

# Privacy Notice to India Workforce

Version 1 - Last updated: 30 April, 2025

## Who we are and what is this notice about.

We are **Sanofi Consumer Healthcare India Limited** (“we”, “us”), a company with registered office at Unit 1104, 11th Floor, Godrej Two, Pirojsha Nagar, Eastern Express Highway, Vikhroli East, Mumbai 400079.

We are part of Opella, a multinational group that includes Opella Healthcare with its affiliates and subsidiaries (collectively “Opella”).

**This Privacy Notice provides you with information about what Data we collect as part of your employment relationship with us, why we collect it, how we use it, and what rights you have in relation to it.**

For the purposes of this Privacy Notice, by “Workforce”, we imply employees, consultants and contractual staff providing services to us. Unless explicitly stated otherwise, we are responsible for the use of your Personal Data (“Data”), as described in this Privacy Notice and according to applicable data protection laws.

## What Data we collect about you.

As part of your working relationship with us, we may collect and process the following Data: **Personal identification data**, such as name and surname, address, citizenship, date of birth, gender, national ID, social security number or other national identification number (the use of these identifiers is restricted to very specific purposes as required by national tax, insurance and labor laws);

- **Physical characteristics**, such as height, clothing size, etc. on need basis only.;
- **Images**, such as badge or profile pictures, CCTV and other video-recordings;
- **Family information**, such as marital status, family structure, names of family members and kinship ;
- **Contact details**, such as email addresses, phone numbers, and emergency contact information;
- **Communication information**, such as email subject line and contents, IM contents, communication logs and meta-data (e.g., date, time, duration, location, addressees, sender, etc.);
- **Financial information**, such as financial account data (corporate credit card number, bank account), financial transaction data (payments, taxes, and other transactions);

- **Educational and professional qualifications**, such as academic degrees or diplomas, professional certifications or licenses, training or workshop completions, membership in professional bodies, published works or research, relevant coursework or specialized training, examinations or tests passed, languages spoken;
- **Employment history and records**, such as previous employers, dates of employment, positions held, promotions or demotions, transfer records, recognition or awards received, disciplinary actions or records, resignation or termination details;
- **Organizational affiliation data**, such as company or organization, job title, role, function, department, BU or division, manager or supervisor's name, direct reports, or subordinates, reporting hierarchy level, office or location assignment, project or task group associations, functional responsibilities or domain areas;
- **Compensation & benefits data**, such as salary or wage amount, bonus structures, stock options or shares awarded, health or medical benefits, retirement or pension plans, travel, car or housing allowances, performance-based incentives, other non-monetary perks or benefits, tax deduction details;
- **HR administrative records**, such as onboarding or induction documents, attendance logs or timesheets, leave requests and approvals, training schedules;
- **Evaluation and assessment data**, such as feedback/notes/observations from managers, peers or other stakeholders, results from aptitude or skills tests, assessment and self-assessment outcomes (behavioral, psychological, personality, promotion or progression), performance appraisal scores;
- **Misconduct & investigation records**, such as details of the alleged misconduct, statements from involved parties or witnesses, documentation or evidence submitted, notes from investigation interviews or meetings, findings or conclusions of the investigation, recommended or executed actions following the investigation, appeals or responses from the individual concerned;
- **Travel, transport and mobility information**, such as itineraries, destinations, transport tickets, commute information, reservations, travel-related expenses;
- **Location information**, such as GPS coordinates, desk or room number, country;
- **Device and equipment information**, such as the IP address, device type, unique device identification number, browser type, operating system, broad geographic location (e.g., country or area), and other technical information;
- **Interaction and activity logs**, such as computer login times, application login/logout time, file downloads, internet navigation history and other operational behaviors.

