



Data Subject Access Requests:

A Step - by - Step Guide

Comply with the DPDP Act by ensuring data transparency, security

[Schedule a Demo](#)

What is a DSAR?

A Data Subject Access Request (DSAR) empowers individuals to obtain information about the data organizations hold about them. Under DPDP's Right of Access, individuals can verify the lawfulness of processing and understand how their data is used.

DSARs are one of the most common requests organizations receive. Every individual has the right to know the purposes of their personal data processing at reasonable intervals.



Required Information in DSAR Response



Confirmation & Copy

Confirm data processing and provide a copy of personal data



Purpose & Categories

Explain processing purposes and data categories



Third Parties

Disclose any data sharing with third parties



Retention Period

Specify how long data will be kept

Organizations must also provide information about data sources, automated decision-making, and all DPDP rights including rectification and erasure.

Who Can Submit a DSAR?



Customers

Most requests originate from customers rather than employees



Employees

EU employees request data at higher rates than other regions



Partners & Contractors

Anyone whose data is processed can submit a request



Authorized Representatives: DSARs can be submitted on behalf of others with written authorization -parents for children, legal representatives for clients, or appointed guardians.

How Individuals Submit DSARs



Written Requests

Email, forms, or letters



Verbal Requests

Phone calls or in-person



Any Channel

Social media or any department

Requests don't need to mention "DSAR" or "DPDP" - simply asking for data insight qualifies. Key personnel must recognize and respond to these requests promptly.

01

Email Verification

Confirm identity through email correspondence

02

Photo ID

Request identification documents when necessary

03

Login Credentials

Use existing email and password systems

04

Identity Proofing

Leverage specialized verification platforms

Best Practice

According to DPDP Recital 64, use reasonable measures to verify identity - especially for online services. Request only necessary information and avoid formal documents when possible.

Accelerate Compliance Build Trust Scale with Confidence

As risk and regulatory demands surge, businesses need more than spreadsheets. GRC3 is a platform designed and developed by practitioners to **eliminate silos** between compliance, cybersecurity, internal audit, privacy, and vendor risk -enabling enterprises to **scale securely, accelerate revenue, and prove trust** enterprise-wide.

[Learn More →](#)

