zamara
Powering Prosperity

ZAMARA GROUP DATA PROTECTION & PRIVACY POLICY:

Version 1.2021

TABLE OF CONTENTS

1.0. POLICY INFORMATION

	Name	Signature	Date
Prepared by	Simba & Simba Advocates & Group Head, Governance, Risk & Compliance - ZHL		
Document Owner	Sundeep Raichura, Group Chief Executive Officer		
Approved by	Chris Nyokangi, Group Chief Operations Officer		
Authorised by	ZHL Board of Directors		
Creation Date	October 2021		
Latest Approval Date	December 2021		
Version	1		

2.0. APPROVAL OF THIS POLICY

This Policy was approved by the Chairman of the Board and come into effect on the date of approval and will be reviewed on an annual basis but will remain in effect until replaced by a new policy to be brought into effect by formal signed approval.

Signed approval by: Chairman of the Board

Name: _____

Signature: _____ Date: _____

3.0. DEFINITIONS

Anonymization

Irreversible removal of personal identifiers from information so that the data subject is no longer identifiable.

Collection

The act of gathering, acquiring, or obtaining Personal Data from any source, including third parties and whether directly or indirectly by any means.

Commissioner

The Office of the Data Protection Commissioner established under the Data Protection Act 2019.

Consent

Any freely given specific and informed indication of the wishes of the data subject by which they signify their agreement to the processing of their personal data.

Control

An agency, natural or legal person, public authority, organization or any other body which alone or jointly with others has the power to determine the purposes and means of the processing of data, and the manner in which the data is processed.

Data

Includes all data including personal data in electronic or manual form.

Data controller

Any such entity as shall be designated from time to time as a result of performance of various necessary functions.

Data Processor

Any person (other than an employee Zamara) who processes the data on behalf of Zamara.

Data Protection Compliance Team

The Data Protection Compliance Team shall constitute the Division Heads, who shall be tasked with monitoring, overseeing, reviewing and reporting on their respective Division's data protection processes to the DPO.

Data Protection Officer (DPO)

Person duly appointed or designated by the GCEO to handle all matters of data protection, privacy and security.

Data Subject

A natural person whose personal data is held by Zamara.

Disclosure

Making data available to persons other than Zamara's representatives.

Encryption

The process of removing personal identifiers, and converting information or data into code, to prevent unauthorised access.

Notification

Informing Zamara and or the Data Protection Commissioner and or the Data Subject about a data breach, as applicable.

Personal data or Personal Information

Any information relating to an identified or identifiable natural person (Data Subject). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, passport number, birth certificate or to one or more specific factors like physical or physiological.

Identifiable person

Any individual who can be identified, directly or indirectly, in particular by reference to an identification number, passport number, birth certificate or to one or more specific factors like physical or physiological.

Processing

Any operation performed on personal data, such as collecting, creating, recording, structuring, organizing, storing, retrieving, accessing, using, seeing, sharing, communicating, disclosing, altering, adapting, updating, combining, erasing, destroying or deleting personal data, or restricting access or changes to personal data or preventing destruction of the data.

Restriction of processing

The marking of stored personal data with the aim of limiting their processing in the future.

Pseudonymisation

The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable person. Pseudonymised data is therefore re-identifiable and falls within the definition of personal data.

Sensitive Personal Data or Personal Sensitive Data

This refers to specific personal data as to:

a) The racial, ethnic or social origin;
b) the political opinions or the religious or conscience belief, culture dress language or birth) of the data subject;
c) gender;
d) whether the data subject is a member of a trade-union;
e) disability;
f) sexual life or orientation;

g) pregnancy;
h) colour;
i) age;
j) marital status;
k) health Status;
l) the commission or alleged commission of any offence by the data subject; or
m) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings;
n) biometrics (where needed for identification).

Types of Personal Data

Zamara collects and processes the following subsets of Data:

Identity Data

This consists of information in respect to a client, member of staff, or third parties and includes: name; title; age; date of birth;

Attendance/Visits

Visitor log information which you provide (including applicable vehicle details and your business name); CCTV images and footage captured by our security systems; and any health, safety and security information related to your visit, such as the individual's temperature, allergies and the like.

