

DPDP Act - Section-wise Kaagazz Capability Mapping

A practical reference for legal, privacy, compliance and information-security teams

Purpose

This document maps relevant provisions of the Digital Personal Data Protection Act, 2023 to Kaagazz capabilities and the operational evidence those capabilities can support. It should be read as part of the organisation's wider privacy programme.

Section-wise mapping

DPDP provision	Legal requirement	Kaagazz support	Evidence supported
Sections 4 and 7 Lawful processing and certain legitimate uses	Personal data may be processed only for a lawful purpose, based on consent or a use permitted by the Act.	Consent records consent-based processing. Discover helps identify data being held so the organisation can assess lawful basis and purpose.	Consent record; linked purpose; data-location inventory; review trail.
Section 5 Notice	The Data Principal must receive the prescribed notice describing the personal data, purpose and means of exercising rights.	Consent can preserve the notice presented with the request and connect it to the resulting consent record.	Notice text/version; delivery context; timestamp; acknowledgement.
Section 6(1), 6(4), 6(6), 6(7) and 6(10) Consent, withdrawal and proof	Consent must be specific and informed; withdrawal must be available; processing must cease where required; and notice and consent must be provable.	Consent captures, manages, reviews and withdraws consent while preserving tamper-evident evidence.	Consent artefact; identity context; purpose; timestamp; withdrawal and lifecycle history.
Section 8(3) Completeness, accuracy and consistency	Data used for a decision affecting a person, or disclosed to another Data Fiduciary, must meet the statutory quality requirement.	Secure protects document integrity and controlled versions. Discover helps locate duplicate or dispersed records for review.	Document hash; version/activity history; source location; attributable changes.
Section 8(4) and 8(5) Technical measures and security safeguards	The Data Fiduciary must implement appropriate technical and organisational measures and reasonable safeguards against personal-data breach.	Discover locates exposed PII. Secure applies document-level access, sharing, encryption and rule-based redaction controls.	Scan findings; risk classification; permissions; redaction history; access/activity logs.
Section 8(6) Personal-data breach	A personal-data breach must be notified to the Board and affected Data Principals in the prescribed manner.	Discover and Secure provide visibility and traceable activity to support investigation, impact assessment and notification preparation.	Affected-data inventory; document activity; user/device details; timestamps; investigation evidence.
Section 8(7) Retention and erasure	Personal data must be erased when consent is withdrawn or the purpose is no longer served, unless retention is necessary under law.	Secure supports controlled retention, disposal and removal workflows. Consent records withdrawal that may trigger organisational action.	Retention rule; legal-hold exception; withdrawal; authorised deletion; completion trail.

DPDP provision	Legal requirement	Kaagazz support	Evidence supported
Section 9 Children's personal data	Verifiable parental consent and the Act's protections for processing children's data must be addressed where applicable.	Consent can support a configured parent or guardian consent workflow. The organisation determines applicability and lawful process.	Guardian relationship; verification context; consent; purpose; withdrawal history.
Section 10 Significant Data Fiduciary obligations	Where notified as an SDF, the organisation has additional governance, audit and impact-assessment obligations.	The platform provides inventories, control records and evidence that can support the DPO, independent audit and DPIA process.	PII inventory; risk reports; policy/control records; consent evidence; audit exports.
Sections 11, 12 and 13 Access, correction, erasure and grievance	Data Principals have rights to information, correction/completion/updates, erasure and grievance redressal, subject to the Act.	Discover locates information; Secure supports authenticated access and controlled correction or erasure; Consent supplies consent history.	Request identity; search result; authorised action; response; completion date; grievance trail.

How to use this mapping

Legal teams can use this document to identify where Kaagazz supplies a workflow, control or evidence record. Applicability, lawful basis, notices, retention decisions, policies, regulatory reporting and legal interpretation remain the responsibility of the Data Fiduciary and its advisers.

Product roles

Kaagazz Discover	Visibility: locates PII and sensitive information, identifies storage locations and supports risk review.
Kaagazz Secure	Control and evidence: document-level access, sharing restrictions, encryption, AI-assisted rule-based redaction, integrity and forensic-grade traceability records.
Kaagazz Consent	Consent evidence: captures the notice and purpose context, consent action, authentication details, withdrawal and lifecycle history.

Related evidence law: Bharatiya Sakshya Adhiniyam, 2023

Kaagazz Secure preserves attributable document activity and integrity metadata, including user or role, action, date and time, device or system, machine details, operating-system details and document-hash information. This forensic-grade traceability can support electronic-record verification and evidence preparation under Section 57 and Sections 61-63. Section 63 sets statutory conditions and includes the prescribed certificate requirement.

Kaagazz supports traceability and preparation; it does not determine or guarantee admissibility. Official text: <https://www.indiacode.nic.in/bitstream/123456789/20063/1/aa202347.pdf>

Primary DPDP legal reference

Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), official text published by the Ministry of Electronics and Information Technology: <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>