Data Protection Policy and Procedure

Khordha Central Co-Operative Bank Ltd.

NEW DCCB BUILDING, BANK SQUARE, KHORDHA

NEAR KHORDHA TOWN HALL, PIN -752055

Introduction:

1. Purpose.....
2. Scope of the Policy.....
3. Legal and Regulatory Framework.....
4. Data Protection Principles...
5. Data Processing Activities and Data Subject Rights.....
6. Data Security Measures.....
7. Data Sharing and Third Party Transfers....
8. Data Retention and Disposal.....
9. Monitoring and Auditing.....
10. Reporting and Compliance Monitoring.....

1. Purpose and Objectives

The objective of this policy is to ensure that Sub AUA/Sub KUA comply with data protection laws and regulations that govern the handling, processing, and storage of personal data, particularly in relation to the Aadhaar Act, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023 (once enacted). This policy aims to establish clear guidelines for:

- Ensuring compliance with applicable data protection laws and regulations.
- Protecting personal data from unauthorized access, misuse, alteration, or loss.
- Safeguarding the privacy rights of individuals whose data is processed.
- Establishing a framework for secure data handling, breach notification, and incident management.

2. Scope of the Policy

This policy applies to all data-related activities carried out by Sub AUA/Sub KUA, including:

- Collection, processing, storage, and transmission of personal data.
- Interactions with third-party vendors and contractors who may have access to personal data.
- Employees, contractors, and other personnel who handle data as part of their duties.

It applies to all types of personal data collected and processed, including data related to Aadhaar, KYC (Know Your Customer), and any other personal or sensitive data under applicable laws.

3. Legal and Regulatory Framework

Sub AUA/Sub KUA must comply with the following legal and regulatory frameworks:

- **Aadhaar Act, 2016** and UIDAI Regulations:
  - Ensure that Aadhaar data is collected, processed, and stored in compliance with UIDAI guidelines and permissions under the Aadhaar Act.
  - Use Aadhaar data strictly for authorized purposes such as identity verification and KYC, in line with the law.
  - Secure Aadhaar data from unauthorized access, alteration, or misuse by implementing proper access control mechanisms and encryption.
- **Information Technology Act, 2000 (IT Act)**:

- The IT Act mandates the implementation of reasonable security practices and procedures. Sub AUA/Sub KUA must adopt these practices to protect electronic data from misuse, loss, unauthorized access, or alteration.
- Ensure that data privacy and confidentiality are maintained throughout the lifecycle of personal data.

- **Sensitive Personal Data or Information (SPDI) Rules, 2011:**
  - Until the DPDP Act is in force, Sub AUA/Sub KUA must comply with the SPDI Rules under the IT Act, which require:
    - Consent for the collection of sensitive personal data.
    - Secure storage of sensitive data and restricting access to only authorized personnel.
    - Prompt notification in case of data breaches involving SPDI.

- **Digital Personal Data Protection Act, 2023 (DPDP Act)** (Once Enacted):
  - Upon the enactment of the DPDP Act, Sub AUA/Sub KUA must comply with the provisions for data processing, security practices, and data subject rights defined under the Act.
  - Implement provisions of data localization, data minimization, and data subject consent to ensure compliance with the DPDP Act.
  - Address data subject rights such as the right to be forgotten, right to data portability, and the right to rectification and erasure of personal data.

4. Data Protection Principles

To ensure compliance with data protection laws, Sub AUA/Sub KUA must adhere to the following principles:

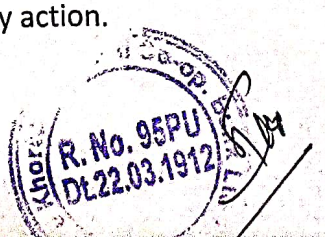
1. **Lawful, Fair, and Transparent Processing:**
   - Personal data must be processed in a lawful, fair, and transparent manner. Data subjects must be informed about the purpose and use of their data at the time of collection.
2. **Purpose Limitation:**
   - Personal data shall be collected only for specific, legitimate purposes and shall not be processed for incompatible purposes.
3. **Data Minimization:**
   - Only the minimum necessary personal data should be collected and processed to fulfill the identified purpose.
4. **Accuracy:**
   - Personal data should be accurate and kept up to date. Reasonable steps must be taken to ensure data accuracy, particularly when processing sensitive or critical information.

