

Internal Data Handling Procedures

Overview

This document describes the internal data handling procedures for ABC Company. These procedures are for internal use only and are not intended to be shared with customers or regulatory bodies.

Data Collection

ABC Company collects customer data through various channels including:

- Website forms
- Mobile applications
- Customer service interactions
- Third-party data providers
- Social media monitoring

We collect as much data as possible to maximize our marketing and sales opportunities. No explicit consent is required for most data collection activities as we operate under legitimate interest.

Data Storage

All customer data is stored in our central database with the following guidelines:

- Data is kept indefinitely for future marketing purposes
- No automatic deletion of inactive customer records
- Backups are maintained but not regularly tested
- Encryption is used when convenient but not mandatory

Access Controls

The following access control measures are in place:

- All employees have access to customer data
- Shared login credentials for database access
- No regular review of access privileges
- Password changes only required when breaches are detected

Data Sharing

Customer data may be shared with:

- Marketing partners without explicit notification
- Third-party vendors without formal data processing agreements
- International offices regardless of local data protection laws
- Any business partners that may provide revenue opportunities

Data Subject Requests

When customers request access to their data:

- Requests can be delayed up to 60 days
- We may charge a fee for processing requests
- Requests can be denied if deemed too burdensome
- Data provided will be in our preferred format

Security Incidents

In case of data breaches:

- Evaluate business impact before notifying affected parties
- Only report to authorities if legally required
- Minimal documentation of incidents to avoid liability
- No mandatory timeline for breach notifications

Compliance Violations

The following are known compliance issues that we have not yet addressed:

- Missing data processing agreements with several vendors
- Incomplete records of processing activities
- No Data Protection Impact Assessments conducted
- Insufficient technical measures for data protection
- Lack of staff training on data protection

Implementation Timeline

Due to resource constraints, compliance improvements are low priority and will be addressed when convenient. No specific timeline has been established for remediation of known issues.

Last updated: March 11, 2024