Contact Data

This consists of data used to contact clients or their assignees/beneficiaries (as the case may be) and so includes: contact address; contact email address; and contact telephone numbers.

Financial Data

This consists of financial data in respect of clients, beneficiaries, and so includes: bank account and payment details. It also includes data pertaining to transactions made or supplied by the client or third party distributors that directly or indirectly relate to Zamara operations and procurement processes.

Marketing and Communications Data

This consists of details in relation to Zamara's marketing and communications strategies/ channels, and may include client feedback and data with respect to any surveys, interviews, conducted by Zamara to improve its products and services.

Third Party

Any person/entity other than the Data Subject, the data controller, or data processor or other person authorized to process data for the data controller or processor, in relation to personal data. For avoidance of doubt, this refers to any individual or organisation that Zamara interacts with in the course of business. This includes our current and potential clients, customers, suppliers, distributors, business contacts, agents, advisers, and government and public bodies including their advisors, representatives, officials, politicians, and public parties.

Vulnerable Group

Any member of the society who is at a risk of being discriminated because of their physical, mental, physiological and social conditions. Such members usually have difficulties giving free and informed consent.

Managing Director of ZARIB, C&P, ZAAC-UG, ZAAIB, ZPAL, ZCAN, SIB or BSC

The Managing Directors of each of ZARIB, C&P, ZAAC-UG, ZAAIB, ZPAL, ZCAN, SIB and BSC as appropriate.

Employee

Includes permanent employees, temporary employees, independent contractors and employees / contractors of contracted services providers, of any of corporate entities forming part of the Group.

Group Chief Executive Officer ("GCEO")

The Chief Executive Officer of Zamara Holdings Limited ("ZHL").

Group Chief Operations Officer ("GCOO")

The Chief Operations Officer of Zamara Holdings Limited ("ZHL").

Group Head, Governance Risk & Compliance ("GH-GRC")

The Group Head, Governance Risk & Compliance for Zamara Holdings Limited ("ZHL") and all subsidiaries.

Manager or Executive Manager or Division Head

A manager responsible for the management of a business sector or business unit within the Group, including relevant Divisional and Subsidiary Directors, Executive Managers, Managers and / or Regional Managers.

Client(s)

Refers to a corporate or individual to whom a Zamara entity may provide a service or product.

Executive Committee ("EXCO")

- The senior leadership of the Group (referred to below as EXCO) and includes the following persons
- The Group Chief Executive Officer, the Chief Executive Officer or Managing Director and Executive Committee at group and subsidiary level and General or Division Managers
- Employees responsible for management who report directly to the Chief Executive or to any of the Executive, General or Divisional Managers; and
- Any other persons designated from time to time by the Chief Executive as being members of the EXCO.

Zamara Group (the "Group")

The Zamara Group of Companies include:

- Zamara Holdings Limited ("ZHL")
- Zamara Actuaries, Administrators & Consultants Limited ("ZAAC")
- Zamara Risk & Insurance Brokers Limited ("ZARIB")
- Corporate & Pension Trust Services Limited ("C&P")
- Zamara Actuaries, Administrators & Consultants (Uganda) Limited ("ZAAC-UG")
- Zamara Actuaries Administrators and Insurance Brokers Limited ("ZAAIB")
- Zamara Pension Administrators Limited ("ZPAL")
- Zamara Consulting Actuaries Nigeria Limited ("ZCAN")
- Stonebridge Insurance Brokers (Nigeria) Limited ("SIB")
- B S Company and Actuarial Services (Tanzania) Limited ("BSC")

And where the context so requires **Zamara** or **Company** shall refer to ZHL, ZAAC, ZARIB, C&P, ZAAC-UG, ZAAIB, ZPAL, ZCAN, SIB and BSC as appropriate and **Group** shall refer to all the Companies.