In addition, we may process the following categories of data only when it is strictly necessary to comply with our legal or regulatory obligations, or to mitigate high-risks, and subject to completion of thorough risk assessments and adoption of state-of-the art security measures:

- **Political, religious, labor or philosophical beliefs, opinion and affiliations**, such as trade union membership, political or religious affiliations;
- **Ethnicity information**, such as race, national or ethnic origin;
- **Medical, health and impairment information**, such as sick leave information, workplace injury and incident reports, disability accommodation information, mandatory health screenings or vaccinations, support program participation. Learn more about this by reading the note on “Data processed by independent medical or occupational health professionals” in the section below;
- **Judicial information**, such as background check information;
- **Biometric information**, such as fingerprint, facial pattern, etc.

## Why and on what grounds we use your Data.

**Sanofi Consumer Healthcare India Limited**, as your employer, is responsible for the processing of the above Personal Data under the following justifications (legal basis) and for the following purposes.

### **Performance of contract.**

We generally process your Personal Data on the basis of the relevant applicable contractual relationship as an employee, consultant and/or contractual staff providing services to us. This means that the processing of Personal Data - for the purposes described below - is necessary to the execution of employment contract or the relevant governing contract that defines your relationship with us and is therefore mandatory. Please keep in mind that, should you refuse that Opella processing such Data, we may be unable to properly carry on this contractual relationship. In particular, we process your Data to:

- to **manage onboarding**, for example to facilitate the negotiation, drafting, and finalization of employment contracts. This involves confirming the candidate's employment terms, benefits, start dates, and any other pertinent details necessary to formalize the employment relationship;
- to **handle financial and contractual matters**, for example to fulfill the employment contract and ensure compliance with local and international tax regulations. This involves data analysis, financial modeling, and regular communications with internal teams, external advisors, and tax authorities to ascertain the organization's tax obligations and optimize tax strategies;
- to **manage planning and administration of payroll, expenses, compensations and benefits**, for example to administer and oversee all aspects of employee benefits and wellbeing programs within the organization. This encompasses both contractual benefits, such as health insurance, retirement contributions, as well as discretionary benefits and wellbeing initiatives aimed at promoting overall staff satisfaction and wellness. Activities include managing benefit enrollment, tracking eligibility criteria,

coordinating with insurance providers, facilitating access to wellness programs and recreational activities, providing mental health support, and administering additional perks and benefits to enhance the employee experience;

- to **manage travels and expenses**, for example to issue, oversee, and administer corporate credit cards designated for various business-related expenses, or to review, authorize, and coordinate business travel requests, managing bookings and reservations, as well as to handle travel-related expense claims;
- to **enhance the skills, knowledge, and capabilities of the workforce**, for example to organize and administer discretionary training programs within the organization. This encompasses identifying skill gaps or development opportunities, selecting appropriate training initiatives, scheduling sessions, and tracking participation and performance outcomes. Additionally, this activity includes evaluating the effectiveness of training efforts and adjusting programs as needed to support employee development and organizational goals;
- to **manage careers, development, performance evaluation and appraisal, and mobility**, for example to develop and execute competency management, career plans, and talent development strategies within the organization. This includes identifying, nurturing, and retaining talent through activities such as skill development, training, talent acquisition, performance evaluations, succession planning, talent pool development, and engagement and retention strategies;
- to **manage workforce and organization**, for example to organize and oversee the structure of the organization and its people. This encompasses activities such as defining job roles, charting organizational hierarchies, coordinating team alignments, evaluating performance, planning career paths, and ensuring that the workforce is aligned with the Company's strategic goals;
- to **manage offboarding**, for example to ensure a smooth and compliant transition out of the organization. This encompasses activities such as finalizing payroll, ensuring the return of company property, revoking access to company systems and premises, conducting exit interviews, and documenting reasons for termination or resignation. Additionally, this data aids in understanding turnover rates, capturing feedback for organizational improvement, and maintaining records for any future rehiring or reference checks. The process ensures that both the organization's and the individual's interests are protected during the separation phase.

### **Compliance with legal obligations.**

Certain processing activities are required to comply with **our legal, regulatory, ethical and compliance obligations**, for example with regards to tax reporting, social security contributions, pharmacovigilance, transparency, regulatory fining and submissions to Health Authorities, managing conflicts of interest and alerts reporting, ensuring the health and safety of our staff (“duty of care”), fighting against fraud, conducting internal investigations, audits, managing

conflict of interest reporting. This also includes ensuring compliance with mandatory training requirements within the organization by delivering training and awareness campaigns on security best practices or compliance (identifying training needs, scheduling sessions, tracking completion status, and maintaining records of training participation and outcomes).

