



From consent to compliance – seamlessly

Understanding Data Subject Rights (DSR)

**A Simple Guide for Enterprises
Under the Digital Personal Data Protection Act, 2023**

Table of Contents

Chapter 1	What is DPDP?
Chapter 2	Data Subject Rights (DSR)
Chapter 3	How a DSR Request Works — Step by Step
Chapter 4	How DataRakshaq Helps You Comply
Chapter 5	Roles & Responsibilities in Your Organization
Chapter 6	Do's and Don'ts for Enterprises

What is DPDP?

India's Digital Personal Data Protection Act (DPDP), 2023 is a landmark law that protects the personal data of every individual in India. Think of it as a set of rules that decides how businesses collect, store, use, and delete your personal information. The law gives individuals — called Data Principals — specific rights over their own data. It also places clear responsibilities on businesses — called Data Fiduciaries — to handle that data fairly and safely.

Key Terms

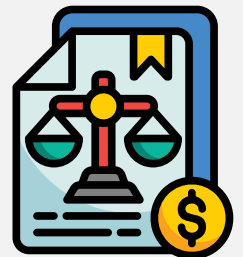
Data Principal

A Data Principal is the individual whose personal data is collected, stored, or processed by an organization. Under the DPDP Act, this person has specific rights over their personal data.



Data Fiduciary

A Data Fiduciary is the organization or company that determines why and how personal data is collected, used, stored, and processed. It is responsible for ensuring compliance with the DPDP Act.



Data Processor

A Data Processor is a third-party vendor or service provider that processes personal data on behalf of the Data Fiduciary. It follows the instructions given by the Data Fiduciary and does not decide how the data is used.



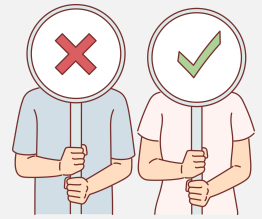
Personal Data

Personal Data is any information that can identify an individual. It includes names, addresses, phone numbers, email addresses, and other information that can be used to identify a person.



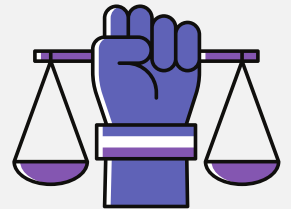
Consent

Consent is the clear and informed permission given by an individual before their personal data is collected or processed. Under the DPDP Act, consent must be specific, voluntary, and easy to withdraw.



DSR (Data Subject Rights)

Data Subject Rights (DSR) are the legal rights individuals have over their personal data. These rights include accessing, correcting, updating, deleting, or withdrawing consent for the use of their personal information.



Data Subject Rights (DSR)



Right to Access Information



Any customer, employee, or vendor whose personal data is held by an organization can use this right. They can ask what personal data the organization has and how it is being used. The organization verifies the request and provides a clear, easy-to-understand summary.

Timeline: Within 30 days.

Right to Correction



If an individual's personal data is incorrect, incomplete, or outdated, they can request a correction. The organization verifies the request, updates the records, and confirms the changes.

Timeline: Within 30 days.

Right to Erasure



If personal data is no longer required or consent has been withdrawn, an individual can request its deletion. The organization checks for any legal retention requirements and permanently deletes the data if none apply.

Timeline: Within 30 days.

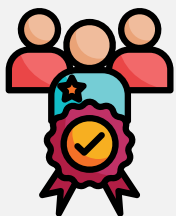
Right to Grievance Redressal



Any individual who believes their data rights have been violated or their request was not handled properly can raise a grievance. The complaint is first submitted to the organization's Grievance Officer. If it is not resolved satisfactorily, the individual can escalate the matter to the Data Protection Board of India (DPBI).

Timeline: Acknowledgement within 48 hours and resolution within 30 days.

Right to Nominate



Any individual can nominate a trusted person to exercise their data rights on their behalf if they become unable to do so. The organization records the nominee's details and processes future requests from the nominee when required.

Timeline: Nomination should be recorded and acknowledged within 7 days.

Right to Withdraw Consent



Any individual who has given consent for data processing can withdraw it at any time. Once the request is received, the organization must stop processing the data for that specific purpose, although any processing carried out before the withdrawal remains valid.

Timeline: Withdrawal must be actioned within 30 days.

How a DSR Request Works — Step by Step



Individual Raises a Request

The Data Principal submits a DSR request via email, portal, or DataRakshaq's self-service platform — specifying the type of right they wish to exercise.



Identity Verification

The organization verifies the identity of the requester to prevent fraud. DataRakshaq automates this step with OTP/document verification.



