Data Privacy Risk and Control Assessment Framework

Global Data Privacy

Dr.Reddy's

Data Privacy Risk and Control Framework

Overview of the framework

PURPOSE

To define & assess data privacy controls, thereby ensure ongoing management of 'key' privacy risks & leadership oversight

SCOPE & FREQUENCY

Annually, for all countries where DRL has presence **Program level (5)** and **Country level (14)** Conrols, assessed with help of a total of **52 measurement critera**

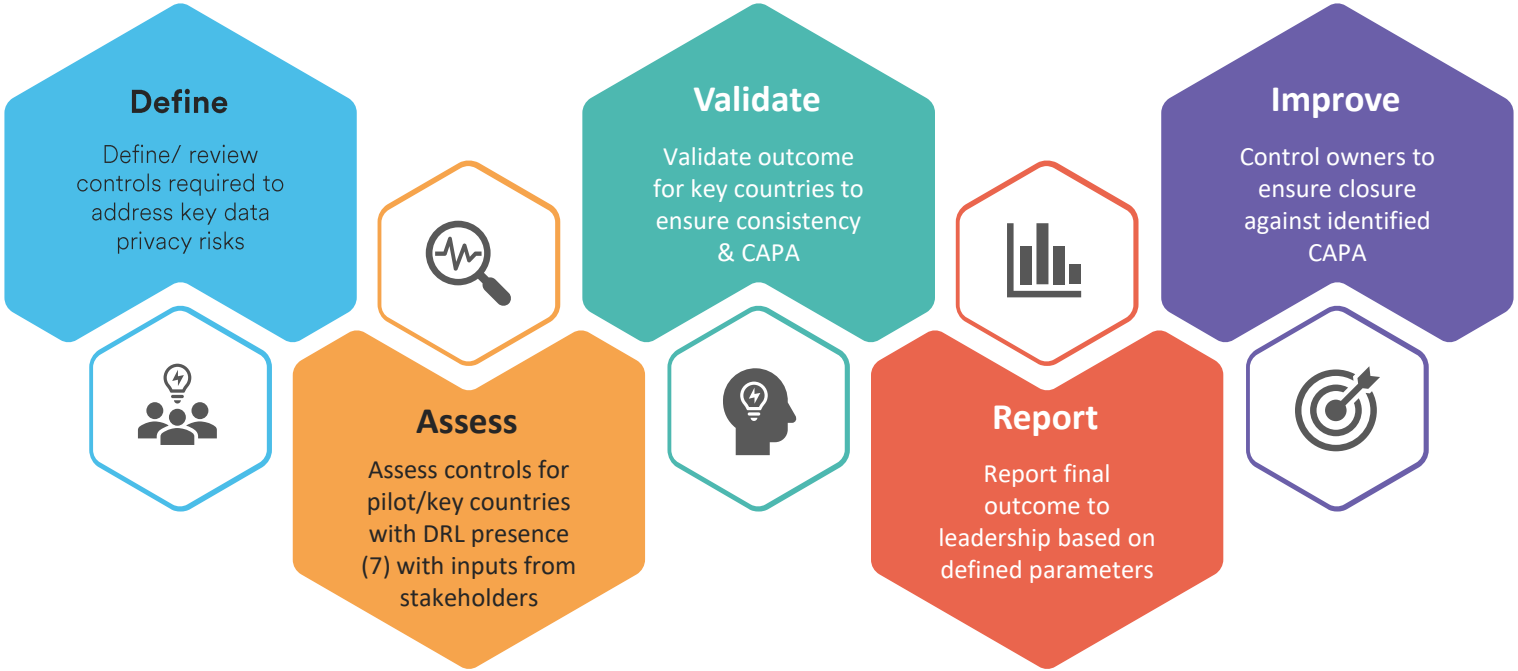
ASSESSMENT APPROACH

Control owners (DP, DPEx, Legal) to assess controls for both implementation status and adequacy. Define & manage CAPA for controls assessed as 'Non-Compliant'

MEASUREMENT

Risk based Control Ratings – Compliant, Partially or Non-Compliant. Improve percentage of controls identified as Compliant and Partially Compliant vs. initial baseline

Data Privacy Control Assessment Process (Annual)



List of Data Privacy Controls and Rating Definitions

Country Level Controls - 14

- Privacy Notices (7*)
- Cookie Compliance (1)
- Legal Basis (7)
- Consent Management (3)
- Data Subject Requests (1)
- Purpose Limitation (1)
- Data Minimization (1)
- Data Transfer Mechanisms/ Localization (4)
- Security, Integrity and Accuracy (1)
- Data Privacy Incident/ Breach Mgmt. (1)
- Minimal Retention (1)
- Records of Processing Operations (1)
- Training and Awareness (1)
- DPO Appointment (1)

Program Level Controls - 5

- DP Organisation and Resources (2*)
- DP Policies and Procedures (11)
- Training and Awareness (2)
- DP Governance (2)
- Monitoring, Audit and Reporting (4)

** Measurement criteria*

Compliant	Control requirements are met with no or insignificant data privacy risk to the company
Partially Compliant	Control requirements are met with some deviations posing minor to moderate data privacy risk to the company.
Non-Compliant	Control requirements are not met with major deviations posing significant data privacy risk to the company

DP Control Assessment Outcome, FY'25 - <Country Name>

DP Risk Category	Control Rating
Privacy Notices	
Cookie Compliance	
Legal Bases	
Consent Management	
Data Subject Requests	
Purpose Limitation	
Data Minimization	

DP Risk Category	Control Rating
Data Transfer Mechanism / Localization	
Security, Integrity & Accuracy	
Data Privacy Incident/ Breach Management	
Minimal Retention	
Records of Processing Operations (RoPA)	
Training and Awareness	
DPO Appointment	

Compliant	Partially Compliant	Non-Compliant	Not Applicable

Key Risks
▪ xxx

Corrective Actions Status <MM'YY>				
Risk	Very High	High	Med.	Low
Total				
Closed				
Open				