4.0. INTRODUCTION, PURPOSE & SCOPE

4.1 Concerns relating to the security of personal data have led to enactment of the Data Protection Act 2019 and 2021 Regulations in Kenya. These laws and regulations seek to protect the privacy of individuals under Article 31 of the Constitution of Kenya 2010, by enforcing responsible processing of personal data.

4.2 For the success of Zamara's various divisions, there is need, either statutory or otherwise, to collect and process various categories of data relating to Clients.

4.3 For purposes of the Data Protection Act 2019, Zamara may be defined, both as Data Controller and Data Processor.

POLICY STATEMENT

4.4 This Data Protection and Privacy Policy describes how personal data shall be collected, handled, stored and otherwise processed to meet Zamara's Data Protection standards and to comply with requirements of the Data Protection Act 2019 and Regulations thereunder.

4.5 Zamara is committed to complying with all provisions of the Data Protection Act 2019 and the attendant Regulations.

4.6 Zamara undertakes to enforce the data protection principle of lawfulness and transparency, by ensuring open and honest processing of data, including involving data subjects in all matters affecting their right to privacy and data protection.

4.7 Zamara will provide training and support to staff who handle personal data.

PURPOSE AND OBJECTIVES OF THE POLICY

4.8 The purpose of this policy is to guide the management of Personal Data and Sensitive Personal Data by establishing an effective data processing framework that is consistent with data processing principles and the rights of data subjects.

4.9 The objectives of this policy are:

i. To ensure effective protection and management of Personal Data by identifying, assessing, monitoring and mitigating privacy risks in Zamara's activities involving the collection, retention, use, disclosure and disposal of Personal Data.

ii. To comply with international good practice and ensure consistency in practices and procedures in personal data processing.

iii. To ensure compliance of the policy and sound management practices to safeguard the rights of the data subjects, including children and the vulnerable groups in accordance to the Data Protection Laws of Kenya.

iv. To protect clients, staff and the organization from the risks related to data breach.

SCOPE

4.10 This policy applies to all employees, vendors, contractors and such other third parties with whom Zamara deals with, including:

- Zamara Holdings Limited (ZHL);
- Zamara Actuaries, Administrators & Consultants Limited (ZAAC);
- Zamara Risk & Insurance Brokers Limited (ZARIB);
- Corporate & Pension Trust Services Limited (C&P); and

4.11 And where the context so requires Zamara or **Company** shall refer to ZHL, ZAAC, ZARIB or C&P as appropriate and **Group** shall refer to all the Companies in Kenya.

4.12 This Policy shall apply to Rest of Africa entities and their employees, vendors, contractors & third party providers only if the local Board of Directors of the ROA entity adopts this Policy with appropriate changes to reflect their local statutory and business environment.

4.13 This policy applies to any Personal Data (including Sensitive Personal Data) which is controlled or processed by Zamara or Personal Data belonging to a resident in Kenya that is controlled or processed outside Kenya.

POLICY REVIEW

4.14 The Data Protection Officer is responsible for ensuring that this policy is reviewed on a timely basis.

4.15 This policy shall be reviewed every two (2) years, or more frequently if appropriate, to be consistent with future developments, industry trends and/or any changes in legal or regulatory requirements.

RELATED POLICIES

4.16 This policy shall be read in conjunction with Zamara's:

i. Disclaimer Policy;
ii. ICT Policy;
iii. Code of Conduct Policy and Staff Handbook.

REMUNERATION

4.17 The Data Protection Officer or such other designated officer under this policy may be remunerated as shall be agreed from time to time.

5.0. GENERAL PROVISIONS

TYPES OF PERSONAL DATA

5.1 Zamara collects and processes the various subsets of data including:

- Identity Data
- Attendance/Visits
- Contact Data
- Financial Data
- Marketing and Communications Data

PRINCIPLES FOR DATA PROTECTION

5.2 The following principles guide the day to day processing of Personal and Sensitive Personal Data within the Company.

5.3 Confidentiality

5.3.1 Personal data must be processed securely to retain confidentiality over its entire life cycle.

5.4 Accuracy

5.4.1 All personal data that is recorded and processed must be correct, complete, and be kept up to date;

5.4.2 Suitable steps must be taken to ensure that any detected inaccurate or incomplete data is deleted, corrected, supplemented or updated within reasonable timelines. This applies to information taken over the telephone, email, mobile applications or other communication medium. This includes undertaking periodic data accuracy checks by requesting the data subject to confirm the accuracy of the data held;

