National e-Governance Division
Ministry of Electronics and Information Technology

Digital India
Power To Empower

Business Requirement Document

For

Consent Management

Under the DPDP Act, 2023

National e-Governance Division
Ministry of Electronics and Information Technology

Digital India
Power To Empower

Contents

1 Introduction 3
2 Objectives 3
3 Key Stakeholder and Responsibilities 3
4 Functional Requirements 4
4.1 Consent Management Lifecycle 4
4.1.1 Consent Collection 4
4.1.2 Consent Validation 9
4.1.3 Consent Update 11
4.1.4 Consent Renewal 14
4.1.5 Consent Withdrawal 17
4.2 Cookie Consent 22
4.3 User Dashboard 25
4.3.1 View Consent History 25
4.3.2 Modify or Revoke Consent 25
4.3.3 Raise Grievances or Data Requests 26
4.4 Consent Notifications 27
4.4.1 User Notifications 27
4.4.2 Data Fiduciary and Processor Alerts 28
4.5 Grievance Redressal Mechanism 29
4.5.1 Complaint Logging 29
4.5.2 Resolution Tracking 30
4.6 System Administration 32
4.6.1 User Role Management 32
4.6.2 Data Retention Policy Configuration 33
4.7 Logging 33
4.7.1 Audit Logs 34

1 Introduction

The Business Requirements Document (BRD) for the Consent Management System (CMS) outlines the objectives and functionalities of the platform designed to align with the Digital Personal Data Protection (DPDP) Act. As personal data protection becomes increasingly critical, organizations face growing challenges in managing consents transparently and effectively while maintaining regulatory compliance. The CMS addresses these challenges by enabling seamless consent management across its lifecycle, including collection, validation, updates, withdrawal and audit readiness.

This document serves as a guideline for the development and deployment of a system that empowers Data Principals to exercise their rights over their personal data. It provides Data Fiduciaries and Processors with the necessary tools and integrations to process consents securely and in compliance with the legal framework.

The BRD defines the CMS's functional requirements. It includes a detailed breakdown of core modules such as Consent Lifecycle Management, User Dashboard, Notifications and Grievance Redressal Mechanisms. Additionally, the document outlines administrative capabilities, including user role management and data retention policy configuration, to ensure operational efficiency and compliance.

2 Objectives

The objective of the Consent Management System is to:

- Enable Comprehensive Consent Lifecycle Management: Facilitate the full lifecycle of consent, including collection, validation, modification, renewal and withdrawal, in alignment with the requirements of the DPDP Act and its rules.
- Empower Data Principals: Provide a user-centric platform where individuals can view, manage and control their consent preferences and exercise their data rights, ensuring transparency and trust.
- Ensure Compliance with DPDP Act and Rules: Design the system to adhere strictly to the DPDP Act’s regulations, including purpose limitation, data minimization and secure processing of personal data.

3 Key Stakeholder and Responsibilities

The stakeholders include Data Principals, Data Fiduciaries, Data Processors and Consent Managements, each playing a critical role in ensuring compliance with the DPDP Act and Rules.

Key Words	Definition
Data Principal	An individual to whom the personal data relates. They have the right to give, manage and withdraw consent for data processing.
Data Fiduciary	Any person or entity that determines the purpose and means of

	processing personal data and is responsible for obtaining and managing consent in compliance with the DPDP Act.
Data Processor	A person or entity that processes personal data on behalf of a Data Fiduciary, following their instructions.
Data Protection Officer	DPO acts as the primary compliance authority to oversee adherence to the DPDP Act

4 Functional Requirements

4.1 Consent Management Lifecycle

The consent management lifecycle consist of

i. Consent collection.
ii. Consent validation.
iii. Consent Update.
iv. Consent Renewal.
v. Consent Withdrawal

4.1.1 Consent Collection

Primary Usage	To enable Data Fiduciaries to explicitly collect, purpose-specific and lawful consent from Data Principles for processing their personal data in compliance with the DPDP Act.

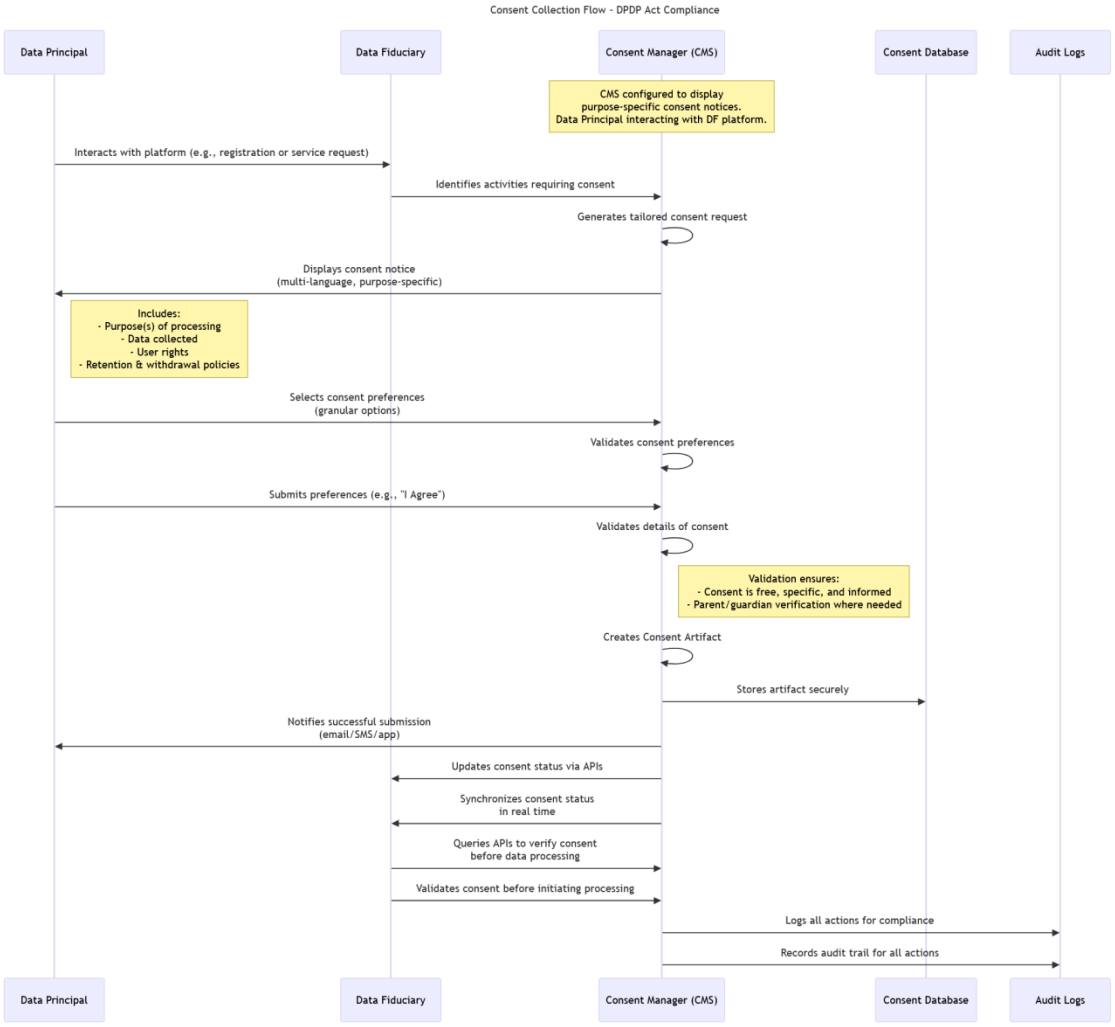
<table>
<tr><td>Actors</td><td>Data Principal: The individual providing or declining consent for their data to be processed.
Data Fiduciary (DF): Organization requesting and using the consent for defined purposes.
Consent Management (CMS): Manages the consent lifecycle, including collection, validation, updates, renewals and withdrawals.</td></tr>
<tr><td>Pre-Conditions</td><td>• The CMS is configured to display consent notices specific to these purposes.
• The Data Principal is interacting with a Data Fiduciary’s service or platform.</td></tr>
<tr><td>Trigger</td><td>The Data Principle initiates a service request (e.g., registration, service onboarding) that requires their personal data to be collected or processed.</td></tr>
<tr><td>Functional Requirements</td><td>User-Friendly Interface:
• The consent collection interface must be accessible and intuitive, ensuring users understand the terms of data processing.
• Support WCAG-compliant designs for users with disabilities.
Purpose-Specific Consent:
• Users must provide consent for each distinct purpose (e.g., account creation, marketing, analytics).
• The system must prevent "bundled consent" by separating optional purposes from mandatory ones.
Granular Consent: Allow users to provide or withhold consent for each purpose separately.
Explicit and Affirmative Action:
• Require users to take a clear, affirmative action to provide consent (e.g., clicking "I Agree," ticking a checkbox).
• Default settings must not pre-check consent options.
Multi-Language Support: Enable consent notices in English and languages as listed in the Eighth Schedule of the Constitution of India.
Consent Metadata Logging:
• User ID
• Timestamp
• Purpose ID(s)
• Consent status (granted or denied)
• Language preference</td></tr>
<tr><td>Workflow (Indicative)</td><td>
<table>
<tr><th>Step</th><th>Trigger/Action</th><th>Description</th></tr>
<tr><td>Initiation</td><td>Trigger: Data Principal interacts with the Data Fiduciary’s platform (e.g.,</td><td>The system identifies activities requiring consent (e.g., account creation, marketing).</td></tr>
</table>
</td></tr>
</table>

