ORACLE

Addressing India's Digital Personal Data Protection Act (DPDPA) with Oracle AI Database 26ai

A practical approach to supporting India's DPDPA requirements

April 2026, Version 1.0

Purpose statement

This document provides an overview of Oracle AI Database 26ai security features and related products, highlighting how they can be used to help address certain requirements of India's Digital Personal Data Protection Act, 2023 (DPDPA). This document helps evaluators assess options for reducing security risk and improving regulatory compliance for Oracle Database environments. This technical brief is written for CISOs, database administrators, and security architects responsible for Oracle AI Database environments who need both quick wins and a sustainable path to comprehensive security.

This technical brief provides guidance based on current best practices and Oracle product capabilities as of the publication date. Security threats evolve continuously, and organizations should maintain ongoing assessments of their security posture and recovery capabilities.

Disclaimer

This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. Some of the Oracle Database Security technologies may or may not be relevant based upon an organization's specific environment. Oracle strongly recommends testing security solutions within your specific environment to ensure that performance, availability and integrity are maintained.

This document is for informational purposes only and should not be regarded as legal advice or compliance capabilities. It is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

ORACLE

Contents

Executive summary **4**

India's Digital Personal Data Protection Act **5**

Overview 5

Key parties and obligations 5

DPDPA's security mandates for databases 5

Why database security matters 6

Implementation timeline 6

Assessment and compliance evidence 6

Why this matters now 7

Oracle's design philosophy: native, layered, centrally managed **7**

Challenges with bolt-on security 7

Comparing Oracle native security and third-party security tools 8

Mapping Oracle Database Security to DPDPA requirements **9**

DPDPA Section 6 Rules: Technical security mapping summary 9

DPDPA assessment tools: Oracle Data Safe, DBSAT, and Database Security Central 10

Rule 6(a) Encryption: Oracle Transparent Data Encryption 12

Rule 6(a) Anonymization and masking: Oracle Data Redaction 12

Rule 6(a) Static data masking: Oracle Data Masking and Subsetting, and Oracle Data Safe Masking 14

Rule 6(b) Enforcing mandatory access controls: Oracle Database Vault 15

Rule 6(b) Access controls: Oracle AI Database 26ai SQL Firewall 15

Rule 6(b) Access controls for limitation enforcement: Oracle Label Security 16

Rules 6(c) and 6(e) Logging and monitoring: Oracle Unified Auditing 17

Rule 6(d) Availability: Oracle Active Data Guard and Real Application Clusters 19

Conclusion **21**

Key takeaways 21

Learn More **22**

References **22**

ORACLE

Executive summary

Every day, Indian enterprises store millions of records, including customer identities, financial transactions, and health histories, inside Oracle Databases. India's Digital Personal Data Protection Act, 2023 (DPDPA) elevates safeguarding that data from recommended practice to a legal obligation, with severe penalties and lasting reputational consequences for noncompliance. With finalized rules now in place and core compliance obligations scheduled to take effect in May 2027, the question for every Data Fiduciary is no longer *whether* to act. It is *how* to respond decisively and durably without disrupting day-to-day operations.

The finalized DPDPA rules, published in November 2025, leave little room for ambiguity. Section 6 mandates encryption at rest and in transit, access restricted to authorized personnel by stated purpose, tamper-resistant audit trails, continuous monitoring, anonymization for non-identification use cases, and documented availability safeguards. Core obligations take effect in May 2027, leaving 18 months that will outpace most security roadmaps.

This is where many organizations make an expensive misstep. When a new privacy regulation arrives, the common reflex is to add more tools around the database: network monitors, endpoint agents, and application-layer controls. On the surface, that looks like momentum. In reality, it often produces a patchwork of controls with uneven policy enforcement, performance trade-offs, and audit gaps that surface at exactly the wrong time.

Most importantly, in most configurations, network-layer tools cannot reliably intercept queries executed through local database connections. Likewise, external access-control tools typically cannot reliably prevent a privileged DBA from querying personal data. At best, it can only alert after the fact.

Oracle takes a fundamentally different approach. Oracle embeds security directly in the database kernel, where every SQL statement executes, regardless of connection path or user privilege. Transparent Data Encryption helps protect data at rest with AES-256 and a FIPS 140-2–validated key management system. Oracle Database Vault enforces mandatory access controls that prevent even DBA accounts from accessing personal data tables. SQL Firewall blocks unauthorized query patterns before they execute. Oracle Unified Auditing captures a centralized, tamper-resistant record of database activity, including access to personal data as defined in audit policies. Oracle Data Safe and Oracle Database Security Central provide continuous posture management and the structured compliance evidence the Data Protection Board can request at any time.

This technical brief maps each DPDPA Section 6 mandate to the specific Oracle capability that addresses it, explaining not only what each control does but also why database-native enforcement is architecturally superior to alternative approaches. For security architects, it is a technical blueprint. For CISOs and IT teams, it is a business case for treating DPDPA readiness not as a compliance checkbox, but as an opportunity to modernize data security, strengthen customer trust, and operate in India's digital economy with genuine assurance.

The data is already there. The DPDPA deadline is approaching.

ORACLE

India’s Digital Personal Data Protection Act

Overview

India's Digital Personal Data Protection Act (DPDPA) represents a landmark data privacy regulation governing the processing of digital personal data within India and, in specified cases, outside India. Enacted in August 2023, with finalized rules released in November 2025, DPDPA applies to digital personal data collected within India (whether originally digital or later digitized) and to processing outside India when connected to goods or services offered to individuals in India.

DPDPA establishes a consent-first framework that seeks to balance individual privacy rights with lawful data processing needs. The legislation empowers Data Principals (individuals) to control their personal data while imposing clear security, governance, and breach-notification obligations on Data Fiduciaries (organizations). The Data Protection Board of India enforces compliance, with penalties that may reach up to INR 250 crore (approximately USD 27.5 million) for certain violations.