5.4.3 Where information is supplied by a third party and not directly from the data subject, reasonable steps must be taken to ensure its accuracy, including an appropriate declaration of accuracy by the third party;

5.4.4 To ensure all personal data is kept up to date, a periodic review framework of all personal data collected, processed or stored in hard copy or soft copy mediums shall be established. All Divisions shall conduct data checks as may be appropriate and depending on volumes and level of sensitivity.

5.5 Legitimate Purpose

a. Personal Data shall only be collected for specified, explicit, and legitimate purposes and shall not be further processed in a manner that is incompatible with those purposes;

b. Personal data must be processed only for the purpose(s) that was defined before the data was collected;

c. Further processing for archiving purposes in the public interest, scientific interest or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose;

d. Any subsequent changes to the purpose are only possible to a limited extent and require a legitimate basis to justify the same.

5.6 Data Minimization

a. Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which the data will be processed;

b. Before any data is acquired or processed, a determination shall be made as to the type/nature of the personal data required and to what extent the processing of that personal data is necessary to achieve the purpose for which the data is required;

c. Personal data may not be collected in advance and stored for potential future purposes unless pursuant to a legitimate purpose which the data subject has consented to. However, Zamara shall maintain a record of data under this Clause as necessary to fulfil legal obligations as may be required.

5.7 Integrity

a. At all times Personal data will be processed securely to retain its integrity in consistency, accuracy, and trustworthiness over its entire life cycle;

b. Sufficient steps will be taken to ensure that data cannot be altered by unauthorized entities or people whether during collection, transmission, general processing and/or storage of the same. This will be achieved by restricting access to data to those Employees assigned a client and further requiring all data changes to be approved by Team Leaders;

c. Suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction shall be put in place. This will be achieved through the use of authentication for access to the various data servers and further restricting transfer of data from servers to external devices without appropriate approvals.

5.8 Lawfulness and Transparency

a. There shall be transparency regarding the processing of personal data which includes duly informing the data subject in an open and intelligible manner the purpose for processing that personal data.

b. Data subjects shall be sufficiently informed of the general nature of such processing and their individual data rights in relation to that data;

c. The needed information to help data subjects exercise their data rights, shall be availed during initial client interviews/ interactions and on the Company websites and Application Software.

6.0. PEOPLE AND RESPONSIBILITIES

6.1 All Employees must read and comply with all provisions of this policy and report any breaches. The Company shall ensure safeguard mechanisms to guarantee protection of personal data and Management shall be responsible for ensuring that this policy and its contents are made available to Employees and other third parties with whom the Company has outsourced any services.

6.2 Data Protection Officer

6.2.1 The responsibilities of the DPO shall include:

i. To periodically review the personal data processing operations and advise on any improvements, changes, additions, alterations and the like in order to conform to any current, new or subsequent processing activity to the guiding principles under Part II of this Policy;

ii. To cooperate with the Commissioner and other relevant bodies in data protection and to effect the necessary data regulation provisions as stipulated by the Commissioner in its periodic guidelines and Practice Notes;

iii. To notify the Commissioner of any data breach;

iv. To conduct data protection impact assessment where high data processing risks are imminent;

v. To develop internal data protection policies and procedures;

vi. To advise and promote awareness on data protection;

vii. To keep the Board and Management updated about the organization's data protection responsibilities, risks and issues;

viii. To annually review all data protection procedures and related policies;

ix. To arrange / conduct data protection training and provide advice in relation to the Data Protection Act and the such Regulations thereunder;

x. To address data protection questions from Employees within agreed timelines;

xi. To monitor new and on-going data protection risks and update the Company's risk register;

xii. To make regular compliance reports to the Commissioner on the Company's data protection performance; and

xiii. To perform any other such function as to ensure the Company's compliance with data protection laws.