		registration or service request).	
		Action: CMS generates a tailored consent request for the specific purpose(s).	Purpose categories are mapped to consent requirements.
	Consent Notice Presentation	**Trigger**: User accesses a page, app or interface where personal data collection is requested.	Display a clear and concise consent notice as per DPDP Act, covering: • Purpose(s) of data collection and processing. • Data being collected. • User rights under the DPDP Act. • Data retention and withdrawal policies.
		Action: Notice is available in English and in the languages as listed in the Eighth Schedule of the Constitution of India.	
	Consent Options	**Trigger**: User is prompted to select consent preferences.	Provide explicit options (e.g., checkboxes or toggles) for granular consent for each purpose. Example: Separate checkboxes for marketing emails, analytics, or third-party sharing.
	Consent Submission	**Trigger**: User submits their preferences by interacting with the consent options.	User confirms consent by clicking a button (e.g., "I Agree" or "Submit Consent").
		Action: CMS validates the consent. Where applicable, Parent/guardian identity and certificates should	• Free, specific, informed, unambiguous and explicit and affirmatively expressed. • Limited to the stated purposes.

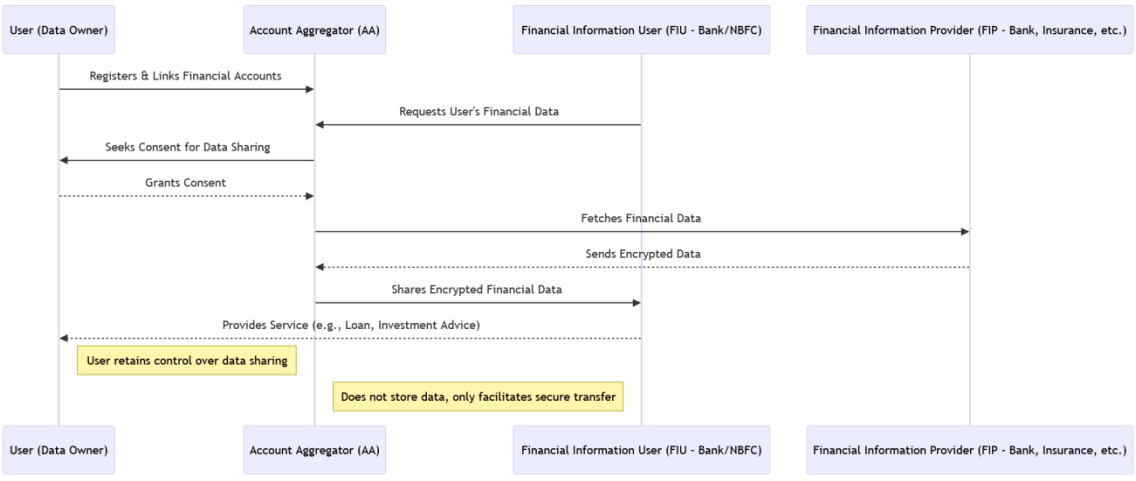
		be verified (through existing a/c or DigiLocker)	
	Consent Artifact Creation	**Trigger**: Consent submission is validated successfully.	• The CMS generates a Consent Artifact containing Purpose(s) of consent, Metadata (e.g., timestamp, user ID, session ID, consent method). • The Consent Artifact is securely stored in the Consent Database.
	Acknowledgment	**Trigger**: Consent is successfully recorded.	Notify the user of successful consent submission via email, SMS, or app notification.
	Real-Time Synchronization	**Trigger:** Consent artifact is stored.	• Consent status is synchronized across internal systems and third-party processors in real time. • Data Fiduciaries receive updates via APIs to validate user consent before data processing.
	Post-Submission Validation	**Trigger:** User data is processed based on consent.	Fiduciaries query CMS APIs to verify consent status before initiating processing workflows.
	Monitoring and Logging	**Trigger:** Consent collection is completed.	All actions are logged in an audit trail for regulatory compliance.
Assumptions	• The Data Fiduciary has accurately mapped all data collection activities to their respective purposes. • The DF is compliant with DPDP Act regulations, including multi-language support and accessibility standards. • The Data Principal has access to the consent interface (e.g., web or mobile app).		
Business Rule	• **Purpose-Specific Consent**: Consent must be collected for specific purposes, not as a blanket agreement. • **Explicit Action**: The Data Principal must take an affirmative action (e.g., clicking "I Agree") to provide consent. • **Revocability**: Consent must be revocable by the Data Principal at any time. • **Transparency**: The consent notice must include clear information about data use, retention, rights and grievance redressal mechanisms. • **Granular Consent**: The Data Principal must be able to consent or decline for each individual purpose independently.		

Indicative Flow

Use case 1:



Use Case 2:



