# DATA PROTECTION CHECKLIST

## Compliance Guide for East African Organizations

**RBC ENTERPRISE LIMITED**

## CONTENTS

## REGULATORY FRAMEWORK

### Kenya Data Protection Act, 2019

□ Registration with the Office of the Data Protection Commissioner
□ Implementation of all required data subject rights
□ Appointment of Data Protection Officer if applicable
□ Compliance with cross-border data transfer restrictions
□ Implementation of appropriate security measures
□ Mandatory breach notification procedures

### Tanzania Electronic and Postal Communications Act

□ Registration of all databases containing personal information
□ Compliance with data retention limitations
□ Implementation of technical security measures
□ Registration with the Tanzania Communications Regulatory Authority
□ Consent requirements for processing personal information
□ Restrictions on direct marketing communications

### Rwanda Law on Protection of Personal Data and Privacy

□ Registration with the National Cyber Security Authority
□ Implementation of privacy by design principles
□ Compliance with data minimization requirements
□ Documentation of all processing activities
□ Implementation of access control mechanisms
□ Mandatory impact assessments for high-risk processing

### Uganda Data Protection and Privacy Act, 2019

□ Registration with the Personal Data Protection Office
□ Implementation of data collection limitations
□ Compliance with purpose specification requirements

□ Implementation of accountability measures
□ Security safeguards for all personal data
□ Restrictions on automated decision making

### EAC Framework for Cybersecurity

□ Alignment with EAC harmonized approaches to cybersecurity
□ Implementation of cross-border data protection mechanisms
□ Compliance with regional incident response requirements
□ Participation in information sharing initiatives
□ Implementation of critical infrastructure protection measures
□ Alignment with EAC cybersecurity capability maturity model

## DATA PROTECTION OFFICER REQUIREMENTS

### □ Appointed Data Protection Officer

○ Position formally established in organizational structure
○ Reporting line directly to executive leadership established
○ Independence from IT and business operations ensured
○ Adequate resources and budget allocated
○ Authority to intervene in data processing activities granted

### □ DPO job description documented

○ Responsibilities clearly defined
○ Required qualifications and expertise specified
○ Relationship with other departments articulated
○ Decision-making authority documented
○ Performance evaluation criteria established

### □ DPO contact information published

○ Contact details accessible on company website
○ Information included in privacy notices
○ Internal staff directory updated
○ Registered with relevant regulatory authorities
○ Alternative contact methods provided

### □ DPO reporting structure established

○ Direct reporting line to board or executive leadership
○ Regular reporting schedule implemented
○ Escalation paths for critical issues defined
○ Independence from operational decisions ensured
○ Authority to engage external expertise when needed

## DATA INVENTORY AND CLASSIFICATION

□ **Personal data inventory completed**

- ○ All databases and systems containing personal data identified
- ○ Types of personal data collected documented
- ○ Purpose of collection for each data type defined
- ○ Legal basis for processing each data type established
- ○ Data flows between systems mapped

□ **Data classification scheme implemented**

- ○ Classification levels defined (e.g., public, internal, confidential, restricted)
- ○ Classification criteria established
- ○ Data labeling procedure implemented
- ○ Handling requirements for each classification documented
- ○ Staff trained on classification procedures

□ **Special categories of data identified**

- ○ Health data identified and specially protected
- ○ Biometric data identified and specially protected
- ○ Financial data identified and specially protected
- ○ Children's data identified and specially protected
- ○ Additional security controls implemented for special categories

□ **Data flows documented**

- ○ Internal data transfers mapped
- ○ External data transfers identified
- ○ Cross-border transfers documented
- ○ Data sharing agreements reviewed
- ○ Transfer mechanisms assessed for compliance

□ **Data retention periods established**

- ○ Retention schedule developed
- ○ Legal requirements for retention documented
- ○ Automatic deletion/anonymization procedures implemented
- ○ Exceptions handling process established
- ○ Regular retention compliance audits scheduled

## CONSENT MANAGEMENT

□ **Consent collection mechanisms in place**

- ○ Clear affirmative action required (no pre-ticked boxes)
- ○ Granular options for different processing activities
- ○ Age verification for children's consent
- ○ Consent language clear and understandable
- ○ Mechanism records time, date and method of consent

### □ Privacy notices reviewed and updated

- ○ Identity and contact details of data controller provided
- ○ Purposes of processing clearly explained
- ○ Legal basis for processing specified
- ○ Recipients or categories of recipients identified
- ○ Retention periods stated
- ○ Data subject rights explained
- ○ Cross-border transfer information included
- ○ Use of automated decision-making disclosed

### □ Opt-in/opt-out mechanisms implemented

- ○ Separate consent for different purposes
- ○ No bundling of consent with other terms
- ○ Specific consent for marketing communications
- ○ Ability to opt out without detriment
- ○ Preference center for managing consent choices

### □ Consent withdrawal process established

- ○ Simple withdrawal process implemented
- ○ Information on withdrawal process provided
- ○ Immediate processing of withdrawal requests
- ○ System updates to reflect withdrawal
- ○ Confirmation of withdrawal sent to data subject

### □ Records of consent maintained

- ○ What the data subject consented to documented
- ○ When consent was provided recorded
- ○ How consent was provided recorded
- ○ When/if consent was withdrawn documented
- ○ Regular review of consent records scheduled

## DATA SUBJECT RIGHTS

### □ Process for handling access requests

- ○ Request intake procedure established
- ○ Identity verification process implemented
- ○ Response timeline tracking system in place
- ○ Standard response templates created
- ○ Staff trained on handling requests

