SokoFresh Agri Innovations East Africa Ltd
Head Office: Jasmine Centre, 7 Pio Gama Pinto Road Westlands
Field Office: Murang'a | Makueni | Kitui
Tel: 020 2000 154 | P.O Box 2648,00606 Nairobi, Kenya
Email: info@sokofresh.co.ke | Web: www.sokofresh.co.ke

Employee Data Protection Policy

Version Control: 1
Date of Publishing:1st March 2024

Introduction

The Data Protection Act of Kenya is designed to safeguard personal information and ensure responsible handling of sensitive data by organizations. As an employee, it is crucial to understand the significance of data protection to maintain trust and compliance with the law.

Roles:
Data Controller: SokoFresh Agri Innovations EA Ltd.

Data Protection Officer (DPO):
Winnie Moige Nyachieo. (legal@sokofresh.co.ke | wnyachieo@haysadvisory.co.ke)
Responsible for overseeing data protection within the organization, ensuring compliance with the law, and handling data-related issues.

Supervisor/Manager:
Rachael Njeri Ngige. (rachael@sokofresh.co.ke)
Holds responsibility for enforcing data protection policies within their teams and promptly escalating any reported incidents to the DPO.

Employees: Obligated to follow data protection guidelines, handle sensitive information responsibly, and report any breaches or concerns promptly.

Key Principles

1. Purpose of Policy

This policy applies to all Personal and Sensitive Data we process, covering customers, suppliers, employees, and other third parties. Your compliance is crucial to meet legal requirements.

Personal and Sensitive Data:
Sensitive data includes personal information that, if disclosed, can result in harm or

SokoFresh Agri Innovations East Africa Ltd
Head Office: Jasmine Centre, 7 Pio Gama Pinto Road Westlands
Field Office: Murang'a | Makueni | Kitui
Tel: 020 2000 154 | P.O Box 2648,00606 Nairobi, Kenya
Email: info@sokofresh.co.ke | Web: www.sokofresh.co.ke

discrimination. This may include details about an individual or an Organisation, e.g:
- Personal identifiers such as National Identification Numbers (ID), or KRA numbers
- Financial records, payment information, or credit history of buyers
- Records of communication, such as emails, messages, or call logs, which may contain sensitive details about negotiations or agreements.

2. Scope

Protecting the confidentiality and integrity of Personal Data is everyone's responsibility. The Company may face fines of up to **Kshs 5 million or 1% of the annual turnover** for non-compliance.

Responsibility of Staff:
Employees play a vital role in data protection. It is your responsibility to handle sensitive information with care, follow established security protocols as highlighted below, and report any suspicious activities promptly. Regular training and awareness programs will be provided to ensure compliance.

Personal Data Protection Principles(Security Protocols)

Lawfulness, Fairness, Transparency
Process Personal Data lawfully and transparently. Consent is crucial; ensure Privacy Notices provide clear information.

Consent
Affirmative action is required for Consent. Special Category Data needs Explicit Consent. Maintain and evidence Consent records.

Transparency (Notifying Data Subjects)
Provide clear Privacy Notices when collecting data directly or indirectly. Directly collected data requires immediate notification.

Purpose Limitation
Collect data only for specified, explicit, and legitimate purposes. Inform and obtain Consent for new purposes.

Data Minimization
Collect only necessary data for job duties. Delete or anonymize data following retention guidelines.

SokoFresh Agri Innovations East Africa Ltd
Head Office: Jasmine Centre, 7 Pio Gama Pinto Road Westlands
Field Office: Murang'a | Makueni | Kitui
Tel: 020 2000 154 | P.O Box 2648,00606 Nairobi, Kenya
Email: info@sokofresh.co.ke | Web: www.sokofresh.co.ke

Accuracy
Ensure accuracy, completeness, and relevance of Personal Data. Correct or delete inaccurate data promptly.

Storage Limitation
Do not retain data longer than necessary. Follow retention schedules and inform Data Subjects.

Security, Integrity, and Confidentiality
Implement security measures against unauthorized processing, loss, or damage. Exercise care with Special Categories of Personal Data.

