






	<b>Data Privacy Breach Management Procedure</b>		Status	Approved
			Version	1.0
			Department	Global Legal & Compliance
	Issued by:	Data Privacy Office	Classification	Internal

Author	Signature	Date
<b>Umesh Prasad</b> Manager - Data Privacy		22.01.19
Reviewers	Signature	Date
<b>Subhajt Deb</b> Chief Information Security Officer		22.1.19
<b>Irfan Ahmed</b> Chief Compliance Officer & Deputy Data Privacy Officer		22.1.19
<b>Suprio Dasgupta</b> General Counsel & Chief Data Privacy Officer		22.01.2019
Approver		
<b>Saumen Chakraborty</b> President & Chief Financial Officer		23.01.2019
<b>Effective date</b>	1-FEB-2019	

#### Revision History

Date	Version	Description of Change	Created/ Modified By
10-01-2018	1.0	Initial Version	Umesh Prasad

	<b>Data Privacy Breach Management Procedure</b>		Status	Approved
			Version	1.0
			Department	Global Legal & Compliance
	Issued by:	Data Privacy Office	Classification	Internal

## Table of Contents

1. Purpose .....	3
2. Scope .....	3
3. Definitions .....	3
4. Responsibility .....	3
5. Data Privacy Breach Management Procedure .....	4
STEP 1: IDENTIFICATION AND CLASSIFICATION .....	4
STEP 2: CONTAINMENT .....	4
STEP 3: EVALUATION AND INVESTIGATION .....	5
STEP 4: NOTIFICATION .....	5
STEP 5: PREVENTION .....	5
6. Data Classification .....	6
7. Data Privacy Breach Management Work flow .....	7
8. ANNEXURE .....	8
9. Abbreviations .....	10
10. Contact Details .....	11

	<b>Data Privacy Breach Management Procedure</b>		<b>Status</b>	Approved
			<b>Version</b>	1.0
	<b>Issued by:</b>	<b>Data Privacy Office</b>	<b>Department</b>	Global Legal & Compliance
			<b>Classification</b>	Internal

### 1. Purpose

This Data Privacy Breach Management Procedure (“**Procedure**”) is to be read along with Global Data Privacy Framework, Local Data Privacy Policies and Global Data Privacy Notice of Dr. Reddy’s Laboratories Limited, its subsidiaries and affiliates (“**Company**”).

This Procedure proposes a standardized management approach to be implemented throughout the Company to, communicate, report, manage and remediate personal data breaches (includes personal and personal sensitive information) in a timely manner as required under local laws.

### 2. Scope

This Guideline applies to:

- All data subjects including but not limited to (employees, customers, contractors, suppliers, gifts’ recipients, Company web-sites’ users, Vendors, Processors, Key Opinion Leaders (“**KOLs**”), patients and Health Care Professionals (“**HCPs**”) whose data is collected/handled/processed/stored by the Company (Controller) or by the vendors(Processors) in any format (including paper records), whether used in the workplace, stored on media backup or cloud, transmitted from the workplace physically or electronically or accessed remotely.
- Data held on all Information Technology (“IT”) systems managed centrally by the Company and any other IT systems managed by outsourced business partners and service providers on which the data is held or processed, including data in physical copies, i.e. automated and non-automated systems of Personal data processing.
- All employees and business partners that are receiving or holding or processing any Personal information on behalf of the Company.
- All locations where the Company operates and where personal information is processed, even if local regulations do not exist in relation to data privacy.

### 3. Definitions

This Guideline shall incorporate by reference the definitions set forth in the Global Data Privacy Framework, the global Data Privacy Notice, and the Local Data Privacy Policies. Any term not specifically defined herein shall adopt such previously defined meanings.

“**Data Privacy Breach**” means and includes, but is not limited to, any illegal usage, unauthorized disclosure, acquisition, access, destruction, alteration of, or any similar action involving Personally Identifiable Information (“**PII**”), Personally Sensitive Identifiable Information (“**PSII**”) or any other incident where the confidentiality, integrity, and availability of personal information may have been compromised, whether by accidental or deliberate causes.

Examples of Data Privacy Breach include either PII or PSII being sent to the incorrect recipient, PII and/or PSII being accessed without authority, and paperwork or computers containing PII and/or PSII being lost or stolen, trans-border transfer with no legal consent of the PII holder.

