2021

Data Protection Policy

sewa assets

Sewa Assets Management Limited Data Protection Policy & Procedures

1. Policy Statement

Sewa Assets Management Limited (SEWA or Company) obtains, uses, stores, and otherwise processes personal data relating to data subjects. When processing personal data, SEWA is obliged to fulfil individuals' reasonable expectations of privacy by complying with the General Data Protection Regulation (GDPR), the Nigeria Data Protection Regulation (NDPR) and other relevant data protection regulations.

The Company has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles. Ensuring and maintaining the security and confidentiality of data is one of our top priorities to protect personal information.

2. Purpose

The purpose of this policy is to ensure that we are clear about how personal data must be processed and SEWA's expectations for all those who process personal data on its behalf:

i. to comply with the data protection law and with good practice.
ii. to protect SEWA's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights.
iii. to protect SEWA from risks of personal data breaches and other breaches of data protection law.

The purpose of this policy is to ensure that the Company meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and in the best interest of the information owner.

This policy also serves as a reference document for employees and third parties on the responsibilities of handling and accessing personal data and data subject requests.

3. Data Classification

This policy establishes and defines four classifications for data: Public (Level 1); Company Private Information (Level 2); Confidential (Level 3); and Vital Trust (Level 4); and establishes minimum levels of control for each classification. The definitions for the Company's data classifications are set forth below.

If a system or document contains information falling under more than one Level, it must be classified according to the higher Level contained in that

system or document. A system or document must comply with the standards and requirements for its Level and the Levels below it. For example, if a system is classified as Level 3, then the system must follow the requirements and standards applicable for Levels 1, 2 and 3 classifications.

This policy applies to all data used by Company employees, contractors and consultants, whether created by the Company or entrusted to us by a third party.

3.1 Public (Level 1)

Public information is the least-sensitive type, intended for public disclosure. It includes press releases and marketing messages – the type of information found on company websites. This includes basic historical data, career information, job postings, news releases, and logos.

Employees are responsible for ensuring source copies of public information are protected.

3.2 Company Private Information (Level 2)

Company Private Information is not intended for public release. If Company Private Information is inappropriately disclosed, such disclosure might cause some embarrassment to the Company, but it would not cause any serious loss or business interruption. It includes training materials, guidelines, legal contracts, requests for proposals, requests for quotes, requests for information, information about projects, and other information found on the company's homepage.

Employees should not share Company Private Information with Non-SEWA individuals or entities, unless those individuals or entities have a business need to know.

Data classified as Level 2, may not contain Personally Identifiable Information (PII), in which case it must be classified as Level 3 or higher.

3.3 Confidential (Level 3)

Confidential information is more sensitive than Level 1 or Level 2 information. If confidential information falls into the wrong hands, it might cause serious loss, business interruption, or embarrassment to the Company or a client. It includes trade secrets, computer codes, restaurant recipes, employee performance and personnel files, employee benefits information, customer lists, guest profiles, non-credit card branded gift and stored value card numbers and more.

Employees are forbidden to access or share Confidential data without a valid need to know in support of the business, and then only in full

compliance with the IT Privacy Policy and personal data handling policy.

Confidential data, including PII data can only be shared with a third party (e.g., a contractor or supplier) if a data processing agreement is signed (such an agreement can take the form of a number of clauses in the general service agreement between the contractor/supplier).

Breach of PII data can lead to significant liabilities for the Company as per GDPR/NDPR legislation.

Data classified as Level 3, may not contain sensitive personally identifiable Information (PII), in which case it must be classified as Level 4.

3.4 Vital Trust (Level 4)

Vital Trust information is the most sensitive of the information data classes. It is narrowly defined as:

3.4.1 Sensitive data as defined in GDPR legislation.

Racial or ethnic origin
Political opinions
Religious or philosophical beliefs
Trade union membership
Genetic data
Biometric data for the purpose of uniquely identifying a natural person data concerning health or data concerning a natural person's sex life or sexual orientation.

3.4.2 Government-issued identification numbers (including Personnel numbers; bank verification numbers; Insurance numbers; Voter's Card numbers; Driver's License numbers; National ID numbers; and Passport numbers)

3.4.3 Bank account numbers (including current and saving account numbers)

3.4.4 Credit Card Company Branded card numbers (including credit card, debit card, gift card and stored-value card numbers)

3.4.5 User account names and passwords

The above list is not exhaustive but are merely samples of Vital Trust Data. Any type of personal data not mentioned specifically in the list, but which nonetheless constitutes sensitive data in the meaning of the GDPR falls within the Level 4 category.

In the case of some of the above, truncated numbers or anonymized information may not be Vital Trust. Contact the IT department for more information.

Employees are required to treat Vital Trust information with extreme care.

Sensitive personal data in the definition of the GDPR can only be processed in exceptional cases such as:

- Based on explicit consent for one or more specified purposes
- For the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection when authorized by law.