For database security practitioners, DPDPA translates general security obligations into specific technical requirements:

- Encryption of personal data at rest and in transit
- Access controls restricted to authorized personnel by purpose
- Tamper-resistant logging of all personal data access
- Continuous monitoring for unauthorized access
- Anonymization or masking for non-identification purposes
- Availability safeguards with documented business continuity plans

These controls are most effective when enforced at the database layer—where personal data resides. DPDPA's security requirements map directly to Oracle Database Security capabilities, making database-native security controls essential for sustainable compliance.

Key parties and obligations

Data Principal: The individual whose personal data is processed. Data Principals have rights to access, correct, erase, and nominate another individual to exercise their rights.

Data Fiduciary: The organization or person determining why and how personal data is processed. Data Fiduciaries must implement reasonable security safeguards, conduct regular assessments, notify breaches promptly, and maintain audit evidence.

Data Processor: An entity processing data on behalf of the Data Fiduciary under valid contract.

Data Protection Board: The enforcement authority responsible for investigating breaches, imposing penalties, and accepting voluntary undertakings.

DPDPA's security mandates for databases

The finalized DPDPA rules (November 2025) establish six technical security mandates under Section 6. These requirements directly impact databases storing personal data:

Rule 6(a): appropriate data security measures, including securing of such personal data through its **encryption, obfuscation or masking** or the use of virtual tokens mapped to that personal data

Rule 6(b): appropriate measures to **control access to the computer resources** used by such Data Fiduciary or such a Data Processor

Rule 6(c): visibility on the accessing of such personal data, through **appropriate logs, monitoring and review, for enabling detection of unauthorized access, its investigation and remediation to prevent recurrence**

Rule 6(d): reasonable measures for **continued processing in the event of confidentiality, integrity or availability** of such personal data being compromised as a result of destruction or loss of access to personal data or otherwise, including by way of **data-backups**

Rule 6(e): for enabling the detection of unauthorized access, its investigation, remediation to prevent recurrence and continued processing in the event of such a compromise, **retain such logs and personal data for a period of one year**

Why database security matters

Enterprise databases often hold the densest repositories of regulated personal data, including customer records, financial transactions, health information, and identity data. To meet DPDPA obligations effectively, technical security mandates such as encryption, access governance, audit trails, breach response, and availability should be implemented and enforced at the database layer.

Many organizations respond to privacy regulations by layering disparate security tools around the database. This fragmented approach introduces deployment complexity, performance impacts, inconsistent policy enforcement, and audit gaps. External tools operating at the network or application layer generally cannot intercept queries executed through local database connections, direct JDBC connections, or administrative tools.

Database-native security controls operate inside the database kernel, where all SQL statements execute regardless of connection path. These controls protect data before query results return, enforce policies consistently across all applications, and provide complete audit coverage. For DPDPA compliance, database-layer enforcement delivers:

- **Completeness:** Coverage of all connection paths (local, network, internal)
- **Consistency:** Single policy model applied uniformly
- **Tamper resistance:** Controls enforceable even against privileged users
- **Audit integrity:** Kernel-level capture of all SQL execution
- **Minimal performance impact:** Native execution without proxy overhead

Implementation timeline

DPDPA follows a phased implementation schedule to allow organizations time to operationalize compliance requirements:

Effective immediately (November 2025): Data Protection Board establishment, definitions, composition, and procedural provisions

Twelve months from publication (November 2026): Consent Manager registration requirements

Eighteen months from publication (May 2027): Core compliance obligations including consent and notice requirements, reasonable security safeguards (Rule 6), personal data breach notification, data retention rules, Data Principal rights, Significant Data Fiduciary obligations, and Data Protection Impact Assessments (DPIAs)

Organizations should prioritize database security posture assessments, security configuration reviews, sensitive data discovery, and gap analysis during the implementation period to ensure readiness for May 2027 enforcement.

Assessment and compliance evidence

DPDPA requires Data Fiduciaries to maintain documented, evidence-based assessments of their personal data security posture. Organizations must conduct Data Protection Impact Assessments (DPIAs) and periodic security safeguard reviews (Section 8) and must be prepared to demonstrate compliance to the Data Protection Board upon request.

Database security assessment tools provide the structured evidence packages required to satisfy DPDPA assessment obligations:

- Security configuration assessments against best practices and regulatory benchmarks
- Sensitive data discovery to identify personal data locations
- User privilege assessments to verify least-privilege access
- Audit trail analysis demonstrating control effectiveness
- Breach investigation capabilities for impact assessments

Assessment reports must be timestamped, reproducible, and exportable for inclusion in DPIA documentation. Organizations lacking continuous assessment capabilities risk compliance gaps and lack the evidence required to respond to Data Protection Board inquiries.

Why this matters now

With finalized rules in place and an 18-month implementation window, DPDPA readiness should be treated as a business-critical risk priority. Noncompliance can trigger penalties of up to INR 250 crore and cause lasting reputational damage. For most enterprises, the fastest route to durable compliance is to protect personal data where it resides in the database by using native, layered security controls that reduce exposure, streamline audit evidence, and operationalize monitoring at scale.

Organizations that prioritize database security posture management, least-privilege access enforcement, and continuous monitoring will both reduce breach likelihood and demonstrate ongoing control effectiveness. DPDPA compliance becomes not just a regulatory milestone but an opportunity to modernize data security, strengthen customer trust, and enable growth in India with greater assurance.

Oracle's design philosophy: native, layered, centrally managed

Oracle's design approach embeds security controls directly in the database kernel, so protection follows the data, not the perimeter. Native controls reduce disruption because they eliminate the need for application rewrites to achieve baseline protections, and they prevent conflicting policy models that often emerge when multiple third-party tools enforce overlapping rules. This also reduces operational complexity by minimizing extra components and routing dependencies that can introduce latency, outages, and troubleshooting overhead at scale.

