KARIBU HOMES

# DATA BREACH & PRIVACY POLICY

September 2021

## CONFIDENTIALITY INTERNAL

The contents of this document are confidential and the property of KHL (herein after referred to as ***"KHL"***). It contains confidential information that captures KHL'S know-how and expert knowledge. Any reproduction and/or circulation either by electronic or any other means is strictly forbidden without prior approval of KHL. Circulation is strictly restricted to the stated recipients.

# ABBREVIATIONS AND ACRONYMS

| | | |
|---|---|---|
| **AML** | - | Anti-Money Laundering |
| **ARC** | - | Audit Risk Committee |
| **CEO** | - | Chief Executive Officer |
| **CRM** | - | Customer Relationship Management |
| **DBMC** | - | Data Breach Management Committee |
| **DBMP** | - | Data Breach Management Plan |
| **DC** | - | Data Commissioner |
| **DCO** | - | Data Commissioner's Office |
| **DPA** | - | Data Protection Act (No.24 of 2019) |
| **DPIA** | - | Data Protection Impact Assessment |
| **DPO** | - | Data Protection Officer |
| **GDPR** | - | General Data Protection Regulations (EU Standard for Data Protection) |
| **GPS** | - | Global Positioning Systems |
| **HR** | - | Human Resources |
| **ICT** | - | Information Communication Technology |
| **IT** | - | Information Technology |
| **KHL** | - | Karibu Homes Ltd |
| **KYC** | - | Know Your Customer |
| **MD** | - | Managing Director |
| **PEP** | - | Politically Exposed Persons |
| **PPD** | - | Protected Personal Data |
| **QMS** | - | Quality Management System |
| **SMT** | - | Senior Management Team |

# DEFINITION OF KEY TERMS

**Agent:** means any third party that collects and/or uses Personal Information provided by KHL to perform tasks on behalf of and under the instructions of KHL.

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

**Biometric Information:** "Biometric Data", including biometric identifiers and biometric information, means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, regardless of how it is captured, converted, stored, or shared, which is used to identify an individual. Biometric data is considered "sensitive" personal data under the Data Protection Act No.24 of 2019.

**Breach:** "a breach of security leading to the unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed." (See also data security incident or incident)

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

**Consent:** Any freely given specific and informed indication of the wishes of the data subject by which they signify their agreement to personal data relating to them being processed.

**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.

**Critical system:** Any system whose 'failure' could threaten human life, the system's environment or the existence of the organization which operates the system. Such systems include but not limited to electric grid, manufacturing system, transportation system, financial institutions, water treatment facilities and water supply systems.

**Cross-Border Processing**: means either

(a) processing of personal data which takes place in the context of the activities of establishments in more than one country of a controller or processor where the controller or processor has partners, business operations or branches outside Kenya.
(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in Kenya but which substantially affects or is likely to substantially affect data subjects in other countries outside Kenya.

**Data: A**ll data including personal data in electronic or manual form.
**Data Breach**: A data breach relates to the loss of personal data and should be notified following the procedure described.

**Data Breach Management Plan:** A framework which sets out the roles and responsibilities for managing an appropriate response to a data breach as well as describing the steps to be taken by KHL in managing a breach if one occurs.

**Data controller**: A person who either alone or jointly with other persons or in common with other persons or as a legal duty determines the purpose for and the manner in which data is processed or is to be processed. It is responsible for establishing practices and policies in accordance with the Data Protection Act of Kenya. KHL is the Data Controller of all personal data relating to it and used in facilitating real estate development, conducting research and all other purposes connected with its business purposes.

**Data Impact Assessment:** means an assessment of the impact of the envisaged processing operations on the protection of personal data.

**Data Processor**: In relation to personal data, any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

**Data Processing:** Any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties. In brief, it is anything that can be done to personal data from its creation to its destruction, including both creation and destruction.

**Data Protection Focal Point:** In principle, the most senior KHL staff member in a KHL branch office or operation, who assists the data controller in carrying out his or her responsibilities regarding this Policy.

**Data Protection Impact Assessment:** A tool and process for assessing the protection impacts on data subjects in processing their personal data and for identifying remedial actions as necessary in order to avoid or minimize such impacts.

**Data Protection Officer (DPO):** the person appointed as such under the Data Protection Act of Kenya, and in accordance with its requirements. A DPO is responsible for advising the organisation (including its employees) on their obligations under various data protection laws, for monitoring compliance with data protection law, as well as with KHL's polices, and providing advice. He can also be referred to the Data Controller in an organization setting.

**Data Security Incident:** A "Data Security Incident" or "Incident' shall mean an accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication or information resources of KHL (See also Breach or Incident)
**Data Subject:** A Natural person whose personal data is held by the data controller.