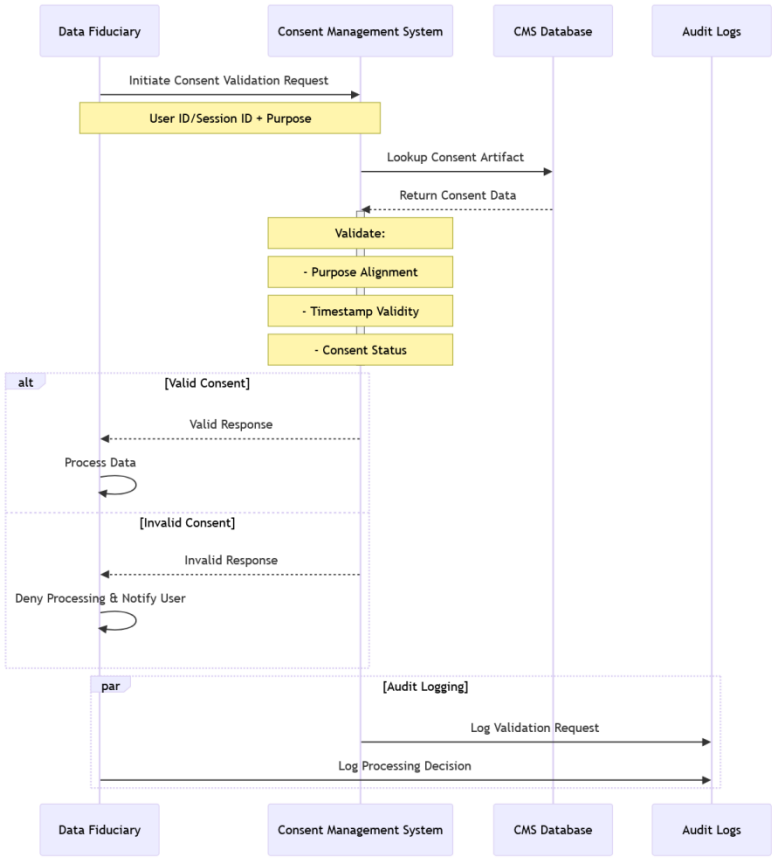
4.1.2 Consent Validation

<table>
<tr><td>Primary Usage</td><td>To validate whether the Data Principal has provided explicit and lawful consent for a specific purpose before the Data Fiduciary processes their personal data.</td></tr>
<tr><td>Actors</td><td>Data Principal: The user whose consent needs to be validated.
Data Fiduciary (DF): The organization that requests consent validation before processing data.
Consent Management System (CMS): The system responsible for managing and validating user consents.</td></tr>
<tr><td>Pre-Conditions</td><td>The Data Principal has provided consent, which is stored securely as a Consent Artifact.</td></tr>
<tr><td>Trigger</td><td>● A Data Fiduciary initiates a data processing activity (e.g., marketing, analytics, or service delivery) that requires user consent validation.
● A system event or API call from the Data Fiduciary requests confirmation of consent status.</td></tr>
<tr><td>Functional Requirements</td><td>Pre-Processing Check: Before initiating data processing, validate whether -
● The consent exists for the given User ID and Purpose ID.
● The consent is still active and not expired or withdrawn.
Metadata Validation: Verify the following metadata -
● User ID
● Purpose ID
● Timestamp of consent
● Status of consent (granted/withdrawn/expired)
Scope Validation:
● Ensure that the processing request does not exceed the purpose specified in the consent.
● Example: Data collected for "identity verification" cannot be used for "marketing" unless explicitly consented to.
Purpose-Specific Validation
● Match the requested processing activity with the purpose(s) consented to by the user.
● Reject requests that do not align with specific purposes.</td></tr>
<tr><td>Workflow (Indicative)</td><td>
<table>
<tr><th>Step</th><th>Actors</th><th>Description</th></tr>
<tr><td>Initiation of Validation Request</td><td>Data Fiduciary</td><td>A request for consent validation is triggered by the Data Fiduciary before initiating any data processing (e.g., marketing email, analytics).</td></tr>
</table>
</td></tr>
</table>

	API Request to CMS	Data Fiduciary	• The Data Fiduciary sends an API request to the CMS specifying: User ID or Session ID. • Purpose for which consent validation is required.
	Consent Lookup	CMS	The CMS searches its database for an active consent artifact corresponding to the specified user ID and purpose.
	Validation of Consent Artifact	CMS	Validate the following criteria: • Purpose alignment: Verify that consent is specific to the requested purpose. • Timestamp validity: Check if consent is still active or has expired. • Status: Ensure the consent has not been withdrawn.
	Validation Response	CMS Data Fiduciary	The CMS sends a real-time response back to the Data Fiduciary with one of the following outcomes: • Valid: Consent exists, is active and aligns with the requested purpose. • Invalid: No active consent exists, or the consent is withdrawn/expired.
	Consent-Based Processing	Data Fiduciary	• If consent is valid: Data Fiduciary proceeds with the requested data processing activity. • If consent is invalid: The processing request is denied and the user is notified.
	Audit Logging	CMS Data Fiduciary	All validation actions, whether successful or unsuccessful, are logged in the CM's immutable audit logs for regulatory compliance.
Assumptions	• Consent artifacts in the CMS are immutable and tamper-proof. • The Data Fiduciary has integrated their system with the CMS API for consent validation. • Consent validation is performed in real time to avoid delays in data processing workflows.		
Business Rule	• **Purpose-Specific Validation**: Consent must be validated for the exact purpose for which data is being processed. • **Timestamp Validation**: Consent must be checked for expiration or withdrawal before data processing. • **Data Minimization**: Consent validation ensures that only data for		

	which explicit consent is given is processed. ● **Auditable Results**: All consent validation actions must be logged in the CMS for compliance and reporting purposes. ● **Error Handling**: If valid consent does not exist, the CMS must return an error or deny the processing request and the user must be notified accordingly.

Indicative Flow:



4.1.3 Consent Update

Primary Usage	To enable Data Principals to modify their previously granted consent for specific purposes or activities while ensuring compliance with the DPDP Act.
Actors	**Data Principal**: The individual who updates their consent. **Data Fiduciary (DF)**: The entity requesting the updated consent. **Consent Management System (CMS):** Manages consent updates and tracks actions.
Pre-Conditions	● The Data Principal has previously provided consent for a specific purpose. ● The existing consent is valid. ● CMS maintains detailed consent artifacts, including metadata.

<table>
<tr><td>Trigger</td><td>

Data Principal logs into the CMS dashboard and selects update consent
The Data Fiduciary introduces a new processing purpose or modifies an existing one that requires user approval.

</td></tr>
<tr><td>Functional Requirements</td><td>
Notification of Consent Updates: Notify users when the scope or purpose of processing changes, or when additional purposes are added. Notifications must clearly explain -

The new purpose or scope.
How it affects their data processing.
The need for updated consent.

Granular Consent Updates: Allow users to update their consent for specific purposes while maintaining previously granted consents for others.

Simplified User Action: Ensure that updating consent is as simple and intuitive as the initial consent process.

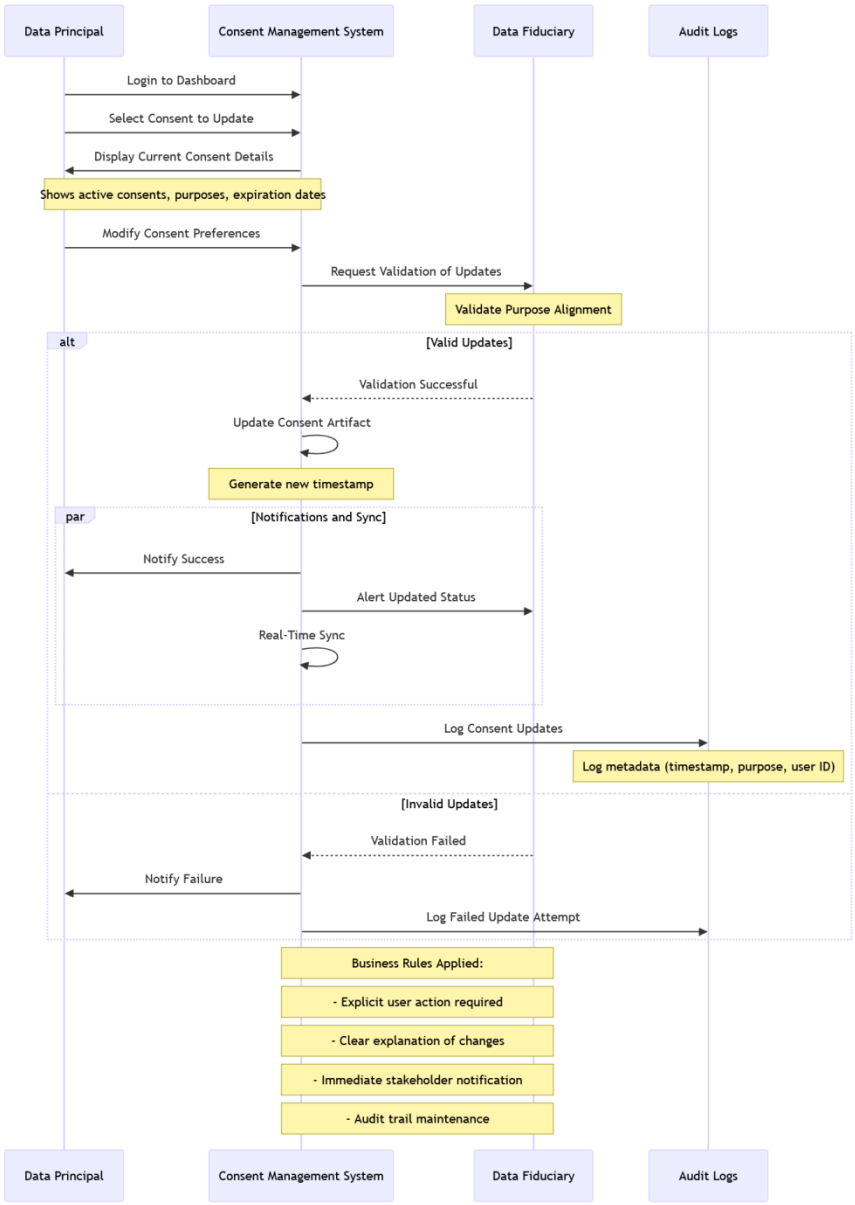
Metadata Logging: Record metadata for all updates, including