### **Legitimate interest.**

In some cases, the processing of your Personal Data is not strictly necessary for the performance of the applicable contract. In such cases, we process your Personal Data to pursue our legitimate interest to:

- to **manage access to and occupation of offices, plants, facilities and other professional premises and to provide on-site services**, for example through surveillance, access controls, and logging mechanisms to ensure the physical and digital integrity of the infrastructure, prevent unauthorized access to the site or to specific areas of the site, and maintain the safety and security of these areas (this encompasses issuing and monitoring access cards or badges); to assign workspaces, desks, or office rooms, manage shared workspace reservations, and monitor workspace utilization for space optimization, to manage and administer on-site services such as cafeterias, gyms, parking spaces or day-care centers, and to track service usage and gather feedback;
- to **manage internal communication and events**, for example to plan, coordinate, and execute events and communication initiatives targeting internal stakeholders. This encompasses activities such as organizing workshops, townhall meetings, retreats, or company-wide celebrations, as well as distributing effective, clear, and timely communication within the organization. Information such as dietary preferences, attendance confirmations, logistical requirements, and feedback on events may be collected to ensure smooth operation and continuous improvement of these gatherings. Various communication platforms, including internal newsletters, intranet posts, email bulletins, digital message boards, and proprietary communication tools, are employed to foster a well-informed workforce, promote transparency, drive alignment with company goals, and cultivate a cohesive organizational culture;
- to **manage labor and industrial relations**, for example to facilitate various aspects of the relationship between the organization and its unions or representative bodies. This includes, conducting collective bargaining negotiations, and ensuring compliance with relevant agreements and regulations. The process aims to foster transparent and productive communication, uphold employee representation rights, and maintain constructive relationships with labor organizations;
- to **establish, exercise or defend our legal rights**, for example to handle and oversee disputes, claims, and litigations;
- to **develop and operate our digital platforms and tools**, for example to oversee the company's digital infrastructure, backup, and disaster recovery processes, or to track, monitor, and manage the company's inventory of digital devices and assets;
- to **protect our staff, visitors, assets and information**, for example to ensure employees' safety and security during business travels, to establish a list of emergency contacts, to

ensure compliance with health, safety, and environmental (HSE) regulations and standards, as well as to manage incidents, to monitor our premises through CCTV and surveillance systems, to handle and respond to security incidents;

- to **engage and ensure satisfaction and wellbeing of our staff**, for example to assess, monitor, and improve employee engagement within the organization. This involves conducting surveys, collecting feedback, analyzing responses, and implementing initiatives or programs based on the insights obtained, including Diversity, Equity and Inclusion (DEI) initiatives. The goal is to foster a positive work environment, improve retention, enhance productivity, and promote a culture of continuous feedback and improvement. Data may also be used to segment and tailor engagement efforts for specific departments, roles, or demographic groups within the workforce;
- to **maintain a favorable operating environment for the company**, for example to handle public affairs by performing activities such as engaging with policymakers, communicating with media outlets, advocating for industry interests, monitoring regulatory landscapes, and coordinating with community and public interest groups;
- to **protect ourselves from financial, reputational and regulatory risk and liability**, for example to design, implement, monitor, and refine Ethics and Business Integrity programs within the organization, to monitor and enforce compliance with internal policies and procedures, to prepare, plan and execute audit activities, to distribute reports and to manage possible findings and follow-ups, to evaluate and rate the inherent and residual risks associated with specific processes, projects, or departments, to document mitigating actions and their status, and to distribute reports to relevant stakeholders.