### 4. Responsibility

Data Privacy Breach is collectively managed by the Chief Information Security Officer (**CISO**) and Regional Data Privacy Officer(s) (“**RDPO**”) of the concerned region supported by the Chief & Deputy Data Privacy Officer(s), Data Privacy Manager, relevant stake holders, Business Process Managers, Manager of IT Services and Facilities and Administration.

Any employee, on being aware of a Data Privacy Breach must report the said breach promptly to [dataprivacy@drreddys.com](mailto:dataprivacy@drreddys.com) or to the responsible employee for data processing in the local jurisdiction, such e-mail address being made available from the local web-site of Dr. Reddy’s representation in the local country of data processing. All employees are responsible for reporting any actual, suspected, threatened or potential Data Privacy Breach and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

	<b>Data Privacy Breach Management Procedure</b>		Status	Approved
			Version	1.0
	<b>Issued by:</b>	<b>Data Privacy Office</b>	Department	Global Legal & Compliance
			Classification	Internal

## 5. Data Privacy Breach Management Procedure

Responding to Data Privacy Breach incidents consists of five key steps:

- Identification and classification
- Containment
- Evaluation and Investigation
- Notification, and
- Prevention

### Step 1: Identification and Classification

A confirmed, potential, or suspected Data Privacy Breach should be promptly reported to Data Privacy team through email "[dataprivacy@drreddys.com](mailto:dataprivacy@drreddys.com)", phone or in person.

The incident can be reported by employees, customers, contractors, suppliers, gifts' recipients, Company websites' users, Vendors, Processors, Key Opinion Leaders ("KOLs"), patients and Health Care Professionals ("HCPs").

Review the incident to determine the next steps. If the reported incident is not a personal data breach, same can be closed post discussion with the incident reporter. If no further action is required, incident can be closed. If the reported incident is a confirmed personal data breach proceed with further investigation.

### Classification of the breach.

- a. **Information Security Breach** - If the breach does not involve loss of any personal or personal sensitive information, the breach shall be classified as Information Security Breach and ISMS Incident Management Policy needs to be followed.
- b. **Physical Security Breach** - If the breach occurs as a result of theft, espionage, terrorist attack and lead to unauthorized access to facilities, equipment and resources shall be classified as Physical Security Breach. Facilities and building administration needs to be notified about the breach. Under given circumstances if physical security breach involves loss of personal data or sensitive personal data, Data Privacy Breach Management Procedure shall to be followed.
- c. **Data Privacy Breach – "Data Privacy Breach"** means and includes, but is not limited to, any illegal usage, unauthorized disclosure, acquisition, access, destruction, alteration of, or any similar action involving Personally Identifiable Information ("PII"), Personally Sensitive Identifiable Information ("PSII") or any other incident where the confidentiality, integrity, and availability of personal information may have been compromised, whether by accidental or deliberate causes.

Log the Data Privacy breach in Incident Management Tool and record the details of the data breach in the in the format in **Annexure I**. Acknowledgement the incident to reporter.

### Step 2: Containment

The measures for the containment of Data Privacy Breach need to be taken as per ISMS Security Incident Management Process, ISMS Acceptable Usage Policy, ISMS Security Logging and Monitoring Policy, Global Data Privacy Framework, COBE and Physical Security Policy.

Containment measures should ensure that:

- Necessary tasks are appropriately allocated and coordinated with concerned team / group for mitigation of the incident
- Guidelines for evidence collection are being followed
- Remedial actions are being followed, recorded and retained (both electronic and physical data)
- Remedial actions are being implemented for containment of incident is reviewed for confirmatory purposes

	<b>Data Privacy Breach Management Procedure</b>		Status	Approved
			Version	1.0
	<b>Issued by:</b>	<b>Data Privacy Office</b>	Department	Global Legal & Compliance
			Classification	Internal

- Local law enforcement agencies within timelines provided under local laws are being notified, if criminal activity is suspected and preserve evidence for investigation (e.g. hacking, theft or unauthorised access);
- The PII holder (whose privacy data has been breached) the was affected) is being notified, due to the breach on measures taken to eliminate the negative consequences of such breach and on preventing the repeated breach further including further steps taken to ensure that the rights of the data subjects is not infringed.