Request Assessment

The DSR team reviews the request — is it valid? Does a legal basis exist to decline it? Is additional information needed?



Processing the Request

The team processes the request — corrects data, erases records, retrieves data summary, or escalates for grievance resolution across relevant systems.



Response to Individual

A formal response is sent to the individual — confirming action taken, or providing a valid legal reason for declining the request.

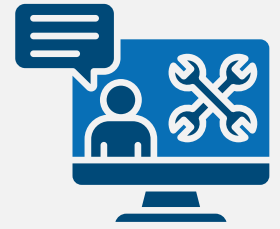


Audit Trail Maintained

DataRakshaq logs every step — request, verification, decision, action, and response — creating a tamper-proof audit trail for regulatory review.

How DataRakshaq Helps You Comply

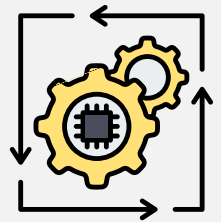
DSR Request Portal: A self-service portal that enables individuals to submit Data Subject Rights (DSR) requests online, supporting all six Data Principal Rights.



Identity Verification Engine: Automatically verifies the requester's identity using OTP, Aadhaar, or document upload before processing requests, ensuring secure handling of all six rights.



Automated Workflow Routing: Routes DSR requests to the appropriate teams, assigns deadlines, and sends alerts to ensure timely processing of all six rights.



Data Discovery & Mapping: Locates personal data across all enterprise systems, making it easier to respond to **Right to Access** and **Right to Erasure** requests.



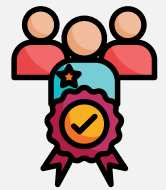
Consent Management Module: Records user consent, manages consent withdrawals, and stops data processing when consent is withdrawn, supporting the **Right to Withdraw Consent**.



Grievance Management System: Captures, tracks, and escalates complaints to the designated Grievance Officer, enabling effective handling of the **Right to Grievance Redressal**.



Nomination Register: Records nominee details and allows authorized nominees to exercise data rights on behalf of individuals, supporting the **Right to Nominate**.



Audit Trail & Reports: Maintains complete audit logs and automatically generates DPDP-ready compliance reports, providing evidence for all six Data Principal Rights.



Compliance Dashboard: Offers a real-time view of pending, in-progress, and completed DSR requests, helping organizations monitor compliance across all six rights.



Penalty Risk Alerts: Continuously monitors request timelines and flags cases approaching deadlines, helping organizations avoid non-compliance and supporting all six Data Principal Rights.





Roles & Responsibilities in Your Organization

Role	Responsibility	How DataRakshaq Helps
Data Protection Officer (DPO)	Oversees DPDP compliance, reviews complex requests, interfaces with DPBI	DPO Dashboard with oversight controls
Grievance Officer	Receives and resolves grievances from Data Principals within timelines	Automated grievance routing to this role
IT / Data Team	Locates, corrects, or erases data from systems upon valid request	Data Discovery tool auto-identifies records
Legal & Compliance	Decides if a request can be declined due to legal obligations	Built-in review workflow with legal flags
HR Team	Handles DSR requests from employees regarding HR data	Separate HR data module with role access
Customer Support	First point of contact for customers raising DSR requests	Integrated ticketing with SLA tracking

Do's and Don'ts for Enterprises



DO's

- **Respond to DSR requests within 30 days** to ensure compliance with DPDP requirements.
- **Verify the requester's identity** before sharing, correcting, or deleting any personal data.
- **Maintain a complete audit trail** of every DSR request and the actions taken.
- **Inform individuals if a request is declined**, clearly stating the reason for the decision.
- **Train employees regularly** on DSR handling procedures and compliance responsibilities.
- **Use DataRakshaq** to automate, track, and manage DSR requests efficiently.
- **Appoint a Grievance Officer** and make their contact details easily accessible to individuals.

DON'Ts

- **Do not ignore or delay DSR requests** beyond the legally mandated timeline.
- **Do not share personal data** without first verifying the requester's identity.
- **Do not process DSR requests verbally** without maintaining proper documentation.
- **Do not reject a request without explanation;** always communicate the reason clearly.
- **Do not assume DSR compliance is only the IT team's responsibility;** it requires organization-wide involvement.
- **Do not manage DSR requests manually** through spreadsheets or emails, as this increases the risk of errors and missed deadlines.
- **Do not make it difficult for individuals to raise grievances;** ensure the grievance process is simple, accessible, and transparent.