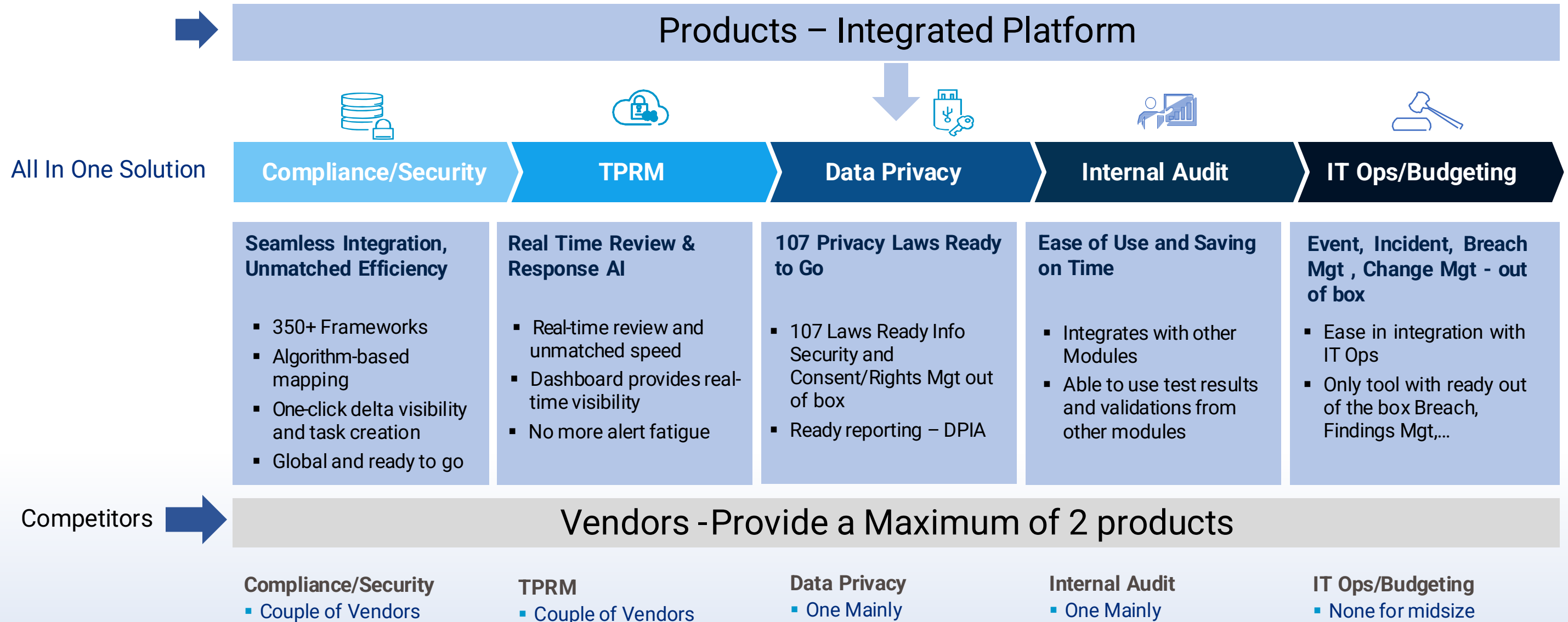
Get Your Free Maturity Assessment

Assess Compliance Maturity



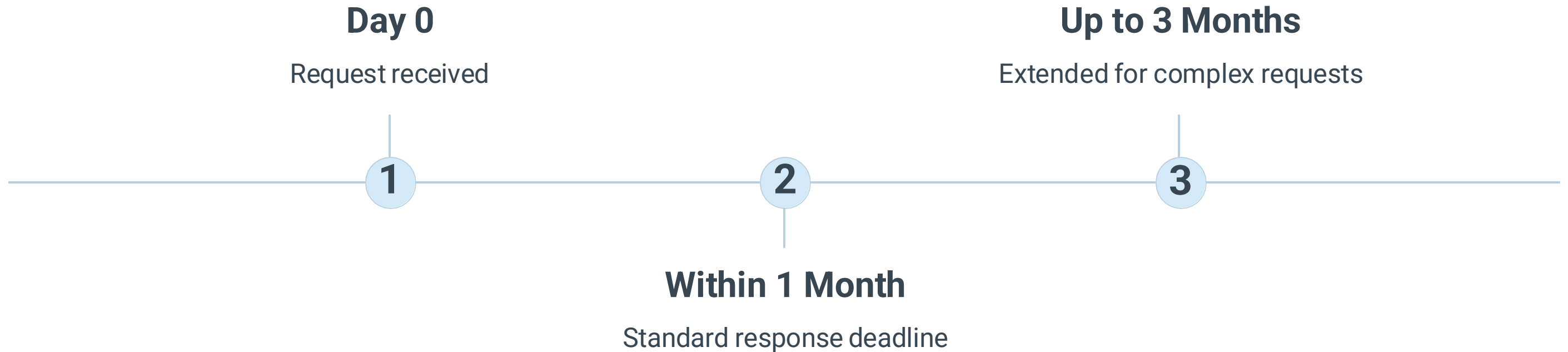
Assess Privacy Maturity





← 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 →

Response Timeline & Fees



Fees

Organizations **cannot charge fees** for DSARs. Exceptions exist only for manifestly unfounded or excessive requests to cover administrative costs.

Warning: The Dutch DPA issued an €830K fine for charging improper fees.

Complex Requests

If extending the deadline, notify the individual within one month with clear reasons for the delay. Multiple simultaneous requests may qualify for extension.

When Can You Refuse?

Manifestly Unfounded

The individual has no real intention to exercise their right or the request has malicious intent with no purpose other than causing disruption.

Manifestly Excessive

The request is unreasonable and disproportionate to the cost or burdens involved with fulfilling the DSAR.

Critical: If refusing a request, you must notify the individual of the reasons, inform them of their right to complain to the supervisory authority, and explain their option to enforce rights through courts. Be prepared to defend your decision.

Why Automate DSARs?



8

GDPR Rights

Organizations must comply with all eight data subject rights

1

Central Platform

Manage all requests from one location

100%

Accuracy

Eliminate human errors in manual processing

Manual DSAR management exposes organizations to significant risks. Top business drivers for automation include DPDP compliance, organizational reputation, CCPA compliance, and customer transparency.