### Step 3: Evaluation and Investigation

Knowing the risks and impact of the Data Privacy Breach, will help to determine the consequences to Dr. Reddy's and data subjects, as well as the steps necessary to notify the regulatory authority and data subjects.

As part of investigation each Data Privacy Breach must be assessed utilizing the breach as enumerated format in Annexure II. Post investigation report for Corrective Actions and Preventive Actions (CAPA) along with Root Cause Analysis (RCA) needs to be prepared.

Concerned RDPO along with DPO in consultation with CISO and concerned data owners may take decision on, shall evaluate the risks and impact of the Data Privacy Breach and shall determine whether the Data Privacy Breach is a Minor Breach or Major Breach. It shall be at the discretion of RDPO, DPO, CISO and Data owner after analysis of risk and mitigating controls to report the incident to supervisory authority. Not all breaches need to be reported to supervisory authority. An indicative guideline is given below.

**MINOR BREACH** – Minor Data breach involves loss of Personal identifiable Information (PII) and leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

**MAJOR BREACH** – Major Data breach involves Personally Identifiable Information (“PII”), Personally Sensitive Identifiable Information (“PSII”) and may be a risk to rights and freedoms of data subjects and such breach could result in:

- Discrimination
- Damage to reputation
- Financial loss
- Loss of confidentiality
- Economic disadvantage
- Social disadvantage
- Any type of humiliation of the human dignity

### Step 4: Notification

#### Notification to Supervisory Authority

Supervisory authority to be notified within 72 hours unless indicated otherwise in the, or within such timeframe as provided under local law. It is the responsibility of the RDPO to ensure that all relevant reporting requirements are complied with as per **Annexure III**.

#### Notification to the any individual (Data Subjects)

In case the breach threatens the rights and freedom of data subjects notify the impacted data. This notification to data subject is intended to provide specific information to the data subjects about the steps they should take to protect themselves (e.g. changing passwords).

### Step 5: Prevention

After the above steps, the relevant stake holders (e.g. CISO, IT managers, Business managers, Facilities) along with RDPO and DPO shall review the cause of the Data Privacy Breach and determine whether existing protections and prevention measures are sufficient to prevent a similar Data Privacy Breach from occurring. The

	<b>Data Privacy Breach Management Procedure</b>		<b>Status</b>	Approved
			<b>Version</b>	1.0
			<b>Department</b>	Global Legal & Compliance
	<b>Issued by:</b>	Data Privacy Office	<b>Classification</b>	Internal

stake holders with DPO and RDPO shall also conduct an investigation of the Data Privacy Breach, and shall recommend regulatory/disciplinary sanctions on responsible employees to HR. The impact assessment of Data Privacy Breach incident must be conducted by RDPO, CISO and relevant stake holders in the format as per **Annexure IV**.

## 6. Data Classification

Data privacy breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that the Company is able to identify the classification of the data and respond to all reported incidents in a timely and thorough manner. All reported incidents will need to include the appropriate data classification in order for assessment of risk to be conducted. Data classification referred to in this policy means the following.

**Personal:** Information that can be used on its own or along with other information to identify, contact or locate a single person or to identify an individual in context. This included but not limited to name, address, phone number, IP address etc.