User ID
Timestamp
Updated purpose IDs
Status (e.g., active, pending)

</td></tr>
<tr><td>Workflow (Indicative)</td><td>
<table>
<tr><th>Description</th><th>Actors</th><th>Key Actions</th></tr>
<tr><td>Initiation of Consent Update</td><td>Data Principal</td><td>The user logs into the CMS dashboard and selects consent to update.</td></tr>
<tr><td>Display Current Consent Details</td><td>CMS</td><td>The CMS displays all active consents with their purposes, expiration dates and metadata.</td></tr>
<tr><td>User Modifies Consent</td><td>Data Principal</td><td>The user modifies preferences for specific purposes.</td></tr>
<tr><td>Validation of Changes</td><td>DF</td><td>DF validates the updates for Purpose alignment.</td></tr>
<tr><td>Consent Artifact Update</td><td>CMS</td><td>The CMS updates the consent artifact with new preferences and generates a timestamp.</td></tr>
<tr><td>Notification of Changes</td><td>CMS</td><td>• Notify the user of successful updates.
• Alert Data Fiduciaries of updated consent statuses.</td></tr>
<tr><td>Real-Time Sync with Data Fiduciaries</td><td>CMS</td><td>Sync updated consent data with all relevant systems, ensuring no processing occurs without updated consent.</td></tr>
</table>
</td></tr>
</table>

	Audit Logging	CMS	Log all changes in audit logs for compliance.
Assumptions	• DF is integrated with all systems that rely on the consent data. • The Data Principal receives timely notifications for consent updates. • The system supports granular consent, allowing the user to modify specific purposes independently.		
Business Rule	**Transparency**: Updated consent must include a clear explanation of the changes (e.g., new data purposes or retention policies). **User Action Required:** Consent cannot be assumed. The Data Principal must actively agree to the update. **Auditability**: All consent updates must be logged, including the metadata (e.g., timestamp, purpose, user ID). **Validity**: Updated consent must specify the duration for which it remains valid. **Notifications**: Notify all stakeholders (Data Fiduciaries and Data Processors) of updated consent status immediately.		

Indicative Flow:



4.1.4 Consent Renewal

Primary Usage	To enable Data Principals to renew their previously granted consent for specific purposes or activities while ensuring compliance with the DPDP Act.
Actors	**Data Principal**: The individual who renews their consent. **Data Fiduciary (DF)**: The entity requesting the renewed consent. **Consent Management System (CMS):** Manages and tracks renewal actions.
Pre-Conditions	• The Data Principal has previously provided consent for a specific purpose.

<table>
<tr><td></td><td>

The existing consent is expired or nearing expiration.
CMS maintains detailed consent artifacts, including metadata.

</td></tr>
<tr><td>Trigger</td><td>The consent is set to expire and the system notifies the Data Principal to renew their consent.</td></tr>
<tr><td>Functional Requirements</td><td>
Time-Limited Consents:

For consents with predefined expiration dates, provide renewal options prior to expiration.
Example: Notify the user 30 days before consent expiry and provide a seamless renewal process.

Simplified User Action: Ensure that renewing consent is as simple and intuitive as the initial consent process.
Metadata Logging: Record metadata for all renewals, including

User ID
Timestamp
Renewed purpose IDs
Status (e.g., active, pending)

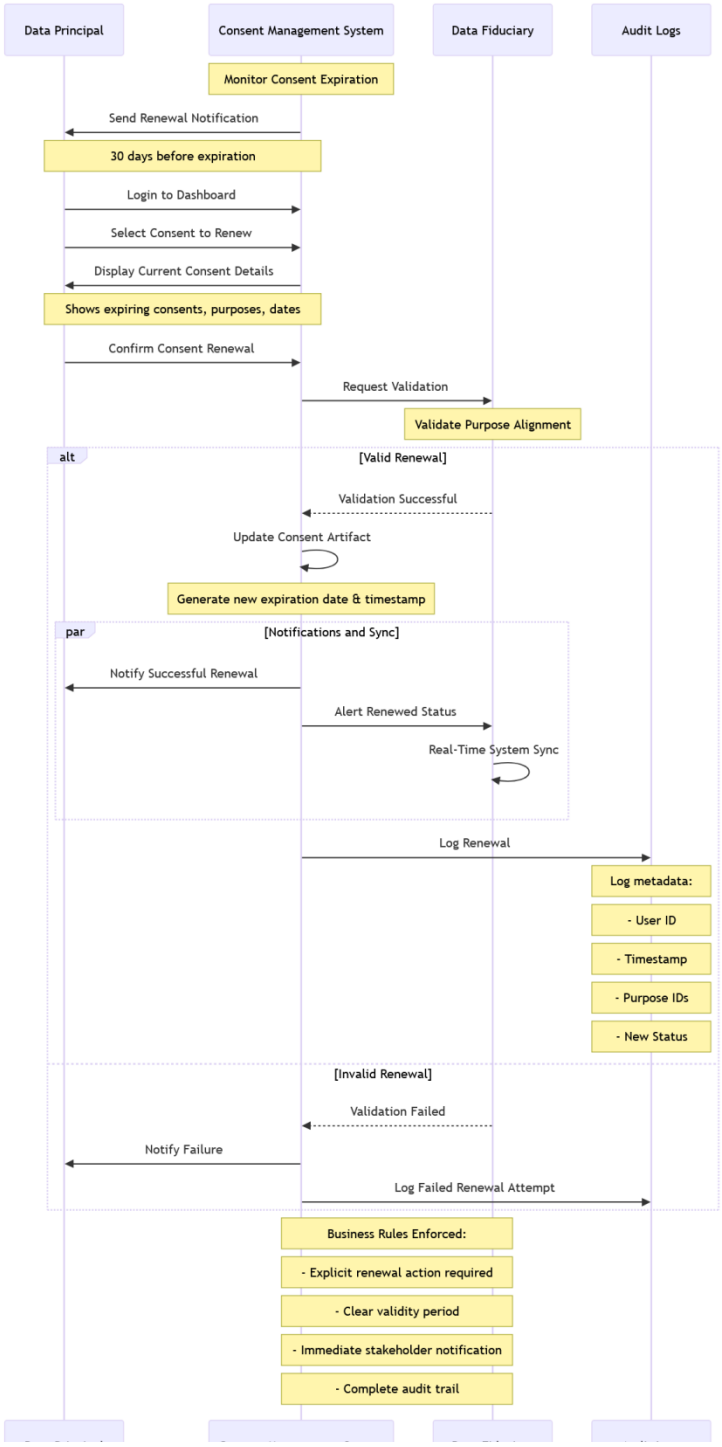
</td></tr>
<tr><td>Workflow (Indicative)</td><td>
<table>
<tr><th>Description</th><th>Actors</th><th>Key Actions</th></tr>
<tr><td>Initiation of Consent Renewal</td><td>Data Principal</td><td>The user logs into the CMS dashboard and selects consent to renew.</td></tr>
<tr><td>Display Current Consent Details</td><td>CMS</td><td>The CMS displays all active consents with their purposes, expiration dates and metadata.</td></tr>
<tr><td>User Renews Consent</td><td>Data Principal</td><td>The user confirms renewal for expiring consents.</td></tr>
<tr><td>Validation of Changes</td><td>DF</td><td>DF validates the updates for Purpose alignment.</td></tr>
<tr><td>Consent Artifact Update</td><td>CMS</td><td>The CMS updates the consent artifact with new preferences and generates a timestamp.</td></tr>
<tr><td>Notification of Changes</td><td>CMS</td><td>

Notify the user of successful renewals.
Alert Data Fiduciaries of updated consent statuses.