**SPEED &
AGILITY****CUSTOMER
EXPERIENCE****INNOVATION**

Commitment to Clients



Fast-Track Certifications



Integrated Risk & Compliance Platform



AI-Driven Efficiency

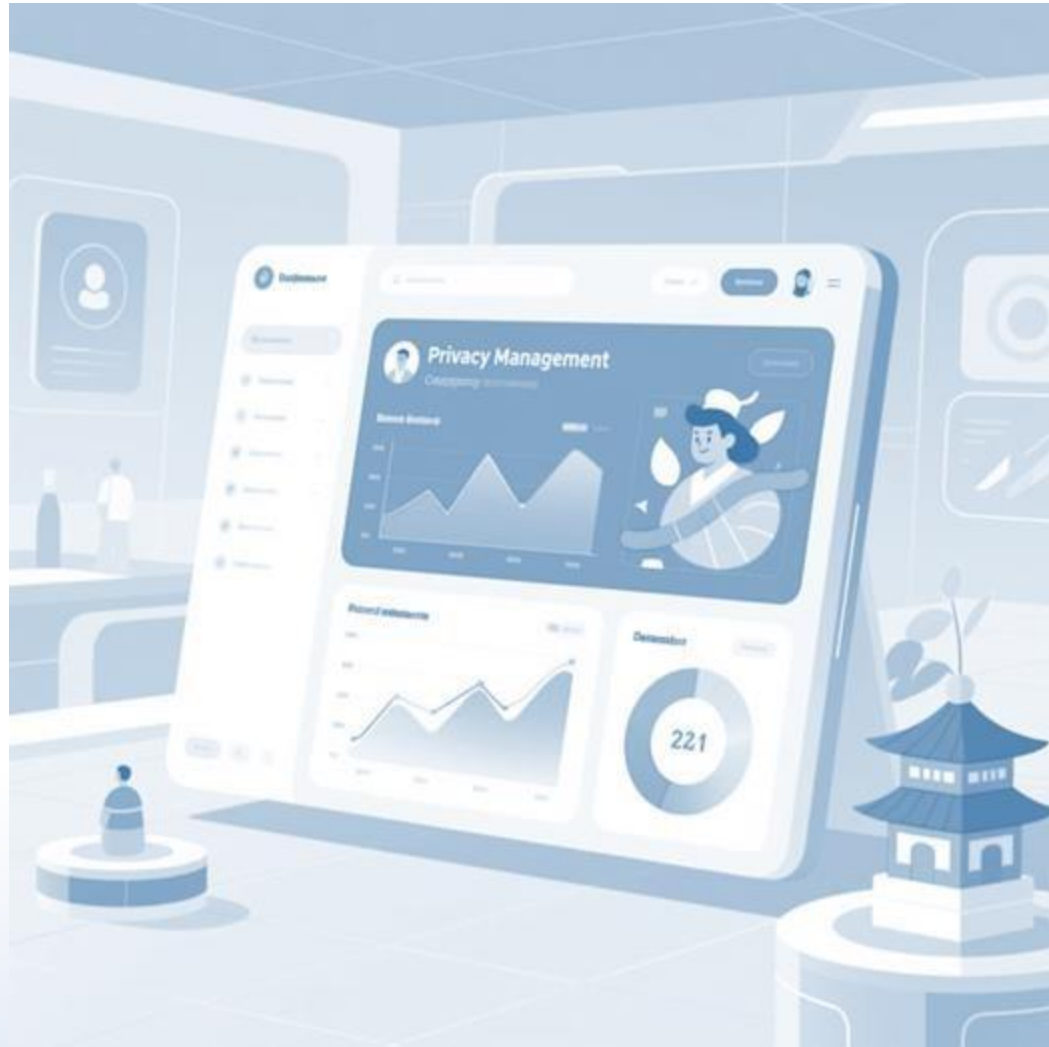


Build Credibility & Confidence



Expand to new territories faster with
agility and built to scale





Automated Workflow

Data Privacy Manager orchestrates the entire DSAR process - from request registration through approval and processing to user notification.

- Central supervision of all requests within response deadlines
- Clear insight at every step of the workflow
- Automated execution across IT systems
- Privacy Portal for customer-facing communication

Combined with Privacy Portal, organizations gain flawless insight into communication preferences, preferred languages, and processing purposes -while data subjects can easily opt-in or opt-out.

www.grc3.io (GRC Cube)

Partner With GRC³ for DPDP Success

Contact:

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