### **Consent.**

In limited circumstances, we may seek your explicit consent as a legal basis for specific activities. These include, for example, participation in voluntary employee engagement surveys, inclusion in corporate marketing materials (e.g., photographs or videos), or processing of Data in relation to optional wellness programs. If we require your consent for any processing activity, we will provide clear and detailed information to ensure that your choice is fully informed. You have the right to withdraw your consent at any time without any negative consequences to your employment.

### **Activities under responsibility of other Opella companies.**

In some circumstances, **Opella Healthcare Group SAS**, a company with registered office at 157 avenue Charles de Gaulle, 92200 Neuilly-sur-Seine, France, is also responsible for processing your Personal Data:

- to **develop and operate our digital platforms and tools**;

- to **protect our staff, visitors, assets and information;**
- to **engage and ensure satisfaction and wellbeing of our staff;**
- to **maintain a favorable operating environment for the company;**
- to **protect ourselves from financial, reputational and regulatory risk and liability.**

This happens, in particular, with regards to some processing of your Data that is performed for the benefit of Opella as a whole, or for goals that can only be achieved by pooling Data from staff members across different affiliates.

When this happens, the processing is performed to pursue the legitimate interests of Opella Healthcare Group SAS and its affiliates (as the case may be) to: ensure efficient group-level operations and maintain a favorable operating environment; safeguard security and integrity of individuals, assets, and information across Opella, allow to fulfill legal, regulatory, ethical and compliance obligations and protect the group's interests and ensure compliance with legal and regulatory requirements.

#### **Data processed by independent medical or occupational health professionals.**

As mentioned in previous paragraphs, we process Data about you that qualifies as “Medical, health and impairment information”. However, in most cases, the processing of health-related Data is carried out by independent medical or occupational health professionals who operate and are autonomously responsible for using and protecting such Data. These professionals are subject to strict confidentiality obligations and legal or ethical duties that govern the handling of sensitive health information. As a result, while we may facilitate medical assessments, workplace accommodations, or health-related support programs, we generally do not have direct access to detailed medical records or diagnoses, unless required by law or when you voluntarily share such information with us.

## **How we collect your Data.**

Depending on the nature and scope of your relationship with us, we may collect your Personal Data from different sources and in a variety of circumstances and ways:

- directly and knowingly from you;
- from other affiliates of Opella;
- through automated tool or tracking technologies;
- from Partners or Service Providers;
- from publicly available sources;
- from Government and Regulatory Authorities.

In addition, new Data about you may be inferred, derived, generated as part of the processing (for example in relation to performance evaluations, training completion records, usage data

from company-provided devices and digital tools, attendance records, feedback from colleagues, or data from employee engagement surveys, etc.).

If we obtain your Personal Data from more than one source, we may combine or link such Data and use it for purposes compatible with those for which it was originally collected.

### **Unsolicited Personal Data.**

In some circumstances, you may voluntarily provide us with unsolicited Personal Data. We ask for your collaboration to avoid sharing Personal Data that is unnecessary. Should this happen, you are directed to recall such Personal Data immediately without delay. Additionally, we will take reasonable steps to delete the unnecessary data and such Personal Data shall not be used.

### **Personal Data you provide about others.**

In some circumstances, you may provide us with Personal Data about others, including that of members of your family (see next section). Whenever you provide us with Personal Data about others, please take reasonable steps to ensure they are aware and do not object to you sharing their data with us. If unsure, please refrain from communicating such Personal Data to us.

## **Family Members' Data.**

As part of our commitment to ensuring the well-being and security of our employees, as well as to fulfill our regulatory or legal obligations, in limited circumstances we may process Personal Data about your family members. This processing is conducted for various legitimate purposes, including but not limited to:

- **Emergency Contact:** Collecting and maintaining contact details of your relatives to reach them in case of emergencies.
- **Benefits Administration:** Managing health insurance, pension plans, and other benefits that may extend to your family members.
- **Leave Management:** Processing data related to family members for purposes such as parental leave, family medical leave, or bereavement leave as applicable.
- **Dependents management:** Gathering information about dependents for tax purposes or to provide dependent care benefits.
- **Travel Arrangements:** Coordinating travel plans for family members when they are involved in company-sponsored events or relocations.
- **Tax and Legal Obligations:** Collecting and processing data to comply with tax reporting requirements and other legal obligations, such as verifying dependent eligibility for benefits.