</td></tr>
<tr><td>Real-Time Sync with Data Fiduciaries</td><td>DF</td><td>Sync updated consent data with all relevant systems, ensuring no processing occurs without updated consent.</td></tr>
</table>
</td></tr>
</table>

	Audit Logging	CMS	Log all changes in audit logs for compliance.
Assumptions	• CMS is integrated with all systems that rely on the consent data. • The Data Principal receives timely notifications for consent renewal requirements. • The system supports granular consent, allowing the user to renew specific purposes independently.		
Business Rule	**Transparency**: Renewed consent must include a clear explanation of the changes (e.g., retention policies). **User Action Required**: Consent cannot be assumed. The Data Principal must actively agree to the renewal. **Auditability**: All consent renewals must be logged, including the metadata (e.g., timestamp, purpose, user ID). **Validity**: Renewed consent must specify the duration for which it remains valid. **Notifications**: Notify all stakeholders (Data Fiduciaries and Data Processors) of renewed consent status immediately.		

Indicative Flow:



4.1.5 Consent Withdrawal

Primary Usage	To allow Data Principals to withdraw previously provided consent for one or more specific purposes, ensuring immediate cessation of related data

<table>
<tr><td></td><td>processing.</td></tr>
<tr><td>Actors</td><td>Data Principal: The individual initiating consent withdrawal.

Data Fiduciary (DF): The organization receiving the withdrawal notification and stopping related data processing.

Consent Management System (CMS): Facilitates the withdrawal process and notifies stakeholders.</td></tr>
<tr><td>Pre-Conditions</td><td>● The Data Principal has previously provided consent for a specific purpose.
● The consent is currently valid (not expired or previously withdrawn).
● The CMS maintains a secure record of all consent artifacts.</td></tr>
<tr><td>Trigger</td><td>● The Data Principal initiates a withdrawal request via a user interface (e.g., dashboard, mobile app, or customer portal).
● A withdrawal request is received through an API from an integrated application.</td></tr>
<tr><td>Functional Requirements</td><td>Ease of Withdrawal:
- Users must be able to withdraw consent through User dashboard.
- Ensure the process is as simple as the original consent-giving mechanism

Real-Time Processing: Upon withdrawal -
● Stop all processing activities related to the withdrawn purpose.
● Update internal records to reflect the withdrawal status.
● Notify downstream systems and third-party processors to cease processing.

Confirmation to the User: Notify the user immediately upon successful withdrawal with:
● Confirmation message.
● Information on implications (e.g., loss of specific features or services).

Metadata Logging: Log withdrawal metadata, including:
● User ID
● Purpose ID
● Timestamp of withdrawal
● Status updates (e.g., confirmation of processing halt)

Processing Exceptions: Allow continued processing if required or authorized under law (e.g., compliance with regulatory mandates)</td></tr>
<tr><td>Workflow (Indicative)</td><td><table><tr><th>Description</th><th>Actors</th><th>Key Actions</th></tr></table></td></tr>
</table>

	Initiation of Withdrawal Request	Data Principal	User logs into a consent dashboard or portal (web/mobile) and selects the option to withdraw consent.
	Presentation of Current Consent Details	CMS	• Display a list of all active consents, grouped by purpose and date, for the user to review. • Include metadata such as the purpose, consent timestamp and associated services.
	Selection of Consent to Withdraw	Data Principal	The user selects the specific purpose(s) or activities for which they wish to revoke consent.
	Confirmation of Withdrawal Action	Data Principal	• Provide the user with a summary of the implications of withdrawing consent (e.g., loss of certain services or features). • The user confirms withdrawal by interacting with the interface (e.g., clicking "Withdraw Consent").
	Validation	CMS	Validate the withdrawal request to ensure: The selected purpose(s) have active consent.
	Consent Artifact Update	CMS	• Update the consent record to reflect the withdrawal. • Mark the associated Consent Artifact as "Withdrawn" with a timestamp and log the action in the audit trail.
	Notification to Data Fiduciaries and Processors	CMS	• Notify all linked Data Fiduciaries and third-party processors about the withdrawal request. • Include details of the affected purposes and associated user data.
	Immediate Cessation of Data Processing	Data Fiduciary	• Halt all processing activities related to the withdrawn consent. • Stop sharing, processing, or analysing any associated data.
	Acknowledgme	CMS	Send a notification (via email/SMS) to the

<table>
<tr><td></td><td><table>
<tr><td>nt to Data Principal</td><td></td><td>Data Principal confirming successful consent withdrawal.</td></tr>
<tr><td>Audit and Compliance Logging</td><td>CMS</td><td>• Record the withdrawal event, including metadata such as the timestamp, purpose and user ID, in an immutable audit log.
• Generate compliance reports if required.</td></tr>
</table></td></tr>
<tr><td>Assumptions</td><td>• The withdrawal process is simple, user-friendly and mirrors the ease of giving consent.
• Data Fiduciaries and third-party processors are configured to immediately cease processing activities upon withdrawal notification.
• The CMS is accessible to both Data Fiduciaries and Data Principals for real-time withdrawal updates.</td></tr>
<tr><td>Business Rule</td><td>Purpose-Specific Withdrawal: Data Principals must be able to withdraw consent for specific purposes without affecting others.

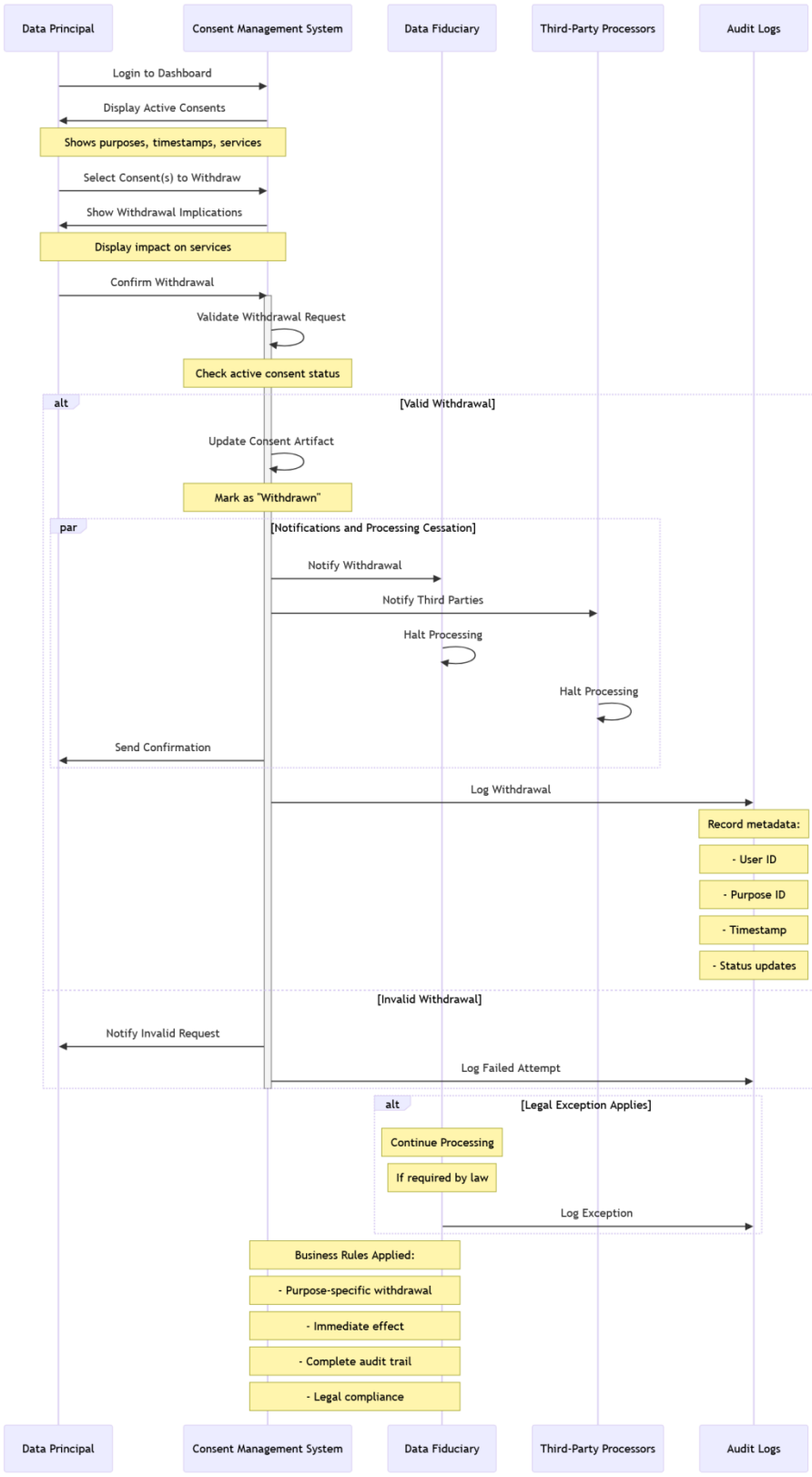
Immediate Effect: Withdrawal of consent must immediately halt all associated data processing activities.