Oracle implements "reasonable security safeguards" through a layered, database-defense model that starts with data discovery and classification, then narrows exposure through least-privilege access and separation of duties. It secures data at rest and in motion through encryption and network protections, sustains visibility through continuous monitoring, auditing, and reporting, and proactively mitigates common attack paths such as SQL injection and credential theft. Centralized posture management and remediation guidance help teams keep controls consistent across on-premises, hybrid, and multicloud deployments.

Challenges with bolt-on security

Many organizations depend on non-native add-on security solutions. While these may appear flexible, they often introduce architectural and operational hurdles.

Common non-native strategies and risks include the following.

- **Network-tap or proxy-based Database Activity Monitoring (DAM):** Intercepts or mirrors SQL, and uses regular expression matching making it much easier to bypass.
- **Endpoint-based agents:** Running agents directly on database hosts can create inconsistent deployments, allow versions to drift out of sync, and make updates harder to manage, especially at scale and across hybrid environments.
- **Application-only security controls:** Relying solely on application-layer controls fails to prevent or detect direct database access.

In practice, third-party bolt-on security approaches often lead to:

- **Deployment disruption** due to additional infrastructure and routing changes.
- **Unpredictable performance degradation** as data volumes and workloads increase.
- **Scaling complexity** requiring more tuning and operational effort as deployments grow.
- **Policy fragmentation** causing inconsistencies in enforcement and reporting.
- **Security gaps** where non-uniform capabilities can leave some systems better protected while others remain exposed.

Comparing Oracle native security and third-party security tools

The comparison between Oracle native database security and third-party security products is less about features and more about architecture. The relevant question is not whether a third-party tool provides logging, masking, or access control capabilities, but whether those capabilities are enforceable with the completeness, consistency, and reliability that DPDPA compliance requires.

Security Dimension	Oracle Native Security	Third-Party External Tools
Enforcement Point	Inside the Oracle kernel: policies execute before query results are returned	Outside the database: policies intercept network traffic or application API calls
Local Connection Coverage	Comprehensive: all connections enforced regardless of path in supported configurations	Little to no coverage for network-based tools; partial coverage for agent-based tools
Privileged User Control	Database Vault can restrict DBA access at the kernel level	Generally, cannot prevent privileged access at the kernel level; most can only detect and alert after the fact
Audit Completeness	Unified Auditing captures all SQL execution at the kernel level	Network-based tools miss local connections; agent-based tools can be stopped by OS admin
Tamper Resistance	Unified audit trail protected from modification by all users including DBAs	Separate audit repository can be modified by OS-level administrators
Performance Impact	Minimal: TDE typically introduces less than 5% overhead in internal benchmarks, and auditing runs asynchronously	Proxy-based tools add network latency; agent-based tools consume server resources
Key Management	Oracle Key Vault with HSM integration, up to FIPS 140-2 Level 3 validated	Varies; often lacks Oracle-native key lifecycle integration

Security Dimension	Oracle Native Security	Third-Party External Tools
Attack Surface	No additional network endpoints; no additional processes to compromise	Additional network services, management interfaces, and administrative credentials required
Vendor Accountability	Single vendor responsible for database and security controls	Split responsibility: Oracle for database behavior, third-party for monitoring accuracy
Operational Complexity	Managed through Oracle Enterprise Manager; consistent with DBA skill set	Requires separate administration, separate skill set, and separate operational procedures

Mapping Oracle Database Security to DPDPA requirements

The sections below map each DPDPA Section 6 requirement to specific Oracle Database Security capabilities that address it. The section opens with a high-level summary that links each rule and technical mandate to the corresponding Oracle capabilities.

Each subsection then walks through the regulatory requirement as stated, interprets the technical control it calls for, identifies the relevant Oracle capability, and explains why enforcing these controls natively in the database is architecturally stronger than relying on third party alternatives.

DPDPA Section 6 Rules: Technical security mapping summary

Section 6, read with the November 2025 final rules, translates the DPDPA's general security obligation into six specific technical requirements, each of which maps directly to Oracle Database Security capabilities:

Rule	Technical Mandate	Oracle Capability
6(a): Encryption	Personal data encrypted at rest and in transit; key management documented and auditable; current cryptographic standards	TDE with AES-256; Oracle Key Vault with HSM integration, TLS 1.2/1.3 (26ai) network encryption; FIPS 140-2/140-3-certified modules
6(a): Anonymization and Masking	Personal data used for non-identification purposes must be anonymized or masked; consistent across all access paths	Oracle Data Redaction; Oracle Data Masking and Subsetting
6(b): Access Control	Access restricted to authorized personnel by purpose; privileged access subject to additional technical controls; separation of duties enforced technically	Oracle Database Vault; Oracle SQL Firewall; Label Security; Virtual Private Database

Rule	Technical Mandate	Oracle Capability
6(c): Logging & Audit	Tamper-resistant logs of all personal data access; user identity, timestamp, data accessed, and operation recorded; retained for evidentiary periods	Oracle Unified Auditing; Fine-Grained Auditing; Oracle Data Safe/ Oracle Database Security Central centralized repository
6(d): Availability	Personal data systems resilient to failure; documented RTO/RPO appropriate to processing criticality; tested continuity plans	Oracle Active Data Guard; Oracle RAC; Zero Data Loss Recovery Appliance/Service
6(e): Monitoring	Continuous monitoring for unauthorized access and anomalous activity; alerts generated and acted upon in a timely manner	Oracle Database Security Central ; Oracle SQL Firewall; Oracle Data Safe

DPDPA assessment tools: Oracle Data Safe, DBSAT, and Database Security Central

Regulatory requirement

The DPDPA's assessment obligations including Data Protection Impact Assessments, periodic security safeguard reviews (Section 8(5)), and breach impact assessments (Section 8(6)) — require organizations to maintain documented, evidence-based assessments of their personal data security posture. These assessments must be producible on request to the Data Protection Board and must demonstrate that security controls have been evaluated against identified risks.