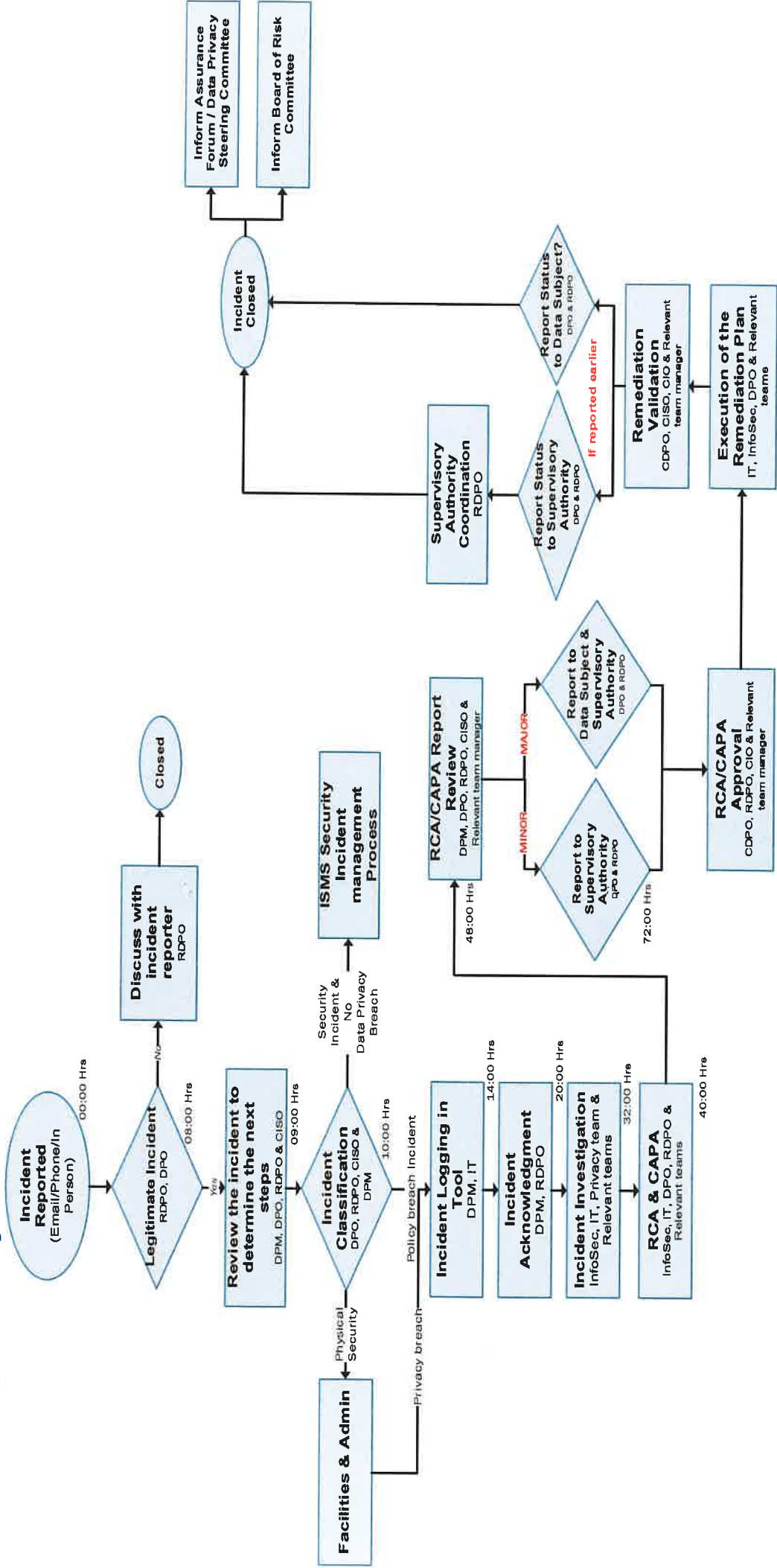
**Sensitive Personal:** Personal Information that requires higher level of protection. Such information may include but not limited to, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, government issued ids (social security numbers, PAN, aadhar etc.) insurance information, criminal charges, conviction/sentence, sexual orientation, health information etc. Data element that make up Sensitive personal information may vary country to country and local laws should be considered while defining the Sensitive Personal Information in the respective counties/geographies.

**Public:** Information which are not confidential and in nature of Personal Data and which are available in public domain.

**Confidential:** Any proprietary information regarding the business operations of Dr. Reddy's including but not limited to technical information, know-how, personal information, personal sensitive information, any information belonging to Dr. Reddy's or derived by any person by reviewing or having access to such proprietary information regardless of the form shall be deemed as Confidential Information.

