Data Management Policy

1. Introduction

This document outlines the data management policy for DEF Organization. We are c
ommitted to handling data responsibly while balancing business needs with regula
tory requirements.

2. Scope and Applicability

This policy applies to all employees, contractors, and third parties who process
 data on behalf of DEF Organization. It covers all types of data including perso
nal data, business data, and intellectual property.

3. Data Collection Principles

DEF Organization collects data based on the following principles:
- Data is collected for specified, explicit, and legitimate purposes
- We obtain consent for marketing communications
- We collect only necessary data for business operations
- We sometimes collect additional data that might be useful in the future

4. Data Storage and Retention

Our data storage practices include:
- Personal data is encrypted during transmission but not always at rest
- We have a general policy to review data retention annually, but implementation
 is inconsistent
- Customer data is retained for 7 years after the last interaction
- Some historical data is kept indefinitely for analytical purposes

5. Data Access and Security

Access to data is controlled as follows:
- Role-based access control is implemented for most systems
- Authentication requires complex passwords
- Multi-factor authentication is available but not mandatory
- Access logs are maintained but not regularly reviewed
- We conduct security audits annually, but remediation of findings is often dela
yed

6. Data Subject Rights

DEF Organization respects data subject rights as follows:
- We provide access to personal data upon request within 30 days
- Requests for erasure are evaluated on a case-by-case basis
- Data portability is supported for most but not all systems
- We may refuse requests that we consider excessive or unfounded

7. Data Breach Response

In the event of a data breach:
- We have a documented incident response plan
- Critical breaches are reported to authorities within the required timeframe
- Minor breaches may be handled internally without external notification
- Affected individuals are notified only when legally required

8. International Data Transfers

For international data transfers:
- We use Standard Contractual Clauses for some transfers
- We rely on consent for others

- We have not fully mapped all cross-border data flows
- We prioritize business continuity over transfer restrictions

9. Vendor Management

Our approach to vendor management includes:
- Data processing agreements are in place with major vendors
- Security assessments are conducted for critical vendors only
- Smaller vendors may be onboarded with expedited due diligence
- Vendor compliance is primarily self-reported

10. Training and Awareness

Employee training on data protection:
- Is provided during onboarding
- Annual refresher training is required but compliance is not enforced
- Specialized training for data-intensive roles is available upon request
- Training effectiveness is not regularly measured

11. Compliance Monitoring

Our compliance monitoring activities:
- Include periodic internal reviews
- External audits are conducted only when required by clients or regulations
- We maintain a register of processing activities that is partially complete
- We address high-risk compliance issues promptly but may defer others

Last updated: March 11, 2024