Reporting a Personal Data Breach
Follow procedures for reporting Personal Data Breaches promptly. Preserve evidence and contact the designated point of contact.

Transfer Limitation
Follow guidelines for transferring Personal Data outside Kenya. Safeguards, Consent, or legal necessity are essential.

Data Subject's Rights and Requests
Respect Data Subjects' rights. Verify identity and forward requests to line managers.

Accountability
Demonstrate compliance with data protection principles. Follow guidelines for resources, controls, training, and ongoing compliance.

Record Keeping
Maintain accurate records of Processing activities. Follow the Company's record-keeping guidelines.

Training and Audit
Undergo mandatory data privacy training. Regularly review systems and processes for compliance.

Privacy by Design and DPIA
Implement Privacy by Design. Conduct DPIAs for high-risk Processing activities. Follow Company guidelines.

SokoFresh Agri Innovations East Africa Ltd
Head Office: Jasmine Centre, 7 Pio Gama Pinto Road Westlands
Field Office: Murang'a | Makueni | Kitui
Tel: 020 2000 154 | P.O Box 2648,00606 Nairobi, Kenya
Email: info@sokofresh.co.ke | Web: www.sokofresh.co.ke

Automated Processing and Automated Decision-Making
Inform Data Subjects about decisions based on Automated Processing. Conduct a DPIA before engaging in such activities.

Direct Marketing
Adhere to rules for direct marketing. Obtain Consent for electronic marketing, offer opt-out options, and honor objections promptly.

Sharing Personal Data
Share Personal Data based on job-related needs within the group or with third parties, adhering to privacy laws and contractual arrangements.

Changes to this Data Protection Policy
Regularly review and update the policy. Consider applicable national data privacy laws in the countries where the Company operates.

Scenarios for Data Breach:
Data breaches can occur through various means, such as direct downloads or unauthorized transfers of data. Examples include accessing confidential files without permission, sharing sensitive information with unauthorized parties, or failing to secure electronic devices containing personal data.

Escalation Procedure:
If you suspect a data breach or witness any violation of data protection policies, report it immediately to your supervisor or the designated data protection officer. The organization follows a defined escalation procedure with specific timelines for investigating and addressing reported incidents.

Personal Implications of Aiding a Data Breach:
Aiding a data breach, whether intentionally or negligently, can have severe consequences. Violations may result in disciplinary action, termination of employment, and legal repercussions. It is essential to be aware of the employee contract's clauses related to data protection and understand the legal implications as per the Data Protection Act.

Complaint Procedure:
In case you believe that data has been mishandled or if you have concerns about data protection practices within the organization, follow the established complaint procedure. Lodge a formal complaint with the data protection officer, and the matter will be investigated promptly.

SokoFresh Agri Innovations East Africa Ltd
Head Office: Jasmine Centre, 7 Pio Gama Pinto Road Westlands
Field Office: Murang'a | Makueni | Kitui
Tel: 020 2000 154 | P.O Box 2648,00606 Nairobi, Kenya
Email: info@sokofresh.co.ke | Web: www.sokofresh.co.ke

NOTE:

This guide is your go-to reference for data protection. Your compliance ensures the integrity, security, and fair treatment of Personal Data. For any queries or concerns, reach out to our DPO.

DocuSigned by:
55205B1C5F6B40B...

Denis Karema Chief Executive Officer Date 01.March.2024

Data Protection Complaint Procedure

Introduction:
This procedure outlines the steps employees should follow when filing a complaint related to data protection concerns. The organization is committed to addressing complaints promptly and transparently to ensure the protection of personal information and compliance with data protection regulations.

1. Initiating a Complaint:

Any employee | vendor | customer who believes their data has been mishandled or has concerns about the organization's data protection practices should submit a formal complaint. The complaint can be submitted in writing or via email to the designated Data Protection Officer (DPO).

2. Complaint Content:

The complaint should include a detailed description of the alleged data protection violation, including relevant dates, individuals involved, and any supporting documentation. Providing as much information as possible will facilitate a thorough investigation.