Notifications: Both the Data Fiduciary and Data Principal must be notified of the withdrawal action.

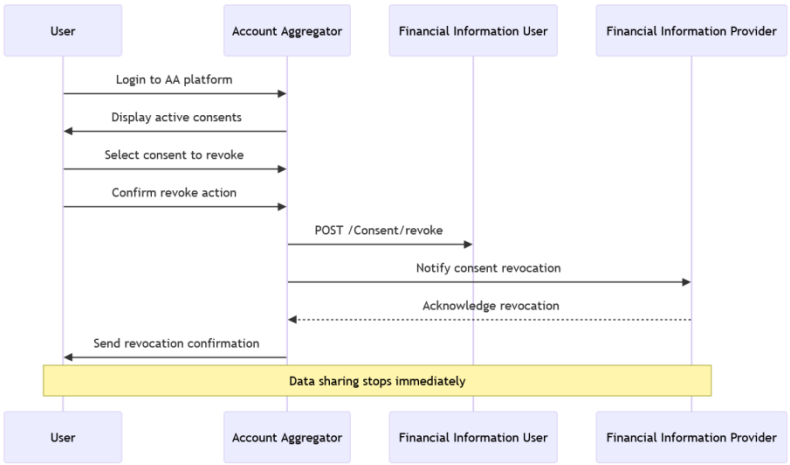
Auditability: The withdrawal request, metadata and response must be logged in an immutable format for compliance and future audits.
Legal Exceptions: Withdrawal does not apply where data processing is required by law or exempted under the DPDP Act.</td></tr>
</table>

Indicative Flow:

Use Case 1:


Data Principal
Consent Management System
Data Fiduciary
Third-Party Processors
Audit Logs
Login to Dashboard
Display Active Consents
Shows purposes, timestamps, services
Select Consent(s) to Withdraw
Show Withdrawal Implications
Display impact on services
Confirm Withdrawal
Validate Withdrawal Request
Check active consent status
alt
[Valid Withdrawal]
Update Consent Artifact
Mark as "Withdrawn"
par
[Notifications and Processing Cessation]
Notify Withdrawal
Notify Third Parties
Halt Processing
Halt Processing
Send Confirmation
Log Withdrawal
Record metadata:
- User ID
- Purpose ID
- Timestamp
- Status updates
[Invalid Withdrawal]
Notify Invalid Request
Log Failed Attempt
alt
[Legal Exception Applies]
Continue Processing
If required by law
Log Exception
Business Rules Applied:
- Purpose-specific withdrawal
- Immediate effect
- Complete audit trail
- Legal compliance
Data Principal
Consent Management System
Data Fiduciary
Third-Party Processors
Audit Logs

Use Case 2:



4.2 Cookie Consent

The purpose of cookie consent management is to ensure that users (Data Principals) are informed about cookies and tracking technologies used on websites and applications, providing them with the ability to grant, modify, or withdraw consent for their use.

Features

- Granular Consent Options: Allow users to consent to specific categories of cookies, such as essential, performance, analytics, and marketing cookies.
- Real-Time Updates: Enable users to modify or revoke cookie consent through a dedicated cookie preferences interface.
- Cookie Policy Display: Provide a clear and accessible cookie policy outlining cookie usage, purposes and data sharing practices.
- Multi-Language Support: Ensure cookie notices are available in languages, supporting inclusivity.
- Auto-Expiry: Set expiration periods for user preferences and cookies, complying with data retention policies.

Functional Requirements

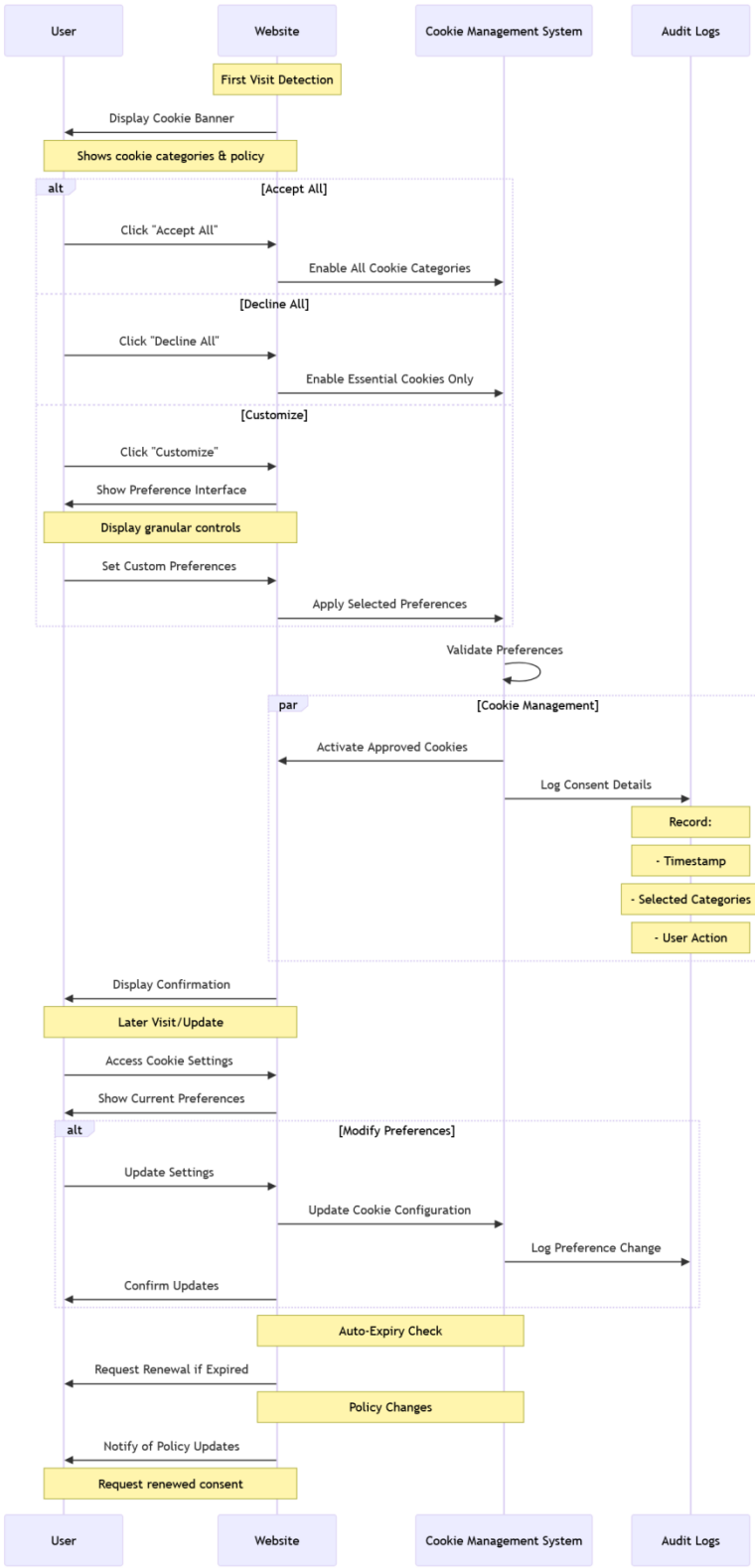
Requirement	Description
Cookie Notice Banner	Display a banner informing users of cookie usage when they first visit the website or app.
Granular Control Interface	Provide a user-friendly interface where users can customize their cookie preferences.
Consent Logging	Maintain detailed logs of cookie consents, including timestamps, consent categories and user actions.
Default Settings	Enable only essential cookies by default until explicit consent is obtained for others.