### □ Procedure for data rectification

- ○ Request validation process established
- ○ System update procedure documented
- ○ Notification to third parties receiving data

○ Confirmation to data subject after completion
○ Records of changes maintained

### ▫ Method for data erasure ("right to be forgotten")

○ Evaluation criteria for erasure requests established
○ Process for identifying all relevant data defined
○ Technical method for complete erasure implemented
○ Procedure for notifying third parties documented
○ Exceptions handling for legal retention requirements

### ▫ Process for data portability

○ Established format for portable data
○ Secure transmission method implemented
○ Procedure for direct transfer to other controllers
○ Scope of portable data defined
○ Validation of output data quality

### ▫ Objection to processing procedures

○ Assessment criteria for objections defined
○ Process for implementing processing restrictions
○ Method for demonstrating compelling legitimate grounds
○ System for tracking and implementing objections
○ Regular review of objection decisions

## SECURITY MEASURES

### ▫ Encryption for data at rest and in transit

○ Strong encryption algorithms implemented
○ Encryption key management procedure established
○ Transport Layer Security (TLS) for all web applications
○ Mobile device encryption enforced
○ Secure email transmission for sensitive information

### ▫ Access controls implemented

○ Role-based access control model implemented
○ Principle of least privilege applied
○ Regular access reviews conducted
○ Strong authentication mechanisms in place
○ Privileged account management implemented

### ▫ Regular security assessments

○ Vulnerability scanning program established
○ Annual penetration testing scheduled
○ Security control effectiveness reviews

○ Compliance assessment with security frameworks
○ Third-party security assessments for critical systems

### □ Incident response plan

○ Incident classification and escalation procedures defined
○ Response team roles and responsibilities assigned
○ Communication protocols established
○ Recovery procedures documented
○ Regular testing and simulation exercises conducted

### □ Data breach notification procedure

○ Breach detection mechanisms implemented
○ Assessment process for breach severity and impact
○ Template notifications prepared
○ Communication channels established
○ Documentation procedures for breach response

## THIRD-PARTY MANAGEMENT

### □ Due diligence process for vendors

○ Security assessment questionnaire developed
○ Risk rating methodology established
○ Review of vendor security certifications
○ Assessment of financial stability
○ Evaluation of privacy practices and history

### □ Data processing agreements in place

○ Processing limitations clearly defined
○ Security requirements specified
○ Sub-processor restrictions established
○ Audit rights secured
○ Breach notification requirements defined
○ Return or deletion of data at contract end specified

### □ Regular vendor assessments

○ Annual security reassessment scheduled
○ Compliance monitoring process established
○ Security incident tracking implemented
○ Service level agreement monitoring
○ Right to audit exercised periodically

### □ Cross-border transfer mechanisms

○ Adequacy decisions leveraged where applicable
○ Standard contractual clauses implemented

○ Binding corporate rules established for group companies
○ Transfer impact assessments conducted
○ Additional safeguards implemented where necessary

## DOCUMENTATION AND ACCOUNTABILITY

### ▫ Data protection impact assessments

○ DPIA trigger criteria established
○ Assessment methodology documented
○ Mitigation action tracking implemented
○ Regular review of existing DPIAs scheduled
○ Integration with system development lifecycle

### ▫ Up-to-date policies and procedures

○ Data protection policy
○ Information security policy
○ Data retention policy
○ Acceptable use policy
○ Incident response procedures
○ Regular review and update process established

### ▫ Training records

○ Initial data protection training for all staff
○ Role-specific privacy training for key functions
○ Annual refresher training scheduled
○ Training effectiveness assessment
○ Training completion tracking system

### ▫ Processing activities register

○ Purposes of processing documented
○ Categories of data subjects and personal data recorded
○ Recipients of personal data identified
○ Transfer mechanisms documented
○ Security measures described
○ Retention periods specified

### ▫ Regular compliance audits

○ Internal audit program established
○ External compliance reviews scheduled
○ Gap remediation tracking system implemented
○ Executive reporting on compliance status
○ Continuous improvement process defined

## IMPLEMENTATION ROADMAP

Phase 1: Foundation (1-30 days)
- Appoint data protection leadership
- Conduct initial data inventory
- Establish basic data subject rights procedures
- Implement critical security controls
- Develop priority policies and notices

Phase 2: Structure (31-90 days)
- Complete comprehensive data mapping
- Implement consent management system
- Establish vendor management program
- Develop training program
- Implement breach notification procedures

Phase 3: Optimization (91-180 days)
- Refine data subject rights processes
- Enhance security controls
- Implement automated compliance monitoring
- Conduct DPIAs for high-risk processing
- Establish regular compliance reporting

Phase 4: Maturity (180+ days)
- Integrate data protection into business processes
- Implement continuous improvement program
- Enhance monitoring and metrics
- Develop advanced third-party management
- Establish privacy by design practices

## ABOUT RBC ENTERPRISE LIMITED

RBC Enterprise Limited is a leading provider of cybersecurity and data protection solutions in East Africa, offering comprehensive security services, training, and consulting to organizations across multiple sectors. With offices in Nairobi, Kigali, and Dar es Salaam, our team of certified security and privacy professionals delivers practical, contextualized solutions that address the unique challenges of the East African regulatory landscape.

For more information about how RBC Enterprise Limited can enhance your organization's data protection compliance, contact us at privacy@rbc-enterprise.com or visit our website at www.rbc-enterprise.com.