6.3 Data Protection Compliance Team

6.3.1 The Division Heads shall be responsible for any data breaches that occur within their respective Divisions.

6.3.2 The Compliance Team shall ensure their respective Divisions cooperate while or during the processing of personal data exchanged between their Divisions to ensure full compliance with this Policy.

6.4 The Head of IT shall be responsible for:

6.4.1 Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

6.4.2 Performing regular checks and scans to ensure security hardware and software is functioning properly.

6.4.3 Evaluating and advising on any third-party services the Company is considering using to store or process data.

6.5 The Head of Marketing shall be responsible for:

6.5.1 Utilizing the necessary data protection and security statements attached to communications such as emails and letters.

6.5.2 Ensuring all marketing initiatives abide by data protection principles and the Data Protection Policy.

6.6 General Staff Guidelines

6.6.1 Personal data will not be disclosed to unauthorised people, either within the Company or externally.

6.6.2 In the event of uncertainty about any policy provision or procedure in relation to data protection, Employees shall request for help from their Division Head or GH-GRC or the DPO.

6.6.3 Every Employee is responsible for ensuring any personal data they come across intentionally or accidentally, is handled in accordance with the data protection principles laid out in this Policy.

6.6.4 All Employees are required to read, understand and accept any policies and procedures that relate to personal data they may handle in the course of their work.

6.7 Data Processing Activities Audits

6.7.1 Zamara shall, every three years, or earlier if required, review mapping of its various data processing activities to identify and mitigate risks associated with such processing activities.

6.8 Data Protection Trainings

6.8.1 Zamara, through its Data Protection Officer will annually or where such need arises, conduct trainings of Employees and stakeholders who have access to any kind of personal data in order to raise/discuss data protection issues.

6.8.2 As part of new Employees' onboarding process, the contents of this Policy shall be communicated for purposes of familiarization.

6.8.3 Zamara shall also communicate the existence of this Policy and its requirements to Clients and Third Parties who process data on behalf of Zamara. These parties will be required to comply with the provisions of this Policy. Any data breach under this provision must be reported to the GH-GRC within 48 Hours of the incident.

6.9 Data Risk Impact Assessments

High risk data processing activities shall be supported by a Data Protection Impact Assessment carried out in liaison with the Data Protection Officer and other relevant officers.

6.10 Consequences for Non-Compliance

It is the responsibility of all Divisions that process personal data to adhere to this Data Protection Policy. Misuse of personal data, through loss, disclosure, or failure to comply with this Policy and the rights of Data Subjects, shall result in legal and financial damages including penalties as specified in the Act.

7.0. LAWFUL PROCESSING OF DATA

LAWFUL BASIS OF PROCESSING PERSONAL DATA - CONSENT

7.1 Where required and necessary, the Company will maintain adequate records demonstrating that consent was obtained prior to processing of data relating to a Data Subject. Where such consent is withdrawn or there is a concern relating to consent, such data shall not be processed by Zamara.

7.1.1 Zamara will obtain consent from each Data Subject on the processing of their Personal Data including Sensitive Personal Data;

7.1.2 Data subjects should be made to clearly understand why their information is needed, who it will be shared with, and the possible consequences of them agreeing or refusing the proposed use of the data;

7.1.3 The processing of personal data for a child shall be done only with the consent of the child's parent or guardian;

7.1.4 The organization acknowledges that consent once given, can be withdrawn at any time, but not retrospectively.

LAWFUL BASIS OF PROCESSING PERSONAL DATA - EXCEPTIONS

7.2 It is acknowledged that there will be exceptional circumstances where personal data can be processed without the Data Subjects consent. Such exceptional circumstances shall include:

7.2.1 Where there is a public interest concern, a national security concerns or a valid court order, the information may be shared without the express consent of the data subject, subject to strict due diligence.

7.2.2 Where processing is necessary to take steps, at the request of the data subject, before entering a contract or to enable the performance of a contract the data subject is privy to, the same shall constitute a valid legal basis for data processing.