It is particularly important to ensure the sensitive data is not used for other purposes than those for which it has been collected.

Vital Trust information must be encrypted in storage and in transit when sent outside of trusted networks. All Vital Trust data should be stored under lock and key when not in use and is not to be left unattended.

4 Data Classification Elevation

The Company may, from time to time, have business requirements to raise data elements to a higher classification. Clients/governing body may require the company to hold their specific data to a higher standard than that required by these standards. The company can reclassify data to a higher level if required by a client/governing body. By doing so, the company will be meeting a higher level of care with respect to that data and will be held to the control objectives of the higher data classification. In addition, the company is required to communicate the data "re-classification" to employees and to the IT Department.

5 Scope

This policy applies to all personal data we process regardless of the location where that personal data is stored (e.g., on an employee's own device) and regardless of the data subject. All staff and others processing personal data on SEWA's behalf must read it. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

6 Personal Data Protection Principles

When you process personal data, you should be guided by the GDPR/NDPR and other relevant data protection regulations. SEWA is responsible for, and must be able to demonstrate compliance with the following data protection principles that require personal data to be:

- processed lawfully, fairly and in a transparent manner.

- collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- accurate and where necessary kept up to date.
- not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed.
- processed in a manner that ensures its security, using appropriate technical and organizational measures to protect against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

7 Data Subjects' Rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

a. where the legal basis of our processing is Consent, they have the right to withdraw that Consent at any time.
b. to ask for access to the personal data that we hold.
c. to prevent our use of the personal data for direct marketing purposes.
d. to object to our processing of personal data in limited circumstances.
e. to ask us to erase personal data without delay:
    - if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed.
    - if the only legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data.
    - if the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest.
    - if the data subject has objected to our processing for direct marketing purposes.
    - if the processing is unlawful.
f. to ask us to rectify inaccurate data or to complete incomplete data.
g. to restrict processing in specific circumstances e.g., where there is a complaint about accuracy.
h. to prevent processing that is likely to cause damage or distress to the data subject or anyone else.
i. to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms.
j. to make a complaint to the appropriate body.

You must verify the identity of an individual requesting data under any of the rights listed.

8 Accountability

SEWA must implement appropriate technical and organizational measures in an effective manner to ensure compliance with data protection principles.

SEWA is responsible for and must be able to demonstrate compliance with the data protection principles. We must therefore apply adequate resources and controls to ensure and to document data protection regulation compliance.

9 SEWA's responsibilities

As the Data Controller, SEWA is responsible for establishing policies and procedures in order to comply with data protection law. SEWA **ensures that:**

a. We protect the rights of individuals with regards to the processing of personal information.
b. We develop, implement, and maintain a data protection policy, procedure, audit plan and training program for compliance with the data protection laws.
c. Every business practice, function and process carried out by the Company, is monitored for compliance with the data protection laws and its principles.
d. Personal data is only processed where we have verified and met the lawfulness of processing requirements.
e. We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested.
f. All employees are competent and knowledgeable about their GDPR/NDPR obligations and are provided with in-depth training in the data protection laws, principles, regulations and how they apply to their specific role and the Company.
g. We maintain a continuous program of monitoring, review, and improvement with regards to compliance with the data protection laws and to identify gaps and non-compliance before they become a risk, affecting mitigating actions where necessary.
h. We have appointed a Data Protection Officer who takes responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws and performs specific duties as set out under GDPR/NDPR.
i. We have a dedicated Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. The audit program is reviewed against our data protection policies, procedures and the relevant regulations to ensure continued compliance.

j. We provide clear reporting lines and supervision with regards to data protection.
k. Any information provided to an individual in relation to personal data held or used about them, will be provided in a concise, transparent, and easily accessible form, using clear and plain language.
l. We have developed and documented appropriate technical and organizational measures and controls for personal data security.

10 Data Protection Officer (DPO) responsibilities

The DPO is responsible for:

a. advising SEWA and its staff of its obligations under data protection regulations.
b. monitoring compliance with GDPR/NDPR and other relevant data protection laws or regulations, and monitoring training and audit activities related to GDPR/NDPR compliance.
c. to cooperate with and act as the contact point for the government data protection office.
d. data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, considering the nature, scope, context and purposes of processing.

11 Staff responsibilities

Staff members who process personal data about data subjects must comply with the requirements of this policy. Staff members must ensure that:

a. all personal data is kept securely.
b. no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorized third party.
c. personal data is kept in accordance with the SEWA policies and procedure.
d. any queries regarding data protection, are promptly directed to the company or any office responsible.
e. any data protection breaches are swiftly brought to the attention of the data protection and or information compliance team and the Data Protection Officer and that they support data protection and or information compliance team/DPO in resolving breaches.
f. where there is uncertainty around a data protection matter advice is sought from the data protection and or information compliance team and the Data Protection Officer.

You must regularly review all the systems and processes under your control to ensure they comply with this policy.