Oracle Data Safe

Oracle Data Safe is a unified, cloud-based security service that provides continuous assessment, monitoring, and governance of Oracle Database instances both on-premises and in Oracle Cloud. For DPDPA compliance, Data Safe delivers four critical assessment capabilities:

- Security Assessment: Data Safe's Security Assessment continuously evaluates the security configuration of Oracle Database instances against a comprehensive set of security best practices and regulatory benchmarks. Assessment reports identify configuration risks, categorize them by severity, track remediation progress over time, and generate a documented compliance baseline: the exact evidence package required to demonstrate compliance with the DPDPA's Section 8(5) periodic review obligation.
- Sensitive Data Discovery: Data Safe's Data Discovery module automatically scans Oracle Database schemas to identify columns containing personal data including national identification numbers, financial account data, health information, contact details, and other data categories recognized as personal data under the DPDPA. Discovery results provide the personal data inventory that is the foundation of a DPIA and the prerequisite for configuring targeted security controls.
- User Assessment: Data Safe's User Assessment evaluates database user accounts: identifying over-privileged accounts, dormant accounts, accounts with critical system privileges, and accounts whose privilege profiles deviate from a security baseline. This assessment directly supports the DPDPA's expectation that access to personal data be restricted to authorized personnel.
- Activity Auditing and Alerts: Data Safe provides centralized audit trail collection and analysis across multiple Oracle Database instances, with pre-configured alert policies for high-risk activities—including

bulk data extraction, privileged login failures, schema changes, and access to sensitive data columns. Alert notifications can be routed to security operations teams in real time.

Oracle Database Security Assessment Tool (DBSAT)

Oracle DBSAT is a command-line assessment tool that analyzes an Oracle Database instance and produces a detailed security assessment report covering database configuration, user privileges, security policies, and sensitive data exposure. DBSAT operates entirely within the database environment. No network connectivity is required, making it suitable for air-gapped and restricted environments.

While DBSAT is a valuable utility, this technical brief will focus on the more advanced and comprehensive capabilities in Oracle Data Safe.

Oracle Database Security Central

Oracle Database Security Central (Security Central) is an enterprise security platform that brings access, data, configuration, and activity together into a single, centralized control plane, combining hardened centralized audit repository management with a network-layer database firewall to provide a connected view of risk across your database fleet along with the monitoring, alerting, and reporting capabilities required to satisfy DPDPA Rules 6(c) and 6(e) at enterprise scale.

- Centralized Audit Repository: Security Central collects audit records from Oracle Unified Auditing, Oracle Database Vault, Oracle Label Security. Oracle Database Security Central additionally supports Microsoft SQL Server, MySQL, IBM Db2, PostgreSQL, SAP Sybase, MongoDB, and operating system logs for Linux, Windows, Solaris, and AIX. Security Central also supports audit trails written to files in XML, CSV, and JSON format. You can use custom collectors to collect the audit logs and send them to the Database Security Central server for all the other targets where audit trails are written to database tables consolidating them in a tamper-resistant central repository. This single-pane-of-glass audit capability is well suited for enterprises with heterogeneous database environments.
- Database Firewall: The Database Firewall part of Security Central inspects SQL traffic on the network and applies multilayer policies to allow, log, alert, substitute, or block SQL statements based on session context, SQL structure, and targeted database objects. Policies can enforce trusted paths, prevent SQL injection, restrict bulk reads or modification of personal data tables, and monitor high-volume exports, supporting DPDPA obligations to implement technical controls that preserve confidentiality and integrity of personal data and to detect and mitigate security incidents. In the event of a suspected personal data breach, investigators can query the consolidated audit trail to determine which records were accessed, by which users, from which client locations, and during which periods, providing the evidentiary basis for breach assessment and notification under DPDPA Section 8(6).

Core Oracle capabilities

The combination of Oracle Data Safe, and Database Security Central provides an integrated assessment, monitoring, and reporting capability that third-party tools typically cannot replicate with equivalent completeness for Oracle Database environments. Security Central release updates (RUs) include security and stability fixes from the underlying Oracle Database Release Updates. By applying the latest Security Central RU, customers automatically consume the CVE fixes delivered in the corresponding Oracle Database and platform Critical Patch Updates, reducing exposure to known vulnerabilities without having to track and patch each component separately. Third-party assessment tools lack access to Oracle internal security metadata. Additionally, they cannot assess Database Vault realm configurations, Label Security policies, or Unified Auditing policy completeness with the same depth as Oracle's own assessment tools. For DPDPA compliance, the ability to generate structured, evidence-based assessment reports that demonstrate control effectiveness is as important as the controls themselves.

ORACLE

Rule 6(a) Encryption: Oracle Transparent Data Encryption

Regulatory requirement

DPDPA Rule - "appropriate data security measures, including securing of such personal data through its **encryption, obfuscation or masking** or the use of virtual tokens mapped to that personal data **"**

Personal data must be protected by encryption that renders it unreadable to unauthorized parties. Encryption must cover data at rest, and encryption key management must be implemented in a manner that protects keys from unauthorized access. The cryptographic standards employed must be current and recognized as providing adequate protection against contemporary attack methods.

Required technical control

Encryption must be applied at the database layer to ensure that all copies of data, including database files, backup archives, export files, and storage snapshots, are encrypted consistently. Key management must be centralized, and auditable. The encryption implementation must not require application changes and must not materially degrade database performance.

Oracle Capability: Transparent Data Encryption

Oracle Transparent Data Encryption (TDE) encrypts database data at rest with zero application changes. TDE encrypts data before it is written to disk and decrypts it when authorized processes read it, without requiring any application changes. Encrypting at the tablespace level protects data files, temporary tablespaces, undo tablespaces, redo logs, and RMAN backups in one operation. The default cipher in Oracle AI Database 26ai is AES-256 with XTS mode, aligned with quantum-resistant cryptography best practices.

Oracle capability: Key Vault

Oracle Key Vault (OKV) provides centralized key management for TDE encryption keys. OKV can be configured to store encryption keys in a FIPS 140-2 certified software appliance with Root of Trust in external HSM providing the highest level of key protection available in commercial deployments. Key operations, including key generation, rotation, revocation, and access, are logged in OKV's audit trail, creating a complete evidentiary record to demonstrate compliance with the DPDPA's key management requirements.

