Business partners must nominate designated security or data protection representatives to coordinate with Dabur's teams. Third parties are expected to implement appropriate technical and organizational safeguards, including confidentiality agreements, personnel screening, secure systems and infrastructure, timely patching, controlled change management, and defined incident reporting and escalation mechanisms. They are also required to support investigations and remediation activities when necessary.

This structured and collaborative approach ensures that both internal teams and external stakeholders collectively uphold Dabur's commitment to data security and privacy.

Disciplinary Actions

- Dabur is committed to continuously improving our data privacy practices.
- Employees found to have breached the data privacy policy, whether deliberately or through negligence, will face disciplinary actions.
- Lessons learned from breaches and disciplinary actions will be used to enhance our policies, training programs, and security measures to prevent future incidents.



Grievances & Complaints Redressal

All Privacy-specific complaints would be recorded and addressed without undue delay and as per any norms specified in applicable laws and regulations. The designated person or team at The Company would redress the grievances expeditiously following due process.

Governance

The Board of Directors has ultimate oversight of this Policy. The board periodically reviews performance, monitors progress against agreed-upon targets, and ensures effective implementation across all operations.

Contact @ Dabur

In case of any grievance, you may contact at: daburcares@dabur.com or corpcomm@dabur.com

Mohit Malhotra
Whole Time director &
Global Chief Executive Officer

Date of revision: 03.08.2026