




Global Data Privacy Policy

“Building trust through responsible use of personal information.”

Version: 1.1

Published on: 15 September 2023

	Issued by:	Global Legal and Compliance	Version	1.1
	Global Data Privacy Policy		Effective Date	15-September-2023

Policy Prepared By:	Reviewed By:	Reviewed By:	Reviewed By:	Approved By:
Abhishek Pandey	Vivek Mittal	Phanimitra B.	Archana Bhaskar	Parag Agarwal
Deputy Data Privacy Officer	Global General Counsel & Data Privacy Officer	Chief Information Officer	Chief Human Resource Officer	Chief Financial Officer
07-Sep-2023 5:12 PM IST	11-Sep-2023 10:24 AM IST	08-Sep-2023 2:47 PM IST	08-Sep-2023 2:48 PM IST	13-Sep-2023 12:14 PM IST
DocuSigned by: Abhishek Pandey 0E15FB3506A7434...	DocuSigned by: vivek mittal 609DA0981B6A47B...	DocuSigned by: Phanimitra B ACB3A4548A3B42A...	DocuSigned by: Archana Bhaskar EA8DC7E530D04F1...	DocuSigned by: Parag Agarwal 50FD9646906E440...

Version Supersedes	Reasons for Change
Version 1.0	<ul style="list-style-type: none"> Simplifying the policy using a principle-based approach. Separating additional elements such as consents, roles and responsibilities, definitions etc

Contents

- 1. Introduction**
 - 1.1. Purpose
 - 1.2. Scope and Applicability
 - 1.3. Roles and Responsibilities
- 2. Privacy Principles**
 - 2.1. Transparency
 - 2.2. Purpose Limitation
 - 2.3. Data Minimization
 - 2.4. Security, Integrity, and Accuracy
 - 2.5. Minimal Retention
 - 2.6. Accountability
- 3. Training and Awareness**
- 4. Breach of this Policy**
- 5. Adaptions**
- 6. Exceptions**
- 7. Review and Modification**
- 8. References**



Issued by:

Global Legal and Compliance

Version

1.1

Global Data Privacy Policy

Effective Date

15-September-2023

1 Introduction

1.1 Purpose

Dr. Reddy's recognizes that all individuals have privacy rights and that we are committed to responsibly using Personal Information ("PI") or Sensitive Personal Information ("SPI") and in accordance with the relevant privacy laws, as reflected in our Code of Business Conduct and Ethics **[1]**.

'Data Privacy Definitions' document **[2]** lists examples of PI, SPI as well as definitions of other relevant terms.

The purpose of this policy is to help the company protect individuals' privacy rights, help you recognize when you are Processing PI or SPI, and guide you on 'what' to consider under each of the six data privacy principles listed below and 'why'. Separate global procedures and standards (adapted locally, where required), will further explain 'how' the requirements laid down under each of the principles will need to be implemented. These documents will be made available via the company's intranet (iHub).

This policy establishes the company's data privacy principles globally. However, privacy laws vary from country to country. Where local laws, regulations or industry codes are more stringent than this policy, follow local requirements, and in case of doubt, reach out to your Data Privacy Partner.


1.2 Scope and Applicability

The scope of this policy is global. Therefore, the policy applies to all:

- Employees of Dr. Reddy's,
- Subsidiaries of Dr. Reddy's, and
- Third parties with access to Dr. Reddy's systems or Processing PI or SPI on behalf of Dr. Reddy's (including third parties who are contractually obligated to follow our standards).

1.3 Roles and Responsibilities

Role	Responsibilities
Employees	Must comply with this policy when handling PI or SPI on behalf of Dr. Reddy's.
Third Parties with direct access to Dr. Reddy's systems	Must comply with this policy when handling PI or SPI on behalf of Dr. Reddy's.
Third parties	Must comply with Dr. Reddy's Data Privacy contractual terms (based on our standards) when Processing PI or SPI on our behalf.
Global Legal & Compliance	Owns and maintains this policy

	Issued by:	Global Legal and Compliance	Version	1.1
	Global Data Privacy Policy		Effective Date	15-September-2023

2 Privacy Principles

2.1 Transparency

Describe in clear and simple language how Dr. Reddy's manages PI and/or SPI and communicate this to data subject(s), at an appropriate time through easily accessible channel(s). Explain how data subject(s) can exercise their privacy rights under local law and honor such requests. By doing so, Dr. Reddy's builds trust with all stakeholders.

Requirements:

- Explain what PI or SPI will be collected, why it is being collected, how it will be used and who it will be shared with.
- Establish the lawful basis, such as consent, legitimate interests, legal obligations, for collection and processing of PI or SPI.
- Communicate this to the data subject(s) at the time PI or SPI is collected in a format that is easily accessible.
- Being transparent may involve providing a link to an online privacy notice, such as a notice or a banner contained on Dr. Reddy's global website or on a local company website.
- Where required or appropriate provide data subject(s) with choices on how Dr. Reddy's uses the PI.
- Provide data subject(s) with an option to exercise their privacy rights under applicable laws.
- Honor data subject(s)' preferences and privacy requests, such as to access, delete, or opt-out / withdraw consents, subject to local laws.

