

Personal Data Under DPDP: Key Insights and Guidelines

Personal data is any information that relates to an identifiable natural person.

Understanding this concept is essential for DPDP compliance and protecting individual privacy rights.

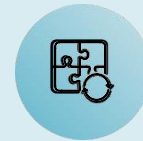
[Schedule a Demo](#)

What Qualifies as Personal Data?



Direct Identification

Information that directly identifies an individual, such as name, ID number, or email address.



Indirect Identification

Data that, when combined with other information, can identify a person.



Automated & Manual

Applies to both digital processing and traditional paper records.

Common Examples of Personal Data

Basic Identifiers

- First and last name
- Home address
- Identification number
- Email address with personal info

Digital Identifiers

- IP address
- Cookie ID
- Location data
- Online identifiers



Even Ganpat Bonde becomes personal data when combined with other identifiers like IP address or location.

Sensitive Personal Data

Special categories require **additional safeguards** and can only be processed in limited



Health & Biometric

Medical records, genetic data, biometric information



Legal & Political

Criminal records, political stands, trade-union membership



Personal Beliefs

Racial/ethnic origin, religious or philosophical beliefs, sexual orientation

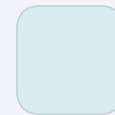
Processing sensitive data is **prohibited by DPDP** except in specific exemptions like employment law o

What's NOT Personal Data?



Legal Entities

Information about companies or public authorities (unless it relates to identifiable individuals like employees or partners)



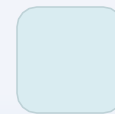
Generic Email Addresses

Addresses without personal information like info@company.com



Deceased Individuals

Information about deceased persons falls outside DPDP scope (though national laws may apply)



Anonymized Data

Data where individuals cannot be identified and the process cannot be reversed

Pseudonymized vs. Anonymized Data

Key Distinction

Pseudonymized data is still considered personal data under DPDP because the process can be reversed to identify individuals.

Anonymized data is not covered by DPDP because individuals cannot be identified and the process is irreversible.

Commitment to Clients



Fast-Track Certifications



Integrated Risk & Compliance Platform



AI-Driven Efficiency



Build Credibility & Confidence



Expand to new territories faster with agility and built to scale

GRC³.io COMMITMENTS

**SPEED &
AGILITY**

**CUSTOMER
EXPERIENCE**

INNOVATION



7 Core Principles

When processing personal data, organizations must comply with these fundamental requirements:

01

Lawfulness, Fairness & Transparency

Process data legally with clear communication

02

Purpose Limitation

Collect data for specific, explicit purposes

03

Data Minimization

Ensure processing is adequate, relevant, and limited

04

Accuracy

Keep data accurate and up-to-date

05

Storage Limitation

Retain data only as long as necessary

06

Integrity & Confidentiality

Implement appropriate security measures

07

Accountability

Demonstrate compliance with all principles

The 4 Building Blocks

WP29 Opinion 4/2007 identifies four essential elements that define personal data:



"Any Information"

Includes objective/subjective data, opinions, assessments in any format or medium - regardless of truth or accuracy.



"Relating To"

Information about an individual through content, purpose (evaluation), or result (impact on rights).



"Identified or Identifiable"

Person is distinguished from others or can potentially be identified.



"Natural Person"

Protection applies to living individuals, not legal entities or deceased persons.

When Does Information "Relate To" an Individual?

Information relates to an individual when at least one of these elements is present:

Content Element

The data is **about** the individual

Purpose Element

Used for **assessment or evaluation** of the individual

Result Element

Processing has an **impact** on the individual's rights and interests

Key Takeaways

Broad Definition

Personal data encompasses any information that can identify an individual, directly or indirectly.

Context Matters

Even seemingly anonymous data becomes personal when combined with other identifiers.

Special Protections

Sensitive categories require additional safeguards and limited processing scenarios.

Compliance is Essential

Organizations must implement the 7 core principles and appropriate security measures when processing personal data.



Visual Dashboard

Continuous insight into all processing activities with clear program overview.

Automated Processes

Innovative SaaS platform designed to automate privacy workflows and minimize risks.