## **Who can access your Data.**

We operate in a complex ecosystem of Opella affiliates, third-party service providers with their sub-contractors, commercial partners, scientific partners, customers, regulatory bodies, public authorities, and law enforcement agencies.

Provided that we are legally authorized to do so, your Personal Data may be shared or otherwise made available to various recipients inside and outside Opella in various circumstances.

Such recipients may include:

- **employees and staff of Opella affiliates and subsidiaries**, to allow for the processing of your Data for the purposes described in the previous sections;
- **our partners, such as service providers, contractors, or vendors**, acting upon our instructions to support the processing of your Data for the purposes described in the previous sections;
- **supervisory & regulation bodies (payers, governmental agencies, ethics committees), public authorities, courts, and law enforcement bodies**. This may happen, for example, in circumstances that include, but are not limited to fulfilling our reporting obligation; responding to requests from them; when it is necessary to establish, exercise, or defend legal claims; when you request us to do so if this does not constitute a violation of our or others' rights; when it is necessary to prevent physical harm or material financial losses to us or others.
- **professional Advisors and Auditors**;
- **potential Buyers or Investors** during Mergers, Acquisitions and Divestitures.

Whenever required by the applicable law, we enter into contractual agreements with these recipients to ensure they provide adequate data protection measures, they commit not to use the Data for purposes other than those described in this Privacy Notice and cooperate with us to ensure that your rights can be effectively exercised.

## Where is your Data processed.

We are part of a multinational group with employees, affiliates, partners and service providers located around the world. Consequently, your Data may be processed in and accessed from countries where different data protection laws apply.

When Personal Data is transferred to or accessed from other jurisdictions, we adopt one of the mechanisms provided by the law to ensure an equivalent level of protection of your Data in the destination country. This includes, for example, the adoption of the Standard Contractual Clauses.

## How long we keep your Data.

Your Data will be kept for a period not exceeding the time necessary to achieve the purposes for which it was collected. The criteria for determining the retention period of the Personal Data consider the period of permitted processing (for all the relevant purposes), applicable regulations affecting the minimum or maximum retention period (if any), limitation of rights, and legal bases for processing.

## How we protect your Data.

While we strive to protect your Personal Data, no Data transmission, use or storage can be guaranteed as 100% secure. To protect your Data, we adopt technical and organizational measures aimed at reasonably mitigating the risk that such Data is leaked, lost, or used for unauthorized purposes.

If a security incident occurs and affects your Personal Data, we will take reasonable actions to mitigate possible impacts on you. When the incident is likely to result in serious harm this may include a notification to you or to competent authorities.

## Your rights.

You have the following rights regarding your Personal Data:

- Right to be informed about the collection and use of your Personal Data
- Right to access and to and receive a copy of your Personal Data
- Right to rectification of your Personal Data, if it is inaccurate, incomplete or out of date
- Right to erasure in situations provided for by applicable data protection laws
- Right to Object to the processing of your Personal Data, if it has been collected and processed on the basis of our legitimate interests
- Right to Opt out withdraw your consent to the processing of your Personal Data at any time, without prejudice to the lawfulness of the processing, if your Personal Data has been collected and processed based on your consent
- Right to raise grievance with Grievance Officer if you believe their rights have been violated
- Right to nominate another person to exercise their rights on their behalf in the event of death or incapacity
- Right to be notified in case of data breach affecting your personal data

If you want to exercise any of your rights, please submit a request using the online form you can access from this webpage: <https://www.opella.com/en/privacy-center>, or use the other contact indicated in this or other privacy notices.

You are also entitled to lodge a complaint with your local Data Protection Authority.

## Contact us.

If you have a question or any concerns regarding our use of your Data, visit <https://www.opella.com/en/contact>.

## **Changes to this Privacy Notice.**

We may update this Privacy Notice periodically to reflect changes in the law or our practices. We will make available to you any new version of this document.