Oracle technical advantage

TDE is purpose built to defend against bypass attacks. If adversaries steal storage files, backups, or other media, they gain only unusable ciphertext. TDE leverages native CPU cryptographic instructions (Intel/AMD AES-NI, SPARC, ARM, IBM Power) and integrates with Exadata Smart Scan and Hybrid Columnar Compression (EHCC). Security does not come at the cost of performance. Third-party storage encryption and application-layer encryption solutions generally cannot match TDE's architectural completeness for Oracle Database workloads. Storage encryption helps protect data at rest if someone bypasses the operating system and accesses the underlying storage directly, for example by obtaining the physical storage device. Application-layer encryption requires each application to implement encryption logic independently, creating inconsistent coverage and breaking database functionality (encrypted columns cannot be indexed or searched using standard SQL). TDE encrypts data once, below all applications, covering all access paths consistently and without compromising database functionality.

Rule 6(a) Anonymization and masking: Oracle Data Redaction

Regulatory requirement

DPDPA Rule- "appropriate data security measures, including securing of such personal data through its **encryption, obfuscation or masking** or the use of virtual tokens mapped to that personal data **"**

When personal data is used for purposes that do not require identifying a specific Data Principal, such as application development, call center support, testing, analytics, and reporting, it should be anonymized or masked so it cannot be tied back to an individual.

Masking should be applied consistently across every data access path and should be enforced in a way that application users cannot bypass.

Note: Static data masking (sometimes just called data masking) permanently replaces sensitive values in a copy of the data set, so non-production users work with realistic but irreversibly anonymized data at rest. Dynamic data masking leaves production data unchanged and instead masks sensitive fields on the fly at query time, showing full values only to authorized users and obscured values to everyone else.

Required technical control

Dynamic data masking must be implemented at the database engine level, applying masking transformations to query results before they are returned to the requesting application or user. Masking policies must be configurable by data classification, user role, and application context. Dynamic masking must not alter stored data and must not be configurable or bypassed by unauthorized users.

Oracle capability: Oracle Data Redaction

Oracle Data Redaction enforces dynamic data masking at the database engine level. Redaction policies are defined centrally within the Oracle Database and applied automatically to the results of SQL queries before data is returned to the requesting process. Data Redaction operates on query results; stored data is not altered, providing masking without any impact on the integrity or searchability of stored personal data.

Oracle Data Redaction provides a variety of ways to redact different types of data.

- **Full Data Redaction** to Redact All Data: Masks the entire contents of a specified table or view column.
- **Partial Data Redaction** to Redact Sections of Data: Masks selected portions of the displayed output.
- **Regular Expressions** to Redact Patterns of Data: Masks specific data within a column value using pattern matching.
- **Redaction Using Null Values**: Replaces column data with null values.
- **Random Data Redaction** to Generate Random Values: Replaces the entire value with a random value.
- **Comparison** of Full, Partial, and Random Redaction Based on Data Types: These styles affect Oracle built-in, ANSI, user-defined, and Oracle supplied types differently.
- Central Management of **Named Data Redaction Policy Expressions**: Reuses named policy expressions across columns in multiple tables and views.

Redaction policies can be based on user characteristics: role, application context, session attributes. This enables fine-grained control that reflects the DPDPA's purpose limitation requirements. A user executing a query in a customer service application context may see partially redacted data (last four digits of an account number) while a user in a reporting context sees fully redacted data. This context sensitivity is enforced by the database engine, not by the application.

Oracle technical advantage

Oracle Data Redaction masks sensitive data at query runtime, with no changes to how it's stored on disk. It introduces little to no measurable performance overhead, even on high-throughput systems. Because redaction policies run in the database layer, most applications require no code changes. You can define and manage policies via SQL scripts for automation or through the Oracle Enterprise Manager console. The same capabilities are available for both on-premises Oracle Database and Oracle Cloud Database instances, enabling consistent policy enforcement across environments.

Rule 6(a) Static data masking: Oracle Data Masking and Subsetting, and Oracle Data Safe Masking

Regulatory requirement

DPDPA Rule- "appropriate data security measures, including securing of such personal data through its **encryption, obfuscation or masking** or the use of virtual tokens mapped to that personal data **"**

Rule 6(a) of the Digital Personal Data Protection Rules, 2025 explicitly names masking as a required technical safeguard for personal data. This obligation also applies beyond production systems. Copies of personal data provisioned to development, testing, analytics, or third-party environments carry identical DPDPA protection obligations. These environments are typically less secure, less monitored, and accessed by a wider user community including developers, testers, and third-party contractors making sensitive data proliferation to non-production databases a material compliance risk.

Required technical control

Before masking can be applied, the personal data requiring protection must first be identified through sensitive data discovery. Static masking is then applied to replace production personal data with realistic, format-consistent, non-identifiable substitutes before any copy is provisioned outside the production environment. Masked output must preserve referential integrity so the database remains functionally valid. The process must be repeatable and documented to demonstrate compliance to the Data Protection Board.

Oracle capability: Oracle Data Masking and Subsetting

Oracle (static) Data Masking and Subsetting addresses the full discover-then-mask workflow. The sensitive data discovery capability scans Oracle Database schemas to identify columns containing personal data, producing a personal data inventory that serves as both the input to masking policy configuration and documented evidence of where personal data resides directly supporting the accountability obligations.

Masking then replaces identified personal data in a database copy with non-identifiable substitutes before that copy is provisioned to development or testing teams. Production data is never altered. Masking definitions are configured once and applied consistently each time a masked copy is produced, preserving referential integrity and format constraints across all related tables so the masked database remains operationally valid.

The Subsetting capability provisions a representative subset of rows rather than a full database copy, limiting the personal data footprint in non-production environments to what is strictly necessary directly reflecting data minimization principle.