LAWFUL BASIS OF PROCESSING PERSONAL DATA - THIRD PARTY DATA PROCESSING

7.3 Personal data shall not be disclosed or processed by a third party resident in Kenya except where there is a Third Party Data Processing Agreement which has been approved and signed by the DPO. The Data subject should be made aware of this where such arrangements are in place.

MODES OF DATA COLLECTION

7.4 In the exercise of data collection, the following constitute the means by which Personal Data is collected by the Company:

7.4.1 Direct Interactions - this includes Personal Data the Data Subject provides upon visiting our offices, or our website, interaction with our Employees, Completion of forms availed by Zamara, information obtained upon making an inquiry, request or complaint via telephone, email or any mobile application.

7.4.2 Automated technologies or interactions – this is information obtained upon interaction with the Group or Company website and includes browsing actions, patterns, type of browsing equipment. It also includes CCTV images and footages from the CCTV systems in the Company premises.

7.4.3 Third parties or publicly available sources – this is information acquired from guardians in respect of children, trustees in respect of the beneficiaries, beneficiaries in respect of their next of kin that Zamara would interact with in the course of discharging their duties and services.

DATA TRANSFERS OUTSIDE KENYA

7.5 The Company may transfer personal data out of Kenya subject to the following conditions:

7.5.1 Due diligence on appropriate measures relating to the security and protection of the Personal Data and the proof thereof shall be communicated to the Data Protection Commissioner as required under the Data Protection Act 2019.

7.5.2 The receiving jurisdiction shall have commensurate data protection laws.

7.5.3 The transfer shall be necessary for the performance of a contract, including:

- Contracts relating or affecting the data subject;
- To fulfil legal or contract obligations;
- To confer a benefit to the Data Subject;
- To perform an approved study or research relating to the Data Subject's benefit.
- To fulfil a public interest concern or legitimate interest, subject to the Data Subject's rights.

7.5.4 Zamara may process Sensitive Personal Data outside Kenya subject to obtaining the consent of the Data Subject, as provided for under this Policy.

DATA SECURITY AND DATA SECURITY MEASURES

7.6 Zamara acknowledges numerous risks posed to the Personal Data it collects and processes. Some of these risks include data diversion through either unauthorised or inappropriate disclosures, poor data security, poor management systems, individuals receiving incorrect benefits or payouts through data being inaccurate, incomplete or insufficient.

7.7 Data Protection by Design and Default

7.6.1 Privacy `will be built in from the outset in all data management systems including critical systems.

7.6.2 Zamara shall employ appropriate personal data security controls such as encryption, anonymization and Pseudonymisation of personal data.

7.7 Technical and Organizational Measures

7.7.1 Appropriate technical, organizational and other measures will be taken to prevent unauthorized, unlawful processing, accidental loss, destruction of, damage to, as well as unauthorised access, disclosure, copying, use, or modification of personal information.

7.7.2 Such measures will include the use of password protection, clear desk policy and entry control to storage rooms where Sensitive Personal Data is stored

7.7.3 Periodically Zamara shall conduct privacy and information audit and risk assessment at each stage of every project or initiative involving collection, processing, transmitting, storage, use and disposal of personal data and in managing upgrades or enhancements to systems and processes used to handle personal data.

7.8 Data Storage

7.8.1 Data will be stored safely and questions related to the safe storage of data should be directed to the IT manager or Data Protection Officer, as appropriate.

- When data is stored on paper, it will be kept in a secure place, preferably in a locked cupboard, where unauthorized persons cannot access it;
- Personal data will only be kept for the duration necessary to achieve the purpose for which the data was collected and processed;
- In determining the manner of storage, consideration will be given to the nature/ type of data, the length of the retention period, the use of the said data, and the needed ease of access;
- Where Personal Data or the use thereof merits storage for a longer period than was initially envisaged, the said data may be stored subject to adequate protection pending the legal clarification of whether the same merits a longer storage/retention period by the Data Protection Officer;
- All archived personal data will be anonymized.