	<b>Data Privacy Breach Management Procedure</b>		Status	Approved
			Version	1.0
		Department	Global Legal & Compliance	
		Issued by:	Data Privacy Office	Classification
		Internal		

### 7. Data Privacy Breach Management Work flow



	<b>Data Privacy Breach Management Procedure</b>		Status	Approved
			Version	1.0
	<b>Issued by:</b>	<b>Data Privacy Office</b>	Department	Global Legal & Compliance
			Classification	Internal

## 8. ANNEXURE

### ANNEXURE I

#### Data Privacy Breach Incident Report

S No.	Description	Details
1	Date of occurrence of the Incident	
2	Time of occurrence of the Incident	
3	Place of occurrence of the Incident	
4	Name of the person reporting the breach	
5	Nature/description of the breach	
6	Details of any IT systems involved	
7	Description of any immediate actions taken, Preventive steps to avoid such Incident in the future	

### ANNEXURE II

#### Data Privacy Breach Incident Assessment Report

S No.	Description	Details
1	How many people were affected by the Data Privacy Breach incident?	
2	To whom does the personal data belong? (E.g. employees, customers, vendors, KOLs, patients and HCPs)?	
3	What types of personal data were involved?	
4	What is the classification of the data?	
5	Is there a risk to reputation, identity theft, safety and/or financial loss to the Company and/or data subjects?	
6	Do any additional measures have to be put in place to minimise the impact of the data breach?	
7	What caused the data breach?	
8	When and how often did the breach occur?	
9	Who might gain access to the compromised personal data?	
10	Will compromised data affect transactions with any other third parties?	
11	Who all needs to be notified?	



	<b>Data Privacy Breach Management Procedure</b>		<b>Status</b>	Approved
			<b>Version</b>	1.0
			<b>Department</b>	Global Legal & Compliance
	<b>Issued by:</b>	Data Privacy Office	<b>Classification</b>	Internal

### ANNEXURE III

#### Data Privacy Breach Incident Notification to Regulatory Authority

S No.	Description	Details
1	The nature of the personal data breach	
2	The categories and approximate number of data subjects concerned	
3	The categories and approximate number of personal data records concerned	
4	The name and contact details of the Data Protection Officer	
5	A description of the likely consequences of the personal data breach	
6	Do any additional measures have to be put in place to minimise the impact of the data breach?	
7	A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.	

	<b>Data Privacy Breach Management Procedure</b>		Status	Approved
			Version	1.0
	<b>Issued by:</b>	<b>Data Privacy Office</b>	Department	Global Legal & Compliance
			Classification	Internal

#### ANNEXURE IV

#### Data Privacy Breach Incident Impact Assessment Report

S No.	Description	Details
1.	Whether Audits were regularly conducted on both physical and IT-related security measures?	
2.	Whether there are processes that can be streamlined or introduced to limit the damage if future breaches happen or to prevent a relapse?  If yes, please explain.	
3.	Whether there were weaknesses/ vulnerabilities in existing security measures, physical security, business processes and protection measures, or weaknesses in the use of portable storage devices or connectivity to the Internet?  If yes, please explain	
4.	Whether the methods for accessing and transmitting personal data were sufficiently secure?	
5.	Whether support services from external parties should be enhanced, such as vendors and partners?  If yes, please explain	
6.	Whether the responsibilities of vendors and partners is clearly defined in relation to the handling of personal data?	
7.	Whether the users are aware of their responsibilities for Data Privacy, Information Protection and are adequately trained?	
8.	What action needs to be taken to reduce the risk of future breaches and minimize their impact?	

#### 9. Abbreviations

S. No	Abbreviations	Expansion
1.	CDPO	Chief Data Privacy Officer
2.	DDPO	Deputy Data Privacy Officer
3.	RDPO	Regional Data Privacy Officer
4.	DPM	Data Privacy Manager
5.	CISO	Chief Information Security Officer
6.	CIO	Chief Information Officer
7.	IT	Information Technology
8.	HR	Human Resources

	<b>Data Privacy Breach Management Procedure</b>		<b>Status</b>	Approved
			<b>Version</b>	1.0
			<b>Department</b>	Global Legal & Compliance
	<b>Issued by:</b>	Data Privacy Office	<b>Classification</b>	Internal

#### 10. Contact Details

**E-mail ID:** [dataprivacy@drreddys.com](mailto:dataprivacy@drreddys.com)  
**Address:** Data Privacy Officer,  
 Dr. Reddy's Laboratories Limited  
 8-2-337, Road No: 3, Banjara Hills,  
 Hyderabad – 500034,  
 Telangana, India