Oracle capability: Oracle Data Safe Masking

Oracle Data Safe delivers data discovery and static data masking as integrated capabilities within a single service, available for Oracle Cloud databases, on-premises deployments, third-party clouds, and Oracle Database@Multicloud. Data Safe's Data Discovery module scans schemas and identifies personal data columns, including national identification numbers, financial account details, healthcare information, employment data, and contact information. Those results feed directly into masking policy configuration, eliminating any manual translation between discovery and masking.

Oracle technical advantage

Both tools are built for Oracle Database and access Oracle internal metadata, including schema definitions, constraint relationships, data type characteristics, and application dependencies. If a masked copy breaks Oracle-specific referential integrity or produces format-invalid substitutes, it fails functionally. In practice, that drives organizations to skip masking or revert to production data. Neither outcome satisfies the DPDPA. Oracle's native masking tools produce copies that are both compliant and operationally valid.

Rule 6(b) Enforcing mandatory access controls: Oracle Database Vault

Regulatory requirement

DPDPA Rule- "appropriate measures to **control access to the computer resources** used by such Data Fiduciary or such a Data Processor **"**

Access to personal data must be restricted to personnel whose access is required for the stated processing purpose. Privileged users, including database administrators, system administrators, and other infrastructure personnel, must be subject to controls that prevent unauthorized access to personal data even where they have administrative privileges over the database infrastructure.

Required technical control

Mandatory access controls must be implemented that are not bypassed by privileged users. Database administrators must be restricted from querying tables containing personal data unless their access to that specific data is explicitly authorized as part of their defined role. Separation of duties must be enforced technically, not merely by policy.

Oracle capability: Oracle Database Vault

Oracle Database Vault is an internal database security control that creates protective realms around application data and enforces fine-grained rules on who can access which objects, from where, and under what conditions, even for highly privileged accounts such as DBAs. By enforcing strong separation of duties and blocking unauthorized privileged access to sensitive personal data, Database Vault helps organizations implement the "need-to-know" and "purpose limitation" controls that support compliance objectives, while also reducing insider threat and configuration error risk for regulated workloads.

Oracle technical advantage

Because Oracle Database Vault enforces realms and command rules inside the Oracle Database kernel, it provides mandatory controls that external access-control tools cannot easily match. Third-party privilege management products can monitor and alert on privileged activity, but they typically see a DBA's query only after the database has executed it. By contrast, a Database Vault mandatory realm can block even a fully privileged user from querying a protected personal data table unless they are explicitly authorized. These controls are designed for low overhead in typical deployments. Oracle testing and customer benchmarks report only minimal additional CPU usage, so organizations gain strong protection against insider access without a noticeable impact on performance.

Rule 6(b) Access controls: Oracle AI Database 26ai SQL Firewall

Regulatory requirement

DPDPA Rule-" appropriate measures to **control access to the computer resources** used by such Data Fiduciary or such a Data Processor **"**

The DPDPA's access control mandate requires restricting access to personal data not only by user identity, but also by the nature and pattern of the SQL operations being performed. Unauthorized SQL access patterns, such as bulk extractions, access from unexpected applications, and queries that touch personal data tables without legitimate application context, must be detectable and prevented as part of a technically enforced access control regime.

Oracle capability: Oracle AI Database 26ai SQL Firewall

Oracle SQL Firewall, native to Oracle AI Database 26ai, is a kernel-level SQL access control feature that can enforce an allowlist of approved SQL statements and connection paths for each database account. Unlike

network-layer database firewalls, which intercept SQL at the TCP level and are blind to local connections, Oracle SQL Firewall operates inside the Oracle Database kernel. It enforces SQL allowlists before any SQL statement executes, regardless of the connection path.

For DPDPA compliance, Oracle SQL Firewall addresses several high-risk scenarios directly.

- SQL Injection Attack prevention: SQL Firewall's allowlist enforcement blocks injected SQL that does not match legitimate application SQL patterns: providing a database-kernel-level defense against SQL injection that operates independently of application-layer input validation.
- Application account privilege restriction: Application service accounts that should only execute specific, approved SQL statements are restricted to exactly those statements. An attacker who compromises an application and gains access to its database credentials cannot execute arbitrary SQL, only the approved allowlist statements will execute.
- Anomalous access detection: SQL Firewall generates audit records for all allowlist violations, including the full SQL text, the connection context, and the violation type. These records can be feed directly into Database Security Central and Data Safe (or third-party SIEM systems) for real-time alerting and forensic investigation.
- Connection context enforcement: SQL Firewall can enforce that specific database accounts are accessible only from approved operating system users, approved program names, or approved network addresses. This helps prevent legitimate credentials from being used in an unauthorized context, such as blocking a web application service account from being used interactively by a developer on the database server.

Oracle technical advantage

Oracle SQL Firewall's kernel-level enforcement is architecturally distinct from network-layer database firewalls. Network-layer firewalls (including the firewall component of Oracle Database Security Central) intercept SQL at the network level and are blind to local database connections. Oracle SQL Firewall operates inside the database kernel and enforces allowlists for every connection type, including local, network, and internal. This kernel level enforcement helps provide broader coverage across Oracle Database connection paths than network layer database firewalls. Its native integration with Oracle Unified Auditing helps ensure that all violations are recorded in the same tamper-resistant audit trail used for all other DPDPA compliance evidence.

Rule 6(b) Access controls for limitation enforcement: Oracle Label Security

Regulatory requirement

DPDPA Rule- “appropriate measures to **control access to the computer resources** used by such Data Fiduciary or such a Data Processor **“**

Personal data should be processed only for the purpose for which it was collected and for which consent was obtained. Technical controls should enforce purpose limitation by conditioning access to personal data on the declared processing purpose. Data collected for one purpose should not be accessible for a different purpose without an appropriate legal basis and, where required, fresh consent.

Oracle Capability: Oracle Label Security

Oracle Label Security (OLS) implements a mandatory row-level access control framework based on security labels. Each row in a database table can be assigned a security label that reflects the processing purpose, data classification, and consent context associated with the data in that row. Access decisions are made by comparing the label on the data row with the label clearance of the requesting user or application session.

