



Data Protection and Privacy Policy

Confidentiality

No part of this document may be disclosed verbally or in writing, including by reproduction, to any third party without the prior written consent of Sulfman. This document, its associated appendices and any attachments remain the property of Sulfman and shall be returned upon request.

INTERNAL

Document Control

Owner	Data Protection Officer
Date Reviewed	24/03/2025
Date Approved	24/03/2025
Approved By	Suleiman Farouk
Classification	Internal
Version	1.0



Version History

The following revision history reflects all changes made to this document

Version	Date	Author	Description of Changes
1.0	22/03/2025	Victoria Nababa	Nil

Document Approval

All parties involved acknowledge that they have read, understood and agree with all that has been specified in this document.

Name	Role	Signature & Date
Suleiman Farouk	CEO	 24/03/2025
Faisal Farouk	Senior Consultant	 24/03/2025

1. Introduction

INTERNAL

This Data Protection and Privacy Policy outlines the principles and practices **Sulfman Consulting Ltd.** adheres to for collecting, processing, storing, and disposing of personal data in compliance with Nigeria's Data Protection Regulation (NDPR). We are committed to protecting the privacy and security of all personal data we process in line with regulatory requirements.

2. Scope

This policy applies to all data collected, processed, and retained by **Sulfman Consulting Ltd.** in relation to employees, job applicants, suppliers/vendors, business partners/clients, website visitors, and visitors to our offices.

3. Types of Data Collected

Sulfman Consulting Ltd. collects and processes the following types of personal data:

- **Customer & Business Partner Information:** Name, Address, Business Registration Number, Contact Details.
- **Employee & Job Applicant Information:** Identification details, employment history, qualifications, and professional records.
- **Cybersecurity & Compliance Data:** Security logs, access credentials, and risk assessment details.
- **Website & System Usage Data:** IP addresses, device information, and interaction logs for monitoring security threats.

4. Purpose of Data Collection

We collect personal data for the following purposes:

- **Cybersecurity Services:** Conducting cybersecurity assessments, risk and compliance evaluations, and penetration testing.
- **Client Engagement & Service Delivery:** Providing IT governance and security training programs.
- **Audit & Compliance:** Maintaining records for regulatory compliance and risk management.
- **Employment & HR Management:** Managing recruitment, employee records, and organizational security protocols.

5. Legal Basis for Data Processing

All data processing activities are based on one or more of the following legal grounds:

- **Performance of a Contract** (*e.g., cybersecurity assessments, service agreements, or employment contracts*)
- **Legal Obligation** (*e.g., compliance with NDPR and industry regulations*)
- **Legitimate Interest** (*e.g., improving cybersecurity threat intelligence and risk mitigation strategies*)
- **Consent** (*when required, such as marketing communications or optional data-sharing agreements*)

6. Data Retention

Personal data is retained only for as long as necessary to fulfill its intended purpose or comply with legal obligations. Retention periods include:

- **General Data:** Retained for a maximum of **two years**, unless legal or regulatory requirements dictate otherwise.
- **Cybersecurity Logs & Risk Assessments:** Retained for **up to five years** to support compliance reporting.
- **Employment Records:** Maintained in line with labor laws and company policies.

7. Data Security

Sulfman Consulting Ltd. implements the following data security measures:

- **Encryption:** Secure encryption of data during transmission and at rest.
- **Access Controls:** Restricted access to personal data based on roles and necessity.
- **Regular Security Audits:** Routine review and updates to security protocols to protect against data breaches.
- **Incident Response Measures:** Rapid response protocols for detecting, investigating, and mitigating security incidents.

8. Data Subject Rights

Data subjects have the following rights under NDPR:

- **Access:** Request access to their personal data.
- **Rectification:** Correct inaccurate or incomplete data.
- **Deletion:** Request deletion of data, where applicable.
- **Objection:** Withdraw consent for specific processing activities.
- **Restriction of Processing:** Request a temporary halt on data processing in certain circumstances.
- **Portability:** Request data to be transferred to another service provider where applicable.

9. Data Sharing

We share personal data only with authorized third-party vendors and partners who comply with NDPR standards. These may include:

- **Cybersecurity Partners & Service Providers** (*for security testing and managed security services*)
- **Regulatory Authorities** (*where required for compliance reporting or legal obligations*)
- **Third-Party IT & Cloud Service Providers** (*only where necessary to support infrastructure and security operations*)

10. Updates to this Policy

This policy will be reviewed periodically and updated as needed to comply with regulatory requirements, industry best practices, and organizational needs.

Contact Information

For questions regarding this policy or personal data processing, please contact:
dpo@sulfman.com

Approved By

Name: Suleiman Farouk

Title: CEO

Signature:

A handwritten signature in blue ink, appearing to be "H. P.", written over a horizontal line.

INTERNAL