2.2 Purpose Limitation

Collect PI or SPI only for specific and legitimate business purpose(s) and ensure it is used responsibly i.e., in ways consistent with the purpose(s) for which it was collected and as communicated. This includes ensuring that the company only transfers (or allows access to) such information across country borders, where it is allowed and in compliance with requirements under applicable law(s).

Requirements:


- Identify the specific purpose(s) for collecting PI or SPI.
- Ensure PI or SPI is collected only for such purposes.
- Such information should be used, disclosed, or made available to the necessary parties only in ways consistent with purpose(s) communicated via privacy notices, consents etc.
- If local law allows transfer of PI or SPI across country borders, internally within the company and externally to third parties under specific conditions, ensure such requirements are met before transfer takes place.
- Be aware that PI transferred across country borders but within Dr. Reddy's affiliates may require an Inter-Company Agreement (ICA) to be executed, if already not in place.

2.3 Data Minimization

Collect only that PI or SPI which is directly relevant and necessary to fulfil a specified business purpose.

Requirements:

- Collect PI or SPI only through fair and lawful means.
- Consider if the business purpose can be achieved with less PI or SPI, and only collect the minimum data needed. Remember that collecting more information may lead to higher costs and higher risk for the company.
- Ensure that all reports and information distributed or disclosed internally within the company and externally with third parties or contractors, contain only that PI or SPI which is relevant and necessary to be made available to the recipients.

	Issued by:	Global Legal and Compliance	Version	1.1
	Global Data Privacy Policy		Effective Date	15-September-2023

2.4 Security, Integrity, and Accuracy

Ensure appropriate Information Security policies and guidelines of the company are followed to prevent unintended or unauthorized access, modification, use or disclosure of PI or SPI. Be alert and immediately report any known or suspected incidents involving unauthorized use or disclosure of PI or SPI.

Requirements:

- Follow appropriate Information Security policies and guidelines, such as 'ISMS Acceptable Usage Policy' [3] while handling company's assets and data.
- Ensure confidentiality of all PI or SPI by sharing or allowing access to such information only on a 'need to know' basis.
- When handling sensitive or special categories of PI such as health information, recognize that additional controls may be needed to protect such information.
- Keep PI or SPI in your custody accurate and up to date (within reasonable time post intimation by data subject(s) to a reasonable extent.
- Immediately report any known or suspected Information Security incident or other unauthorized access, sharing, receipt, or use of PI or SPI, as per the 'Information Security Incident Management Policy' [4]

2.5 Minimal Retention

PI or SPI should not be retained longer than it is necessary to fulfil the specific business purpose(s) for which it was collected, unless needed to comply with legal obligations.

Requirements:

- Follow / create record retention schedules to document specific timeframes for retaining records or data which includes PI or SPI
- Delete PI or SPI when no longer needed (unless otherwise required for legal reasons).
- In some situations, anonymization can be used as an alternative to deletion.
- Information systems and applications should allow identification, selection, and deletion of specific elements of data which constitutes PI. This is required to implement data subject requests in relation to their privacy rights such as 'Right to request erasure of their PI.'

2.6 Accountability

Take responsibility for what you do with PI i.e., how you collect, store, use, share, protect and erase PI or SPI. Ensure appropriate measures and records are in place to demonstrate your compliance with all other principles listed above.

Requirements:

- Be informed of Dr. Reddy's Data Privacy standards which include this policy and any other guidelines, procedures and requirements communicated globally or at a regional/country level.
- Follow relevant data privacy requirements as they apply within region/country. Lack of awareness of such requirements cannot be an excuse for non-compliance.
- As the first line-of-defense, identify, report, and manage data privacy risks or gaps in your work area. Consult your Data Privacy Partner when in doubt.



Issued by:

Global Legal and Compliance

Version

1.1

Global Data Privacy Policy

Effective Date

15-September-2023

3 Training and Awareness

All employees, Third Parties, and contractors of Dr. Reddy's (including affiliates) must familiarize themselves with the requirements laid down within this policy and all other Data Privacy related procedure or guidance document developed and communicated by the Data Privacy Officer or by your Data Privacy Partners, from time to time.

4 Breach of this Policy

Breaches of this policy can result in remedial, corrective, or disciplinary actions up to and including termination of employment. Actual or suspected incidents of misconduct, fraud and unethical or unlawful behavior should be raised using the Ombudsperson Reporting [5]. Dr. Reddy's Non-Retaliation Policy [6] strictly prohibits any form of retaliatory behavior and/or breach of confidentiality, to the extent legally possible, for good faith report of such breaches.

5 Adaptions

There are no adaptions to this policy. In view of diverse and in some cases more stringent requirements under various local Data Protection laws, regional/ country specific policies or procedures may be developed and operationalized for effective implementation of such requirements.

6 Exceptions

There are no exceptions to this policy.

7 Review and Modification

The Data Privacy Officer (or a delegate) in consultation with relevant stakeholders, will review this policy at least once every two years. Modifications, if any, will be made keeping in mind the prevalent Global Data Privacy Regulatory landscape as well as the evolving business environment of the company.

8 References

Reference Number	Document (available on iHub)
1	Code of Business Conduct and Ethics (COBE)
2	Data Privacy Definitions
3	Information Security Management System (ISMS) Acceptable Usage Policy
4	Information Security Incident Management Policy
5	Ombudsperson Reporting
6	Non-Retaliation Policy