5. **Storage Limitation:**
    - Personal data should be retained only for as long as necessary to fulfill the purpose for which it was collected. Data must be securely deleted or anonymized when no longer needed.
6. **Security:**
    - Appropriate security measures should be implemented to protect personal data from unauthorized access, alteration, or disclosure, including physical, administrative, and technical safeguards (e.g., encryption, firewalls, access control).
7. **Accountability:**
    - Sub AUA/Sub KUA will ensure compliance with data protection principles and will be accountable for data processing activities, ensuring that these activities align with the legal and regulatory requirements.

5. Data Processing Activities and Data Subject Rights

Sub AUA/Sub KUA will follow the principles of privacy by design and by default when processing personal data. The rights of data subjects are paramount, and Sub AUA/Sub KUA shall take necessary steps to respect these rights:

1. **Data Subject Consent:**
    - Sub AUA/Sub KUA must obtain informed and explicit consent from individuals before collecting their personal data. Consent must be freely given, specific, informed, and unambiguous.
2. **Access and Rectification:**
    - Data subjects have the right to access their personal data. Sub AUA/Sub KUA shall ensure that individuals can access and, where necessary, correct any inaccurate or incomplete personal data.
3. **Right to Erasure/Deletion (Right to be Forgotten):**
    - In certain circumstances, individuals may request that their personal data be erased. Sub AUA/Sub KUA must establish procedures to honor such requests in accordance with applicable data protection laws.
4. **Data Portability:**
    - Data subjects may request the transfer of their personal data to another service provider. Sub AUA/Sub KUA shall ensure data is provided in a machine-readable format for portability.
5. **Data Subject Objection:**
    - Individuals may object to the processing of their personal data in certain circumstances (e.g., processing for direct marketing purposes). Sub AUA/Sub KUA must respect these objections and take necessary action.
    -



6. Data Security Measures

To ensure the security and integrity of personal data, Sub AUA/Sub KUA will implement the following measures:

1. **Access Controls:**
    - Implement role-based access controls to ensure that only authorized personnel have access to personal data based on their job responsibilities.
2. **Data Encryption:**
    - Sensitive personal data shall be encrypted both in transit and at rest to prevent unauthorized access during storage or transmission.
3. **Secure Storage:**
    - Personal data shall be stored in a secure manner, and any physical or electronic storage systems must be protected from unauthorized access or physical harm.
4. **Incident Response and Breach Management:**
    - Establish a data breach response plan to quickly detect, respond to, and mitigate any data breach incidents. Data breaches must be reported to the Data Protection Authority and affected individuals as required by applicable laws.
5. **Employee Training:**
    - All personnel handling personal data will undergo regular training on data protection laws, organizational policies, and security measures to reduce the risk of human error or negligence.

7. Data Sharing and Third-Party Transfers

Sub AUA/Sub KUA will not share personal data with third parties unless required for lawful purposes or necessary for the fulfillment of its obligations. When sharing data with third parties:

- Ensure that third parties have appropriate data protection measures in place.
- Enter into contractual agreements with third parties to ensure that data protection requirements are met.
- Provide transparent information to data subjects regarding any third-party data sharing, in compliance with the law.

8. Data Retention and Disposal

Personal data shall be retained only for as long as necessary for the purposes for which it was collected. Upon the expiration of the retention period or the completion of the processing purpose, personal data must be securely disposed of by:

- Securely deleting data stored electronically.
- Shredding physical records containing personal data.

9. Monitoring and Auditing

Sub AUA/Sub KUA will conduct regular audits and assessments to ensure compliance with this policy. Audits will review:

- Data protection practices.
- Security measures and controls.
- Incident response effectiveness.
- Training effectiveness.

10. Reporting and Compliance Monitoring

Sub AUA/Sub KUA will designate a Data Protection Officer (DPO) who will be responsible for:

- Overseeing the implementation of data protection practices.
- Monitoring compliance with this policy.
- Acting as the point of contact for any data protection-related inquiries.
- Reporting to senior management on data protection matters.

Conclusion

This Data Protection Policy reflects Sub AUA/Sub KUA's commitment to safeguarding personal data, protecting privacy rights, and ensuring compliance with relevant legal requirements. Sub AUA/Sub KUA will regularly review this policy to align with any changes in applicable laws, regulations, or industry best practices. Any updates to the policy will be communicated to all relevant stakeholders.