# Lab Exercise on DPDP Rules 2025

## Exercise 1: Understanding Personal Data Classification

1. Personal Data: Any data that can directly or indirectly identify an individual (e.g., name, email).

2. Sensitive Personal Data: Data that requires higher protection due to its nature (e.g., Aadhaar number, bank details).

3. Non-Personal Data: Data that does not relate to an identified individual (e.g., anonymized data, aggregate statistics).

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Type** | **Example Value** | **Classification** | **Sensitivity Level** |
| **Name** | Raj, Anita | Personal | Low |
| **Email** | [raj@email.com](mailto:raj@email.com), | Personal | Medium |
| **Aadhaar No.** | 1234-5678-9012 | Sensitive Personal | High (critical) |
| **Bank Account** | 1234567890 | Sensitive Personal | High (critical) |
| **Website Cookies** | Yes | Non-Personal | Low |
| **Purchase History** | Bought Laptop, Clicked on Ads | Personal | Medium |

## Exercise 2: Drafting a Data Consent Request

We respect your privacy. To provide you with personalized offers and a better experience, we request your consent to collect and process the following information:

✅ Email – To send you exclusive offers & updates

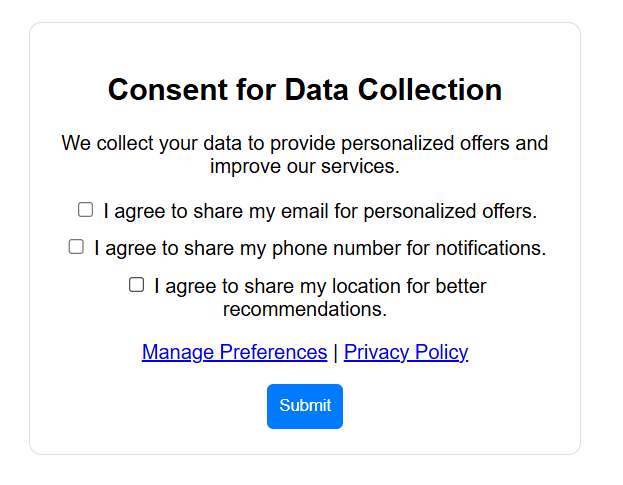
✅ Phone Number – For customer support & order updates

✅ Location – To show relevant deals & recommendations

By clicking “I Agree,” you consent to the collection and processing of this data under our Privacy Policy.

[✅] I Agree (You can withdraw your consent anytime)

[❌] No, I do not consent



## Exercise 3: Rights of Data Principals – Handling a Data Request

Subject: Acknowledgment of Your Data Deletion Request

Dear [User’s Name],

We have received your request to delete your personal data from our records. As per the DPDP Rules 2025, we will process your request within 30 days.

However, certain legal obligations (e.g., fraud prevention, regulatory compliance) may require us to retain some data. If your request qualifies for complete deletion, we will notify you once completed.

If you have any further questions or would like to withdraw your request, please contact us at [Support Email].

Best regards,  
[Your Name]  
Privacy Compliance Team, [Company Name]

## Exercise 4: Assessing Data Fiduciary Compliance

Company Assessment:

• The mobile app collects user data without explicit consent → Violation of DPDP Rules (Consent Requirement)

• It shares data with third parties without informing users → Violation of Data Sharing Norms

• It does not allow data deletion requests → Violation of User Rights (Right to Erasure)

Recommendations:

✔ Implement a clear and explicit consent mechanism.

✔ Notify users before sharing their data and offer an opt-out.

✔ Provide a data deletion request option in the app settings.

## Exercise 5: Simulating a Data Breach Response Plan

**Incident Response Plan (DPDP-Compliant)**

1. Immediate Actions:

🔹 Identify & contain the breach to prevent further damage.

🔹 Assess the impact (number of users affected, data compromised).

2. Notifying Affected Users:

📩 Send email/SMS alerts to users informing them about the breach, potential risks, and recommended actions (e.g., changing passwords).

3. Reporting to Authorities:

📝 Notify the Data Protection Board within 72 hours, as per DPDP guidelines.

4. Corrective Measures:

✅ Conduct a security audit to prevent future breaches.

✅ Strengthen encryption & access controls.