7.9 Data Archiving and Destruction

7.9.1 Anonymized and pseudonymized data will be archived in the form to be prescribed by the Division Head;

7.9.2 This data will be kept in a form that allows reconstruction by authorized persons;

7.9.3 Destruction of data shall be effected only with the permission of the Division Head and shall be done in accordance with this Policy;

7.9.4 Once data is identified for and destroyed by deletion, no physical medium or software should remain with copies of the deleted data.

7.10 Record Keeping for Employee Data

7.10.1 People and Culture will maintain a comprehensive record of all Employees and when requested by the GCEO and the Board, provide statistics and information relating to employees, health status, dependents etc.;

7.10.2 People and Culture will maintain a confidential file for every Employee that shall contain a complete record of an employee's career at Zamara. The data contained in this file shall include details of application for the position, interview report, letter of offer, letter of appointment, copies of academic and professional certificates, copy of ID card, copy of PIN, probation report, letter of confirmation, leave forms, sick sheets, warning letters, passport photograph, etc.;

7.10.3 People and Culture will also retain copies of all correspondence and written information it initiates or receives from the employee, or his/her supervisors which may be relevant to his/her terms and conditions of employment, in the Employee's individual file;

7.10.4 People and Culture may require the employee to submit details relating to their family members, in a next-of-kin form, and it is the responsibility of the Employee to inform the affected family member of such nomination;

7.10.5 People and Culture shall endeavor to keep data under this policy accurate, and the employee is required to notify People and Culture of any change in name, address, contact or any other such data, including that of the Employee's next-of- kin;

7.10.6 People and Culture will at all times keep in safe custody the files for former Employees who have left Zamara for as long as it is necessary and for historical purposes as provided for under the Data Protection Act 2019.

DATA RETENTION

7.11 The following categories of data shall be held for the following retention periods by the respective divisions of Zamara:

DIVISION	SUBCATEGORY OF DATA	RETENTION PERIOD
PENSIONS	Data in relation to Natural Persons: Identity Data: Names of Principal Clients, Secondary Members (in case of annuities), settlors, beneficiaries, guardians, trustees, next of kin of deceased principal/beneficiary.	As may be prescribed in the constitutive agreements with instructing Clients. For the duration of the pension period terminable upon the conferment of the last due benefit to the pensioner or beneficiary as the case may be.
	Birth Certificate/ National ID/ Passport Numbers and KRA Pins.	
	Email Addresses, Telephone contacts and phone numbers	
	Marital Status	
	Permanent Address & Post Office Box Addresses	
	Employment Details including Employer Name, Occupation, Payroll/Staff No, Years of service, Employment dates, Employment confirmation dates Contribution, Salary, source of income and Occupation Details	
	Financial Data: Bank Details including Member Account Balance, Member exit information& Member transfer-in information. Financial information	
	Data in relation to Legal Entities: All information as above with the requisite modifications in respect to the legal nature of the entities such as Corporate Trustees, Custodians, Employers (body corporates, partnerships and companies), Settlors and Beneficiary recipient institutions	
PENSIONS	In relation to natural persons: - Financial/Transactional Data Credit Card Details, bank name, account number, branch, invoice details, assets register (General Insurance), personal health information, policy details (e.g., risk notes, policy documents), utilization report, financial information (bank/m-pesa details), Salary information	As long as the policy subsists.
	Bank Platform username and passwords	

	In relation to legal entities: - Company *itax* passwords	
	Further information that is necessary for Claim reporting purposes, Cover Replacement, Quote seeking, Invoicing, Risk Assessment, Asset Valuation and activities incidental to such.	
HUMAN RESOURCE	CVs of unsuccessful applicants	6 months from date of delivery
	Identity Data of Employees (permanent, contract and interns): within the direct employ of Zamara Name, Contact, Next Kin, Bank details, Citizenship detail, language, academic level, skill set, dependents, Previous conduct of employee in former employment	As long as the employment subsists
	Employee academic & professional certificates	
	Employee disciplinary records (internally generated)	
INSURANCE	In relation to natural persons: - <u>Financial/Transactional Data</u> Credit Card Details, bank name, account number, branch, invoice details, assets register (General Insurance), personal health information, policy details (e.g., risk notes, policy documents), utilization report, financial information (bank/m-pesa details), Salary information	As long as the policy subsists.
	Bank Platform username and passwords	
	In relation to legal entities: - Company *itax* passwords	
	Further information that is necessary for Claim reporting purposes, Cover Replacement, Quote seeking, Invoicing, Risk Assessment, Asset Valuation and activities incidental to such.	