As an example, a DPDPA-compliant OLS implementation might be described as follows:

- Consent labels – Personal data rows are labeled with the processing purposes for which the Data Principal has provided consent. A customer who has consented to marketing communications but not to data sharing with third parties has their data labeled to reflect this distinction.
- Application context labels – Application sessions are assigned label clearances that reflect the processing context of the application; a marketing application has clearance to access marketing-consented data, while an analytics application has clearance only for anonymized or aggregated data.
- Row-level enforcement – OLS enforces label-based access control at the individual row level within a table. A query that retrieves customer records will automatically exclude rows for customers whose labels do not permit access by the requesting application context without additional application-level programming required.
- Write controls – OLS also controls data write operations, ensuring that updates to personal data rows comply with label policies and that label assignments cannot be altered by application users.

Oracle technical advantage

Application logic can express *allowed uses of personal data*, but enforcing those use restrictions reliably at the row level outside the database is fragile because every application, API, report, and administrative tool must implement the same rules without gaps. A single unchecked access path, such as a reporting query that bypasses those checks, can expose sensitive personal data to unauthorized use. Oracle Label Security enforces these data-use restrictions inside the database engine by classifying rows with security labels and mediating every access based on the user's clearance, so the same row-level policy applies consistently across all access paths.

Rules 6(c) and 6(e) Logging and monitoring: Oracle Unified Auditing

Regulatory requirement

DPDPA Rule- "visibility on the accessing of such personal data, **through appropriate logs, monitoring and review, for enabling detection of unauthorized access, its investigation and remediation to prevent recurrence"**

DPDPA Rule- "for enabling the detection of unauthorized access, its investigation, remediation to prevent recurrence and continued processing in the event of such a compromise, **retain such logs and personal data for a period of one year"**

Data Fiduciaries must maintain complete, tamper-resistant logs of all access to and processing of personal data. Logs must record the identity of the accessing user, the time of access, the data accessed, and the operation performed. Logs must be retained for a period sufficient to support investigation of a personal data breach and must be available to the Data Protection Board upon request.

Oracle capabilities: Oracle Unified Auditing with Oracle Data Safe and Database Security Central

Oracle Unified Auditing

Oracle Unified Auditing provides a centralized, policy-driven audit framework that captures database activity at the kernel level. It consolidates all Oracle Database audit trails, including traditional database audit, fine-grained auditing (FGA), Oracle Database Vault audit, Oracle Label Security audit, RMAN audit, Oracle Data Pump audit, and Data Guard audit, into a single, consistent audit trail stored in the AUDSYS schema and protected from modification by any database user, including SYS.

Key features of Oracle Unified Auditing for DPDPA compliance:

- Policy-driven audit configuration – Unified Audit policies can be configured to capture all access, or to capture access selectively, for specific tables, schemas, or data classifications. For personal data tables, audit policies can be configured to record every SELECT, INSERT, UPDATE, DELETE, and DDL operation, with full capture of the SQL text, bind variables, user identity, session information, and execution context.

- Fine-grained auditing – Oracle Fine-Grained Auditing (FGA) enables audit capture to be conditioned on the content of query results capturing audit records only when a query returns rows that match specified conditions (for example, rows containing health data or financial account numbers). This allows high-volume audit environments to focus capture on the specific access events most relevant to DPDPA compliance.
- Tamper resistance – The Unified Audit trail stored in the AUDSYS schema cannot be modified or deleted by any database user other than the specifically designated audit administrator. Even a DBA with full administrative privileges cannot alter audit records. This tamper-resistant property is essential for the audit trail to serve as a reliable evidentiary record.
- Write-to-OS and external SIEM integration – Unified Auditing can write audit records to operating system audit trails and can stream records to Security Information and Event Management (SIEM) systems using standard syslog protocols. This enables integration with enterprise security operations centers for real-time monitoring and alerting.

Audit trail retention and archival: Oracle Database Security Central or Oracle Data Safe extends Unified Auditing with centralized audit repository management, automated retention policy enforcement, and compliance reporting. Security Central /Data Safe provides prebuilt reports for major regulatory frameworks and can generate compliance evidence reports specifically structured for regulatory inquiries.

Oracle Data Safe

For DPDPA compliance, Data Safe (see Oracle Data Safe) provides centralized audit trail collection and analysis across multiple Oracle Database instances, with preconfigured alert policies for high-risk activities such as bulk data extractions, privileged login failures, schema changes, and access to sensitive data columns. Alert notifications can be routed to security operations teams in real time.

Oracle Database Security Central

Oracle Database Security Central (see Oracle Database Security Central) is an enterprise security platform that brings access, data, configuration, and activity together into a single, centralized control plane, combining hardened centralized audit repository management with a network-layer database firewall to provide a connected view of risk across your database fleet along with the monitoring, alerting, and reporting capabilities required to satisfy DPDPA Rules 6(c) and 6(e) at enterprise scale.

Oracle technical advantage

Oracle Unified Auditing, Oracle Data Safe, and Oracle Database Security Central provide Oracle native controls that integrate tightly with Oracle Database. For Oracle specific workloads, this depth of integration can give DBAs and security teams stronger visibility and simpler day to day operations.

Because these tools understand Oracle specific configurations, privileges, audit records, and wire protocols, they can deliver higher fidelity security and user assessments, along with richer audit trails across large fleets. By contrast, third party audit tools typically maintain audit data in their own repositories, separate from the Oracle Database. This separation can introduce a potential gap between what the database executed and what the monitoring tool recorded.

Oracle Unified Auditing generates audit records as an integral part of SQL execution, which helps support completeness and consistency in ways that external monitoring may not match. Audit records can also be stored in the tamper resistant repository of Oracle Data Safe or Oracle Database Security Central.

Because both platforms are designed, maintained, and supported by Oracle, they align with database release cycles and can reduce the integration, tuning, and lifecycle management overhead that is often associated with third party database security tools.

