You're in control

DATA PROTECTION POLICY

MAY 2022

FOR INTERNAL USE

Document Control

Policy version control			
Version #	**Date**	**Approver by**	**Description of change**
1.0	May 26 2022	Board Committee	New policy development
1.1			

Document Location

This document will be published on the company intranet for easy access by all staff.

Document Review and Approval

Prepared by

	Name	Designation	Signature	Date
1	Data Protection Committee	General Manager Operations		29/07/2022
2				

Reviewed by

	Name	Designation	Signature	Date
1	Nixon Shigoli	Managing Director		26/8/2022
2				

BOARD APPROVAL (BY REQUEST OF THE BOARD)

	Name	Designation	Signature	Date
1	Board Committee	Chair – Board Committee		27.08.2022
2				

TABLE OF CONTENTS

1. INTRODUCTION

The Data Protection Act, 2019 is intended to protect individuals from unwanted or harmful uses of personal data so that their personal privacy is protected. It regulates the way in which organisations collect, use, disclose and destroy information about individuals to ensure that they do so in a responsible and accountable manner.

AAR Insurance Kenya (Ltd) ("AIK") collects personal information to effectively carry out its business functions and activities. Such data is collected from employees, customers, suppliers, and includes (but is not limited to) names, telephone numbers, addresses, email addresses, IP addresses, identification numbers, private and confidential information, sensitive information, and bank/credit card details. AIK has developed policies, procedures, controls, and measures to ensure maximum and continued compliance with the data protection law.

2. PURPOSE OF THIS POLICY

This Policy and Procedures Manual is intended to ensure that:

a) All personal data processing carried out by, or on behalf of, AIK complies with the requires of the Data Protection Act, 2019.

b) The personal data rights of customers, staff, intermediaries, suppliers, directors, shareholders, and any other individual are duly protected.

3. SCOPE OF THIS POLICY

This Manual applies to all employees of AIK (meaning permanent, fixed term and temporary employees, any third-party representatives or consultants, agency workers volunteers, and interns and pertains to the processing of personal information.

4. REFERENCES

This Policy should be read in conjunction with the regulations and policies and procedures in force from time to time, including without limitation to AIK's:

a) HR Policy and Procedure Manual
b) IT and communications systems policy.
c) IT acceptable use policy.
d) Data retention and disposal policy
e) Data protection procedures

5. DEFINITIONS

"Consent"	Means any manifestation of express, unequivocal, free, specific, and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the Data Subject.
"Data Controller"	Means an organisation that has full authority to decide how and why personal data is to be processed and has the overall responsibility for the data. This includes deciding on use storage and deletion of the data
"Data Subject"	Means an individual who is the subject of personal data. It includes shareholders, directors, employees, consultants, suppliers, agents

"Data Controller"	A person nominated by the president (with the approval of the national Assembly) to oversee the implementation of and is responsible for the enforcement of the Data Protection Act, 2019.
Data Commissioner	means the Regulator appointed pursuant to the provisions of the Data Protection Act, 2019 and whose main responsibility is to oversee the implementation and enforcement of the Data Protection Act.
"Data Protection Impact Assessment"	This is an assessment done prior to rolling out any new process, system or policy relating to Personal Data that may impact a Data Subject's rights and freedoms. The Data Protection Impact Assessment is described in more detail in Clause 8 of this Policy.
Direct Marketing	Refers to communication by whatever means of any advertising or marketing material, which is directed to individuals, which includes sending a catalogue addressed to a subject through any medium, displaying an advertisement on an online media site a data subject is logged on using their personal data, including data collected by cookies. Relating to a website, it includes the data subject has viewed or sending an electronic message to a data subject about a sale or other advertising material relating to a sale. Using personal data provided by the data subject.
"Data Protection by Design and by Default"	Data protection by design means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. Data Protection by default means that user service setting must be automatically data protection friendly and that only data which is necessary for each specific purpose should be gathered.
"Personal Data"	means information relating to an identified or identifiable individual/person. An identifiable individual is one who can be identified directly or indirectly in particular reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
"Personal Data Breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
"Processing"	Any action taken with personal data. It includes collection, use, storage, disclosure, destruction, or retention of data.
"Sensitive Personal Data"	Means information revealing a person's race, health status, ethnic social origin, conscience, belief, generic data, biometric data, property details, marital status, family details.

6. ROLES AND RESPONSIBILITIES

The board of Directors	▪ The Board of Directors is ultimately responsibility for ensuring that AIK complies with the Data Protection Act. ▪ Board shall exercise oversight to ensure that well designed policies and procedures and adequate risk mitigation practices are in place for the effective management of data protection and privacy obligations ▪ Regularly receive reports from the Data Protection Officer through the ARCC on a quarterly basis and taking necessary decisions required to protect data subjects' privacy.