3. Submission to Data Protection Officer (DPO):

Submit the complaint directly to the Data Protection Officer. If the complaint is against the DPO, the complaint should be submitted to the next level of authority or a designated alternative officer responsible for handling such matters.

4. Acknowledgment of Complaint:

Upon receiving the complaint, the DPO or designated officer will acknowledge its receipt promptly. The acknowledgment will include an estimated timeline for the investigation and complaint resolution.

5. Investigation by Data Protection Officer:

The DPO will thoroughly investigate the complaint, including gathering relevant information, interviewing involved parties, and assessing compliance with data protection policies and regulations.

6. Communication with Complainant:

The DPO will keep the complainant informed of the progress of the investigation. If additional information is required, the DPO will communicate the specific details needed.

7. Resolution and Corrective Actions:

Based on the investigation findings, the DPO will propose and implement appropriate corrective actions to address the complaint and prevent future occurrences. The resolution may include policy updates, additional training, or other measures as necessary.

8. Final Communication with Complainant:

Once the complaint has been resolved, the DPO will communicate the final resolution to the complainant. This communication will include an explanation of the actions taken and any changes implemented to prevent similar issues in the future.

9. Escalation to Regulatory Authorities:

If the complainant is dissatisfied with the resolution provided by the organization, they have the right to escalate the matter to relevant regulatory authorities in accordance with applicable data protection laws.

10. Continuous Improvement:

The organization is committed to learning from complaints and continuously improving its data protection practices. Insights gained from complaint resolutions will be used to enhance policies, procedures, and employee training.

This procedure ensures that employees have a structured and transparent process to address data protection concerns, fostering a culture of accountability and compliance within the organization.

Escalation Procedure for Data Protection Incidents

Overview:
This escalation procedure outlines the steps to be followed in the event of a suspected data protection incident. The goal is to promptly address and mitigate any potential risks to sensitive information and ensure compliance with data protection regulations.

1. Reporting Incident:

Any employee who suspects or becomes aware of a data protection incident must immediately report it to their immediate supervisor or manager. This report should include as much detail as possible about the incident, including the nature of the breach, the individuals involved, and any potential impact.

2. Supervisor/Manager Investigation:
Upon receiving the report, the supervisor or manager will initiate a preliminary investigation to assess the severity of the incident. This may involve gathering additional information from the reporting employee, reviewing relevant documentation, and identifying potential immediate actions to mitigate further risk.

3. Involvement of Data Protection Officer (DPO):
If the incident is deemed significant or if the supervisor/manager is uncertain about the appropriate course of action, they must escalate the matter to the designated Data Protection Officer (DPO). The DPO will take over the investigation and coordinate further steps.

4. Assessment by Data Protection Officer:
The DPO will conduct a thorough assessment of the incident, including evaluating the extent of the data breach, identifying affected individuals, and determining the potential impact on data subjects. The DPO will also assess compliance with data protection policies and relevant regulations.

5. Notification of Relevant Parties:
If required by data protection regulations, the DPO will promptly notify the relevant parties, including affected individuals, regulatory authorities, and other stakeholders. Notification will be done in accordance with the timelines and procedures specified by applicable laws.

6. Remediation and Mitigation:

The DPO, in collaboration with relevant departments, will develop and implement a remediation plan to address the incident's impact. This may involve strengthening security measures, providing additional training to employees, or taking other corrective actions to prevent future occurrences.

7. Documentation and Review:
All steps taken during the incident response will be thoroughly documented. After resolving the incident, a comprehensive review will be conducted to identify lessons learned and implement improvements to the organization's data protection measures.

8. Communication with Employees:
Throughout the escalation process, the DPO will communicate transparently with employees, keeping them informed about the incident, the actions taken, and any changes in data protection protocols.

9. Continuous Improvement:
The organization will continuously assess and improve its data protection measures based on the insights gained from incident responses and reviews.
By following this escalation procedure, the organization aims to respond promptly to data protection incidents, minimize potential harm, and maintain a robust framework for compliance with data protection regulations.