Rule 6(d) Availability: Oracle Active Data Guard and Real Application Clusters

Regulatory Requirement

DPDPA Rule- "reasonable measures for **continued processing in the event of confidentiality, integrity or availability** of such personal data being compromised as a result of destruction or loss of access to personal data or otherwise, including by way of **data-backups"**

Personal data processing systems must be resilient to technical failure. Business continuity and disaster recovery capabilities must ensure that personal data is available for processing when required, and that recovery from system failures occurs within timeframes appropriate to the criticality of the data and the processing obligations of the Data Fiduciary.

Oracle capability: Oracle Active Data Guard and Real Application Clusters

Oracle Active Data Guard (ADG) maintains one or more real-time synchronized physical standby databases that can be open for read-only workloads while they continuously apply redo from the primary database. This architecture delivers strong protection against data loss and corruption, automatic failover for site or database outages, and the ability to perform rolling upgrades with near-zero downtime, helping data fiduciaries satisfy DPDPA expectations for availability and continuity of processing for personal data. By offloading reporting, analytics, backups, and other read-mostly operations to the standby, organizations can keep primary systems focused on transactional workloads, improve performance for data principals, and maintain resilient, geographically distributed copies that support both disaster recovery and data localization strategies under India's evolving regulatory landscape.

Oracle Real Application Clusters (RAC) runs a single Oracle Database across multiple servers in an active-active cluster, giving all nodes shared access to the same data while coordinating a global cache so transactions remain consistent. If one server or instance fails, connections seamlessly fail over to surviving instances that are already open, which helps data fiduciaries meet DPDPA expectations for high availability and continuity of processing for personal data. RAC also lets organizations scale capacity horizontally by adding nodes online and load-balancing sessions across the cluster, so they can handle peak traffic and growth without downtime while maintaining service levels for data principals and critical regulatory processes.

Combined with ADG, RAC provides a layered availability architecture: RAC protects against server node failure, while ADG protects against site-level failures and data corruption.

For DPDPA compliance, these capabilities address the availability obligation in several ways:

- Recovery Time Objective (RTO) – ADG failover can be configured for automatic failover with an RTO of seconds: the time required for the standby database to accept connections after detection of a primary failure. This supports business continuity plans that require near-zero downtime for personal data processing systems.
- Recovery Point Objective (RPO) – Synchronous redo shipping (in Data Guard Maximum Availability or Maximum Protection modes) ensures zero data loss on failover. In Maximum Availability or Maximum Protection modes, the RPO is effectively zero for committed transactions. This can significantly reduce the risk of losing personal data in a database failure event.
- Data Guard Snapshot Standby – ADG's Snapshot Standby feature allows the standby database to be opened in read-write mode for testing, development, or reporting purposes, then re-synchronized with the primary without disruption. This enables DPDPA-compliant testing workflows that use production-like data environments without exposing production personal data.

Oracle technical advantage

Compared with many third-party or "build-your-own" availability stacks, Oracle delivers an integrated, in-database architecture where Oracle Real Application Clusters (RAC) and Oracle Active Data Guard (ADG) are engineered and tested together as native database features. This avoids the operational and support complexity

of stitching together separate clustering, replication, and monitoring products, while still providing clearly defined RTO/RPO targets and automatic failover paths aligned with DPDPA Rule 6(d). Because RAC and ADG are part of the same Maximum Availability Architecture and managed through a unified toolset, data fiduciaries can implement resilient, DPDPA-compliant continuity plans with fewer moving parts, consistent behavior across sites, and a single vendor accountable for end-to-end data availability.

Conclusion

India's DPDPA represents a major turning point for how digital personal data is handled. It puts consent first, strengthens individual rights, and raises the bar on organizational accountability, supported by real enforcement and significant penalties. With finalized rules in place and an 18-month runway to implement, DPDPA readiness is best treated as a core risk and trust initiative, not a box-checking exercise.

For most enterprises, the most direct route to durable compliance is simple in principle: protect the data where it lives, at the database layer. Using native, layered database controls can reduce exposure and produce the structured, repeatable evidence DPDPA expects. A program built on sensitive data discovery, least-privilege access, encryption and masking, tamper-resistant auditing, continuous monitoring, and resilient availability maps cleanly to DPDPA's standard of reasonable security safeguards, while sidestepping the fragmentation, performance tradeoffs, and audit blind spots that often come with bolt-on security.

Key takeaways

- **Enforce at the source**. Database-native controls cover every connection path-local, network, and internal-and apply policy enforcement before results are returned. Network-layer tools typically do not provide the same end-to-end coverage.
- **Restrict privileged access technically**. Separation of duties on paper is not enough. Oracle Database Vault enforces restriction at the kernel level, even for DBA accounts.
- **Make compliance evidence continuous**. DPDPA expects Data Fiduciaries to prove controls work, not merely claim they do. Oracle Data Safe and Security Central provide timestamped, reproducible assessment evidence that the Data Protection Board can request at any time.
- **Start the assessment now**. With core obligations enforceable from May 2027, the current implementation period should be used to prioritize security posture assessments, sensitive data discovery, and gap analysis.

When approached thoughtfully, DPDPA readiness becomes more than a regulatory checkpoint. It can serve as a strong foundation for long term data security, deeper customer confidence, and the day-to-day operational assurance needed to grow in India's digital economy.

ORACLE

Learn More

Experience Oracle Database security in action and explore hands-on labs designed to support DPDPA compliance by visiting livelabs.oracle.com.

For personalized support or questions on DPDPA and Oracle Database, please contact your Oracle Account Representative or visit oracle.com/contact.Oracle Database security features can support DPDPA compliance efforts and help build a long-term foundation for data trust when implemented and operated appropriately

References

Digital Personal Data Protection Act 2023

meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

Digital Personal Data Protection Finalized Rules Nov-2025

meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf

Oracle.com for datasheets, technical briefs, FAQ, documentation, references, blogs, forums, and demonstrations for Oracle Database Security products:

oracle.com/in/security/database-security/