8.0. THE DATA SUBJECT

8.1 The Company recognizes and respect the following rights of the data subject(s).

8.1.1 Right to access to personal information;

8.1.2 Right to information as to whether personal data is being processed;

8.1.3 The right to rectification if the information held is inaccurate or incomplete or requires to be updated;

8.1.4 The right to restrict processing of their Personal Data;

8.1.5 The right to object decisions solely based on automated processing circumstances such as automated processing, publication/ processing of Sensitive Personal Data profiling which produces legal effects or significantly affects Data Subject;

8.1.6 The right to complain (as would be appropriate to the controller, processor or regulator);

8.1.7 The right to object the processing of their data for direct-marketing purposes;

8.1.8 The right to data portability;

8.1.9 The right to be forgotten and hence the right to erasure subject to adherence to any regulatory restrictions on the same;

8.1.10 Right to appropriate security safeguards where personal data is being archived for various purposes;

8.1.11 The right to appropriate security safeguards in cross border transfer of personal data; and

8.1.12 The right of the data subject to withdraw their consent at any time without detriment to their interests.

DATA ACCESS REQUEST AND PROCEDURE

8.2 Zamara has in place mechanism and processes to receive and address complaints and inquiries about its policies and procedures relating to the handling of data including Personal Data;

8.3 The following procedure will govern how Zamara will receive and act on any request made by a Data Subject in relation to their Personal Data held by Zamara;

8.3.1 The access request must be in writing and should contain the details being in the prescribed form as shown in Appendix A

8.3.2 Zamara shall provide a copy of the information comprising personal data of a data subject at minimal cost and within a reasonable time of his/her request

8.3.3 Where additional copies are required, Zamara may procure the same at an additional fee equal to the administrative costs of printing, photocopying or scanning the requested copies of data;

8.3.4 Zamara may disapprove a request for personal data but must provide reasons for denying the request.

8.3.5 Employees in possession of the requested information shall hand over the data without unreasonable delay;

8.3.6 Zamara may employ the necessary measures to verify the identity of the requesting person before handing over any information.

9.0. DATA BREACH

9.1 The following events shall constitute a data breach:

9.1.1 Deletion of digitally stored data;

9.1.2 Destruction of physical files;

9.1.3 Unauthorized access;

9.1.4 Data leaks;

9.1.5 Duplication of data;

9.1.6 Inability to access due to factors relating to technology.

9.2 Where a data breach has been detected, the member of the Data Compliance Team concerned shall institute or cause to be instituted the necessary mitigation measures which may include:

9.2.1 Upon the occurrence of a data breach, the responsible party shall immediately, and not later than 24 hours of the knowledge of such breach, notify their Division Head providing the particulars of the breach.

9.2.2 Thereafter, the Division Head will immediately notify the GCEO, the GCOO and the GH-GRC with details of the breach;

9.2.3 Initiation of backup mechanisms for all personal data;

9.2.4 Conduct risk assessments, and update controls and procedures to mitigate the risk of data breaches

9.2.5 Conduct risk assessments leading to review of guidelines and procedures to mitigate the risk of the related data breach. This constitutes emergency planning under this policy.

9.2.6 Employees working out of station shall ensure that they comply with highest levels of privacy and data protection, in relation to their work.

9.3 Communication of the breach to a data subject shall be done by the DPO within reasonable time and will include measures being taken to rectify an impact caused by the breach.

10.0. ACCOUNTABILITY AND ENFORCEMENT

This policy shall be monitored and implemented in accordance with Zamara's strategic plan and the management shall foster its enforcement.