The chief Executive officer & Executive Management	▪ Design and implement effective internal controls to ensures compliance to data protection laws and data subjects information is protected. ▪ Ensuring that this policy is implemented in letter and spirit. ▪ Provide adequate resources and training to staff for the implementation of this policy. ▪ The data protection officer is informed of any breaches to this policy in time for investigation and remediation
Data Protection officer	The Data Protection Officer (DPO) is responsible for AIK's Day to day compliance with the Data Protection Act. In particular, the Data Protection Officer has the following responsibilities: - ▪ to act as a central authority for the implementation of AIK's Data Privacy Program. ▪ to develop and maintain AIK's Data Protection policy and procedures. ▪ to monitor AIK's compliance with the Data Protection Act 2019 and any other provisions of the law relating to data protection. ▪ to conduct Data Protection Impact Protection Assessments relative to AIK's activities, measures, projects, programs, or systems. ▪ to advise AIK regarding the exercise by Data Subjects of their rights. ▪ to cultivate awareness of privacy and data protection regulations within the Company, including this policy, the Data Protection Act 2019 and its Regulations and any other government issuances on data privacy. ▪ to serve as AIK's contact person vis-à-vis Data Subjects, the Data
Internal Audit	▪ Incorporate compliance testing in their normal audit program. ▪ Report on results of the independent testing to the Board
Employees	Throughout the course of working, AIK employees depending on their roles, may have access to various extract of personal data pertaining to customers, suppliers, directors, shareholders, or any other individuals. An employee is required: a) to abide by and follow the rules and guidelines contained in this Policy and any other data protection policies or rules that may be issued from time to time. b) to access or process personal data only where it is required as part of your role. c) to complete relevant data protection training, appropriate to your role. d) to follow advice, guidance and tools/methods issued from time to time on data protection compliance. e) to identify new systems, processes (including changes to existing processes) contracts, agreements and other activities involving personal data that may require Data Protection Impact Assessments and cooperating with the Data Protection Officer or any advisors to support an assessment and implementation of recommendations to address risks as appropriate. f) when processing personal data on behalf of AIK, to only use it as necessary for your role and not disclosing it unnecessarily or inappropriately. g) to recognise, report internally, and cooperate with any remedial work arising from personal data breaches. h) to recognise, report internally and cooperate with the fulfilment of data subject rights, requests when requested to do so by the Data Protection Officer. i) to ensure that any personal information provided to AIK in connection with

7. DATA PROTECTION PRINCIPLES

All employees of AAR shall apply the following principles when processing personal data: -

7.1 Respect to Privacy; - All personal data processing activities shall be geared towards respecting an individual's right to privacy.

7.2 Lawfulness, fairness, and transparency – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. In this regards: -

a) Lawful: (see section **7.2.1** on lawful grounds)

b) Transparency: - AIK shall provide information to data subjects concerning how their personal data is process by way of privacy policies at the point of collection of the data. AIK shall provide this information in clear and plain language and easily accessible to the data subjects.

c) Fairness: - AIK shall handle person data in a way that the data subject would reasonably expect AIK to. In this regards, shall AIK endeavour to:

i. grant data subjects the highest degree of autonomy with respect to control over their personal data.
ii. enable data subjects to exercise and communicate their rights.
iii. eliminate discrimination against a data subject
iv. guard against the exploitation of the needs or vulnerabilities of a data subject such as a child.
v. incorporate human intervention and to minimise biases that automated decision-making processes may create

7.3 Data Minimisation: - AIK shall process minimum personal data that is adequate, relevant, and limited to what is necessary in relation to the purposes for which the data was collected. The guiding question to an employee is:

a) why do I need this information?
b) how is this data relevant to the processing in question?
c) do i need to pseudonymise/anonymise personal data that is no longer necessary? how can i achieve this?
d) what technologies can we adopt to achieve data minimisation?

7.4 Purpose Limitation: - AIK shall process personal data for explicit, specified, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

- Before AIK processes any personal data, employees shall

a) be clear on why they are collecting personal data and what it shall be used for.
b) communicate or confirm that they have communicated to the data subject, through a privacy policy, the reasons why they need the data.
c) use personal data only for what has been specified/communicated to the data subject.

7.5 Valid Explanations for family information: - AIK shall collect personal data relating to an individual's family or private affairs only where a valid explanation is provided.

7.6 Accuracy: - AIK shall keep an accurate, and where necessary, up to date, personal data records. In this regard, AIK shall: -

a) ensure that any inaccurate record of personal data is erased or rectified.
b) Data subjects shall periodically be reviewed to confirm their data is accurate and up to date.

19. ANNEX A: ACKNOWLEDGEMENT OF RECEIPT AND REVIEW

I, acknowledge that on this day of I received and read a copy of the AIK's Data Protection Policy dated and understand that I am responsible for knowing and abiding by its terms. I understand that the information in this Data Protection Policy is intended to help Company Personnel work together effectively on assigned job responsibilities and assist in the use and protection of Personal Data. I understand that this Data Protection Policy does not set terms or conditions of employment or form part of an employment contract.

Signed .....

Name .....

Date .....