Requirement	Description
Notification of Changes	Notify users of changes to cookie policies and request renewed consent.

Workflow (Indicative)

- Cookie Banner Display: The website displays a cookie banner on the first user visit.
- User Interaction: The user selects cookie preferences (accept all, decline all, or customize).
- Consent Validation: The system validates the preferences and activates cookies accordingly.
- Consent Logging: The system logs the preferences with a timestamp for auditing.
- Preference Updates: Users can access the cookie preferences interface to modify or withdraw consent.

Indicative Flow:


User
Website
Cookie Management System
Audit Logs
First Visit Detection
Display Cookie Banner
Shows cookie categories & policy
alt
[Accept All]
Click "Accept All"
Enable All Cookie Categories
[Decline All]
Click "Decline All"
Enable Essential Cookies Only
[Customize]
Click "Customize"
Show Preference Interface
Display granular controls
Set Custom Preferences
Apply Selected Preferences
Validate Preferences
par
[Cookie Management]
Activate Approved Cookies
Log Consent Details
Record:
- Timestamp
- Selected Categories
- User Action
Display Confirmation
Later Visit/Update
Access Cookie Settings
Show Current Preferences
alt
[Modify Preferences]
Update Settings
Update Cookie Configuration
Log Preference Change
Confirm Updates
Auto-Expiry Check
Request Renewal if Expired
Policy Changes
Notify of Policy Updates
Request renewed consent
User
Website
Cookie Management System
Audit Logs

4.3 User Dashboard

4.3.1 View Consent History

The dashboard will allow users to view the history of all consent-related actions performed.

Field	Details
Purpose	Provide Data Principals with a detailed log of all consent-related activities including cookies, ensuring transparency and accountability.
Features	• List all active, expired and withdrawn consents. • Metadata display (e.g., timestamp, purpose, consent status). • Search and filter options for easier navigation.
Functional Requirements	• Consent Log Display: Show the complete consent history grouped by status (Active, Expired, Withdrawn). • Search & Filter: Enable users to search for consents by purpose, date or status. • Export Options: Allow users to download their consent history in a secure format (e.g., PDF, CSV).
Workflow	• User logs in to the dashboard. • Selects "View Consent History." • The system retrieves the consent history. • Displays categorized data with search and filter options.

4.3.2 Modify or Revoke Consent

Field	Details
Purpose	Empower Data Principals to modify or revoke their consent for specific purposes in real time including cookie consent.
Features	• Modify granular preferences for specific purposes. • Revoke consent with immediate effect. • Receive acknowledgment of actions.
Functional Requirements	• Granular Modification: Allow updates for individual purposes without affecting other consents. • Immediate Revocation: Halt data processing for revoked consents in real time.

	• Notifications: Inform the user and Data Fiduciaries of consent changes.
Workflow	• User accesses the dashboard and selects "Modify or Revoke Consent." • The system displays all active consents. • The user selects a purpose and updates or revokes consent. • The CMS validates the action and updates the consent artifact. • Notifications are sent to all stakeholders (user, Data Fiduciary). • The action is logged for auditing.

4.3.3 Raise Grievances or Data Requests

Field	Details
Purpose	To provide Data Principals with a simple and transparent mechanism to raise complaints regarding consent violations, misuse of personal data, or to request access, correction, or erasure of their data as per the DPDP Act.
Features	**Grievance Logging**: Allow users to submit complaints related to data handling or consent. **Data Requests**: Enable users to request data access, correction, or erasure. **Tracking System**: Provide users with real-time updates on the status of their grievances or requests. **Notification System**: Notify users about resolution status via email or SMS. **Escalation Mechanism**: Automatically escalate unresolved grievances to the designated officer or Data Protection Officer (DPO).
Functional Requirements	**Grievance Submission Interface**: Provide an easy-to-use form to log complaints. **Data Request Options**: Include predefined options (e.g., Access Data, Correct Data, Erase Data). **Reference Number Generation**: Generate a unique reference number for each grievance or request. **Status Updates**: Display the status of grievances (e.g., Submitted, In Progress, Resolved). **Escalation Workflow**: Automatically escalate unresolved complaints after a predefined time frame.

Workflow	**1**. **Initiation**: The user logs into the dashboard and selects the "Raise Grievances or Data Requests" option. **2**. **Submission**: The user completes the form with required details (e.g., complaint category, description, data request type). **3**. **Validation**: The CMS validates the submission for completeness and compliance with the DPDP Act. **4**. **Acknowledgment**: The system generates a unique reference number and notifies the user of successful submission. **5**. **Processing**: The CMS routes the request to the appropriate team (e.g., DPO or designated department). **6**. **Resolution and Updates**: The team resolves the issue and updates the status in the CMS, notifying the user at every step. **7**. **Escalation (if needed)**: If unresolved within the stipulated time, the request is escalated to a higher authority. **8**. **Closure**: Once resolved, the system marks the request as "Closed" and provides the user with a resolution summary.

4.4 Consent Notifications

The Consent Notifications Module ensures that all stakeholders—Data Principals, Data Fiduciaries and Data Processors—are promptly informed about consent-related activities. This module enhances transparency, operational efficiency and compliance by delivering real-time updates through multiple channels. Notifications are segmented into User Notifications and Fiduciary and Processor Alerts, each catering to specific stakeholders and actions.

4.4.1 User Notifications

Field	Details
Purpose	To keep Data Principals informed about their consent-related activities, such as updates, approvals, withdrawals, or renewals, ensuring transparency and trust.

Features	Notify users about: • Consent approval or rejection. • Consent withdrawal confirmations. • Renewal reminders for expiring consents. • Processing updates for data-related requests (e.g., erasure, correction). Multi-channel support for notifications via email, SMS, or in-app messages.
Functional Requirements	**Notification Triggers:** Automatically send notifications based on user actions or system events (e.g., consent expiration, withdrawal). **Customizable Templates:** Predefined notification templates for various scenarios. **Multi-Language Support:** Notifications in languages as listed in the Eighth Schedule of the Constitution of India. **Acknowledgment Mechanism:** Allow users to acknowledge receipt of notifications where necessary.
Workflow	**1. Trigger:** A consent-related action (e.g., withdrawal, renewal) is initiated by the user or system. **2. Notification Generation**: The CMS generates a notification based on predefined templates. **3. Delivery**: The notification is delivered to the user via their preferred communication channel (email, SMS, or in-app). **4. Acknowledgment (Optional):** The user acknowledges the notification and the system logs the acknowledgment.

4.4.2 Data Fiduciary and Processor Alerts

Field	Details
Purpose	To notify Data Fiduciaries and Processors of consent updates, withdrawals, or validation requests to ensure real-time compliance and operational continuity.