12 Governance Procedures

Our main governance objectives are to:

a. Educate senior management and employees about the requirements under the data protection laws and the possible impact of non-compliance.

b. Provide a dedicated and effective data protection training program for all employees.
c. Identify key stakeholders to support the data protection compliance program.
d. Allocate responsibility for data protection compliance and ensure that the designated person(s) has enough access, support and budget to perform the role.

13 Reporting a personal data breach

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or the necessary authority where we are legally required to do so.

14 Record Keeping

The GDPR/NDPR requires us to keep full and accurate records of all our data processing activities. We must keep and maintain accurate corporate records reflecting our processing, including records of data subjects' Consents and procedures for obtaining Consents, where Consent is the legal basis of processing.
These records should include, at a minimum, the name and contact details of the SEWA Data Controller and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.
Records of personal data breaches must also be kept, setting out:

a. the facts surrounding the breach
b. its effects and
c. the remedial action taken.

15 Data Retention & Disposal

The Company has defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and our business requirements, as well as adhering to the NDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects and prioritizes the protection of the personal data in all instances.

16 Security & Breach Management

We ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. Our **Information Security Policies** together with our **Communications & Operations Management Policy, Acceptable Use Policy** and **Access Control Policy**

provide the detailed measures and controls that we take to protect personal information and to ensure its security from consent to disposal.

We carry out information audits to ensure that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on data subject(s). We have implemented adequate and appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

Whilst every effort and measure are taken to reduce the risk of data breaches, the Company has dedicated controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and data subjects (where applicable).

17 Transfers & Data Sharing

The Company takes proportionate and effective measures to protect personal data held and processed by us at all times, however we recognize the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred.

Where data is being transferred for a legal and necessary purpose, we utilize a process that ensures such data is encrypted and where possible is also subject to our data minimization methods.

The DPO verifies the encryption and security methods and measures.

18 Audits & Monitoring

This policy and procedure document details the extensive controls, measures and methods used by the Company to protect personal data, uphold the rights of data subjects, mitigate risks, minimize breaches and comply with the data protection laws and associated laws and codes of conduct. In addition to these, we also carry out regular audits and compliance monitoring processes with a view to ensuring that the measures and controls in place to protect data subjects and their information are adequate, effective and compliant always.

The DPO has overall responsibility for assessing, testing, reviewing, and improving the processes, measures and controls in place and reporting improvement action plans to the Senior Management Team where applicable. Data minimization methods are frequently reviewed, and new technologies assessed to ensure that we are protecting data and individuals to the best of our ability.

All reviews, audits and ongoing monitoring processes are recorded by the DPO and copies provided to Senior Management and are made readily available to the Supervisory Authority where requested.

The aim of internal data protection audits is to: -

- Ensure that the appropriate policies and procedures are in place.
- To verify that those policies and procedures are being followed.
- To test the adequacy and effectiveness of the measures and controls in place
- To detect breaches or potential breaches of compliance
- To identify risks and assess the mitigating actions in place to minimize such risks.
- To recommend solutions and actions plans to Senior Management for improvements in protecting data subjects and safeguarding their personal data.
- To monitor compliance with the data protection laws and demonstrate best practice.

19 Training

Through our strong commitment and robust controls, we ensure that all staff understand, have access to and can easily interpret the data protection laws requirements and its principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role.

Employees are continually supported and trained in the data protection laws requirements, and obligations around data protection.

20 Penalties

The Company understands its obligations and responsibilities under the data protection laws and recognizes the severity of breaching any part of the law or Regulation. We respect the Supervisory Authority's authorization under the legislation to impose and enforce fines and penalties on us where we fail to comply with the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

21 Responsibilities

The Company has appointed a Data Protection Officer (DPO) whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

The DPO will work in conjunction with the Compliance Officer, IT Manager and Executive Management Committee and Heads of SBUs and Shared

Services to ensure that all processes, systems and staff are operating compliantly and within the requirements of the data protection laws and its principles.

The DPO has overall responsibility for due diligence, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the data protection laws and our own internal objectives and obligations.
Staff who manage and process data information will be provided with extensive data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledgeable for the role they undertake.

For more information on our policies and procedures see our Privacy Policy; Information Security Policy; Remote working and Removable Media Policy; Acceptable Use Policy; Access Control Policy, Communications & Operations Management Policy.

Document Control Sheet

DOCUMENT CONTROL SHEET

Version and Update History:

Version	Date	Author	Change from Previous Version
1.0	JULY 2021	ERM Unit	

Approval List:

Name	Position	Signature	Date
	IT Unit		
	Legal & Compliance Unit		
	Enterprise Risk Management Unit		
	Managing Director		
	Chairman Board Risk, Audit & Compliance Committee		

Distribution List:

Name	Version	Date
All Staff	1.0	JULY 2021
Partners, Clients, Vendors	1.0	JULY 2021

Policy Review

This policy is subject to continuous changes. In case there are no changes, then an annual review shall be performed.