Cross-Departmental Cooperation

Support seamless collaboration ensuring compliance across your organization.

6

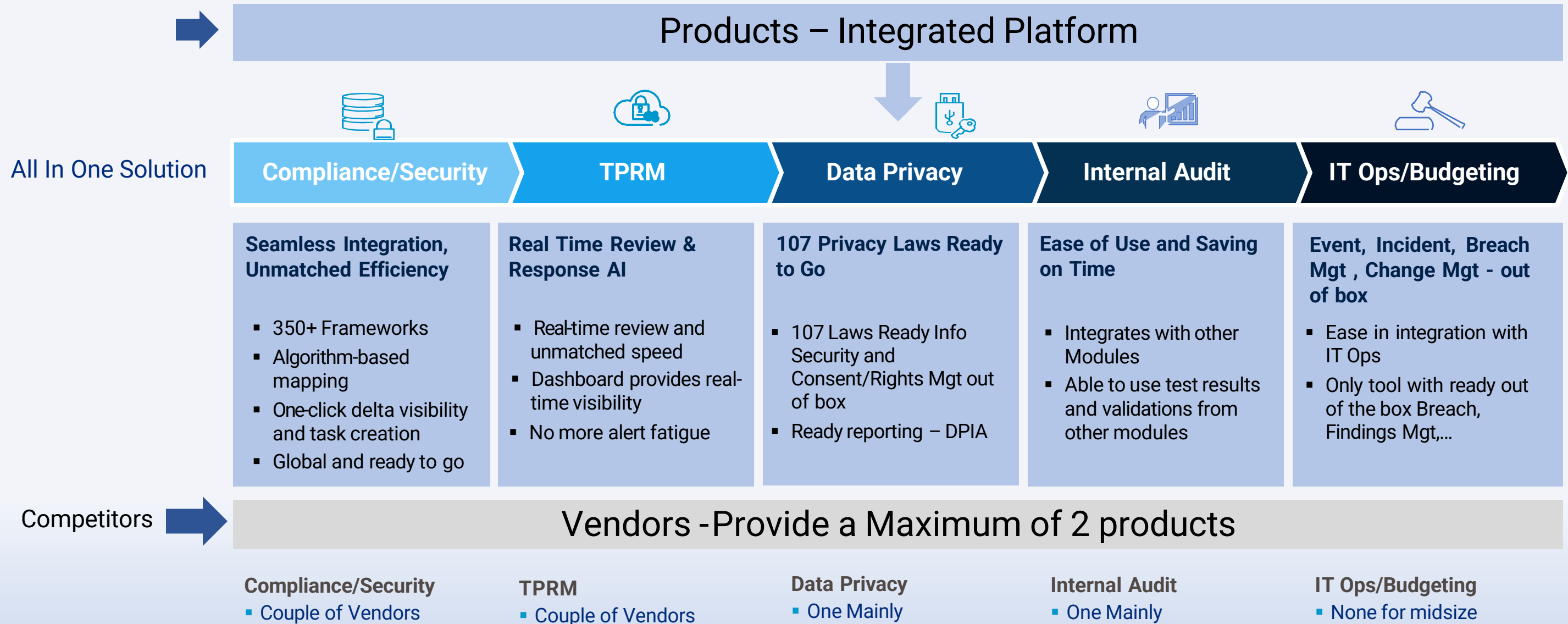
Product Lines

Comprehensive suite addressing key privacy challenges

20+

Multiple Modules

Each targeting specific compliance requirements



← Multiple providers, limited frameworks, duplication of work, lack of integration, risks falling through the gaps, adoption challenges, costs, inadequate reporting, no centralized dashboard, inadequate service management and findings documentation →



Expert Guidance for Your Compliance Journey

GRC Cube provides comprehensive support for navigating India's DPDP Act, from initial assessment through implementation and ongoing monitoring.

Connect With Our Team

info@grc3.io

www.grc3.io



Nidhi P. - Nidhi.p@grc3.io / +91 9004735605

Mayuri B. - mayuri.b@grc3.io / +91 8097235523

Pooja D. - pooja.d@securetain.com

Charu P. - charu.pel@grc3.io