Features	1. Alerts for: • Consent withdrawal or expiration. • New or updated consents. • System-triggered compliance checks. 2. Support for secure API-based alerts for automated workflows. 3. Real-time updates to ensure immediate data processing adjustments.
Functional Requirements	**API Integration:** Alert Data Fiduciaries and Processors through secure APIs (e.g., /api/alerts/notify). **Event-Based Triggers:** Automate alerts for specific consent-related events (e.g., a user's consent withdrawal). **Audit Logging:** Record all alerts in the log for compliance and future reference. **Escalation Workflow:** Escalate unacknowledged or unprocessed alerts within a predefined time frame.
Workflow	**1. Trigger:** Consent change (e.g., withdrawal, update) is recorded in the CMS. **2. Alert Generation:** CMS generates an alert for the relevant Data Fiduciary or Processor. **3. Delivery:** The alert is delivered via API or email with actionable details (e.g., "Stop processing data for User ID X"). **4. Action Confirmation:** Fiduciaries or Processors confirm that they have acted on the alert (e.g., halted data processing). **5. Escalation (Optional):** Unaddressed alerts are escalated to higher authorities or the DPO.

4.5 Grievance Redressal Mechanism

The Grievance Redressal Mechanism ensures that Data Principals can raise complaints or grievances related to data processing, privacy violations, or consent management issues. It facilitates efficient complaint resolution and compliance with the grievance provisions of the DPDP Act.

4.5.1 Complaint Logging

Field	Details
Purpose	To provide Data Principals with a platform to submit complaints related to data misuse, consent violations, or grievances about data handling practices.

Features	**Simplified Complaint Form**: User-friendly interface to log complaints with predefined categories. **Complaint Categorization**: Automatically categorize complaints (e.g., consent violation, data breach, processing errors). **Reference Number Generation:** Assign a unique reference ID for each complaint for tracking purposes. **Acknowledgment Notifications:** Send confirmation of complaint receipt to the user.
Functional Requirements	**Categorization System:** Predefine complaint categories for streamlined processing. **Multi-Language Support:** Allow users to submit complaints in regional languages. **Metadata Logging:** Log complaint details such as user ID, timestamp, category and description. **Secure Submission:** Encrypt all complaint submissions using TLS 1.3 for secure transmission. **Integration with CMS:** Link complaint details with consent records for context.
Workflow	**1. Initiation:** The Data Principal logs into the system and navigates to the complaint section. **2. Form Completion:** The user fills out the complaint form, providing details such as category, description and supporting evidence (if applicable). **3. Submission Validation:** The system validates the form for completeness and compliance. **4. Acknowledgment:** A unique reference ID is generated and the user receives a confirmation notification. **5. Routing:** The complaint is routed to the appropriate department or team for resolution.

4.5.2 Resolution Tracking

Field	Details

Purpose	To provide Data Principals with real-time updates on the status of their complaints and ensure timely resolution of grievances.
Features	**Complaint Status Dashboard:** Display real-time status updates (e.g., Submitted, In Progress, Resolved). **Escalation Mechanism:** Automatically escalate unresolved complaints after a predefined time frame. **User Notifications:** Notify users about status changes and resolution outcomes. **Action Logs:** Maintain detailed logs of actions taken during the resolution process. **Feedback Collection:** Allow users to provide feedback on the resolution process.
Functional Requirements	**Real-Time Updates:** Enable dynamic status updates visible to users. **Escalation Triggers**: Set time-based escalation rules for unresolved complaints. **Audit Logging:** Record every action taken for complaint resolution in an immutable format. **Notification System**: Send automatic updates to users via email or SMS. **Resolution Workflows**: Predefine workflows for different complaint categories to standardize processing.
Workflow	**1. Status Update:** The complaint's status is updated as it progresses through the resolution stages. **2. Notifications:** The user receives status updates at each significant stage (e.g., Assigned, Resolved). **3. Escalation:** If the complaint remains unresolved for a predefined time, it is escalated to a senior authority or the Data Protection Officer (DPO). **4. Resolution Closure:** Once resolved, the system updates the status to "Closed" and sends a resolution summary to the user. **5. Feedback Collection:** Users can submit feedback on the resolution process.

4.6 System Administration

The System Administration Module provides administrative capabilities to ensure secure and efficient operations of the Consent Management System (CMS). It includes managing user roles, configuring policies and maintaining compliance standards. Key sub-modules include User Role Management and Data Retention Policy Configuration.

4.6.1 User Role Management

Field	Details
Purpose	To define and manage access controls within the CMS, ensuring only authorized personnel can perform specific actions based on their roles.
Features	**Role-Based Access Control (RBAC):** Assign permissions based on predefined roles (e.g., Administrator, Auditor, Data Protection Officer). **Custom Role Creation:** Allow customization of roles to match organizational needs. **Permission Hierarchy:** Enable multi-level access controls to segregate responsibilities. **Audit Trail Integration:** Maintain logs of role assignments and changes.
Functional Requirements	**Role Definition:** Predefine roles such as Admin, DPO, Auditor and Operator with their respective permissions. **Access Revocation:** Allow real-time removal of user roles in case of misuse or unauthorized activities. **Authentication Integration:** Support multi-factor authentication (MFA) and single sign-on (SSO) for admin accounts. **Role Audits:** Provide audit reports of user access and role modifications.
Workflow	**1. Role Assignment:** Admin assigns roles to users based on their responsibilities. **2. Permission Validation:** System enforces access permissions based on the assigned role. **3. Monitoring:** The system tracks all user activities and logs any role changes. **4. Revocation (if required):** Admin revokes or modifies roles in real time as necessary.

4.6.2 Data Retention Policy Configuration

Field	Details
Purpose	To configure data retention policies to comply with the DPDP Act, ensuring that personal data and consent records are retained or deleted based on predefined schedules.
Features	• **Retention Schedules**: Define data retention periods for personal data and consent artifacts. • **Automated Deletion**: Schedule automatic purging of expired records. • **Exemption Handling**: Configure exceptions for data retained under legal or regulatory requirements. • **Notifications**: Notify administrators before critical data is deleted.
Functional Requirements	• **Policy Definition**: Allow administrators to create, modify and apply retention policies to specific data categories. • **Compliance Validation**: Ensure that retention periods adhere to regulatory requirements. • **Data Purging**: Implement secure deletion protocols (e.g., cryptographic erasure) for expired data. • **Audit Logging**: Maintain a record of all data retention and deletion activities.
Workflow	1. **Policy Creation**: Admin defines data retention policies, specifying retention periods for different data categories. 2. **Policy Enforcement**: CMS enforces policies by monitoring data age and triggering deletion workflows for expired records. 3. **Exception Handling**: System identifies records exempted from deletion due to legal requirements. 4. **Audit Trail**: All retention and deletion activities are logged for compliance purposes.

4.7 Logging

Logging ensures that all consent-related activities within the Consent Management System (CMS) are documented in a transparent, secure and tamper-proof manner. This provides an immutable trail for compliance verification, dispute resolution and regulatory audits as mandated by the DPDP Act.

- **Comprehensive Logging:** Record every consent action, including:
  - Consent grant, update and withdrawal.
  - Metadata such as User ID, Purpose ID, timestamps and consent status.
  - Notifications sent to Data Fiduciaries and acknowledgment receipts.

- **Audit Readiness:**
  - Maintain audit logs in a structured format for easy retrieval and reporting.
  - Ensure logs are compliant with regulatory requirements for data retention and security.
- **Access Control:** Restrict access to audit logs using Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA).

4.7.1 Audit Logs

Immutable audit logs are a cornerstone of a secure and transparent Consent Management System (CMS). They ensure that every consent-related action is recorded in a tamper-proof manner, providing an auditable history of all interactions for compliance with the DPDP Act. Immutable logs offer organizations the ability to demonstrate accountability and resolve disputes efficiently.

Metadata for Audit Logs

Each audit log entry must contain the following metadata:

Field	Description
Log ID	Unique identifier for the audit log entry.
User ID	Unique identifier for the Data Principal.
Purpose ID	Identifier for the specific purpose of the consent action.
Action Type	Action performed (grant, withdraw, update, validate, or notification).
Timestamp	Precise date and time of the action.
Consent Status	Status of the consent (e.g., active, withdrawn, expired).
Initiator	The entity that triggered the action (e.g., user, system, Data Fiduciary).
Source IP	IP address of the device initiating the action.
Audit Hash	A cryptographic hash of the log entry to ensure tamper detection.