**Data Transfer Agreement:** An agreement between KHL and an Implementing Partner or third party that states the terms and conditions of use of personal data, including which data components are to be shared, the mode of transfer, how the data may be used, data security measures and other related issues.

**Disclosure:** Making data available to others outside KHL.

**Encryption**: The process of converting information or data into code, to prevent unauthorised access.

**Filing System:** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

**Implementing Partner:** An organization established as an autonomous and independent entity from KHL that KHL engages through a project partnership agreement to undertake the implementation of strategic or operational or programmatic activities within its mandate.

**Incident:** A "Data Security Incident" or "Incident' shall mean an accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication or information resources of KHL. (See also Breach or Data Security Incident).

**Incident Management:** is the process of handling incidents and breaches in a controlled way ensuring they are dealt with efficiently, with a consistent approach to ensure that any damage is kept to a minimum and the likelihood of recurrence is reduced by measures taken.

**Investigation** — means an investigation relating to:

(a) A breach of this policy;
(b) A contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or
(c) A circumstance or conduct that may result in a remedy or relief being available under any law;

**KHL:** Means Karibu Homes Ltd and all its subsidiaries.

**National Interest** — includes national security, defense, public security, the conduct of international affairs and the financial and economic interest of Kenya;

**Notification:** Notifying the Data Protection Regulator/Data Subject about the data breach.
**Office of the Data Protection Regulator:** An independent public authority established by government to regulate compliance with data protection law by Data Controllers and Processors and take enforcement action in the case of non-compliance. (See also supervisory authority)

**Personal data:** any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. in particular by reference to an identification number, passport number, birth certificate or to one or more specific factors like physical or physiological. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

**Personal Data Breach:** any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data, where that breach results in a risk to the data subject. It can be an act or omission.

**Persons of Concern:** A person whose protection and assistance needs are of interest to KHL. This includes KHL Board of Directors, employees, suppliers, regulators, subsidiaries, partners, service providers, customers, members and all other stakeholders.

**Processing:** Any operation performed on personal data, such as collecting, creating, recording, structuring, organising, 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.

**Profiling**: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.

**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 organisational 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.
**Security Breach**: A security breach relates to the loss of equipment containing personal data.

**Sensitive personal data**: means 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)

**Sites:** For the purpose of this agreement sites means KHL's or any of its subsidiary website

**Supervisory Authority:** means the Office of the Data Commissioner in Kenya created under Section 5 of the DPA No.24 of 2019.

**Systems:** refers to mechanisms and platforms that clients may use to access KHL's services

**Third Party**-Third party, in relation to personal data, means 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.

**Vulnerable Group/ people with incapacity** – 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.

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

As a corporate organization we hold, process and share personal data for many purposes. Every care is taken to protect this personal information from accidental or deliberate misuse, to avoid a data breach that could compromise security and confidentiality.

However, as the amount of data available grows and technology develops, there are new ways by which data can be breached. KHL needs to have in place a robust and systematic process for responding to any reported data breaches, to ensure it can act legally and responsibly, and protect personal data which it processes.

Data security breaches are increasingly common occurrences whether caused through human error or via malicious intent. As the amount of data and information grows and technology develops, there are new ways by which data can be breached. KHL as a responsible corporate organization needs to have in place a robust and systematic process for responding to any reported data security breach, not only to comply with the legal requirements but also to ensure it can act responsibly and protect personal data which it holds.

KHL considers that the new notification requirement has a number of benefits. When notifying the office of the data commissioner (supervisory authority), we as an organization can obtain advice on whether the affected individuals need to be informed. Indeed, the Data Commissioner may also order the KHL to inform the data subjects about the breach. Communicating a breach to data subjects allows KHL to provide information on the risks presented as a result of the breach and the steps those data subjects can take to protect themselves from its potential consequences.

The policy also describes the principles relating to documentation, appropriate reporting internally and externally, and communication so that organizational learning occurs. It establishes responsibility and accountability for all steps in the process of addressing information security incidents that result in data breaches and describes clear roles and responsibilities with the aim of ensuring a comprehensive and well-managed privacy and information governance program.

This policy has been developed in line with the requirements of the Data Protection Act No.24 of 2019 and other international best practice guidelines such as Article 29 Data Protection Working Party- Guidelines on Personal data breach notification under Regulation 2016/679; and the General Data Protection Regulations (GDPR-EU). Hence this Data Breach Policy assists with

a) Meeting KHL's obligations under the Data Protection Act No.24 of 2019 e.g.
    (i) Basic personal data breach notification under DPA No.24 of 2019
    (ii) Notification to Supervisory Authority
    (iii) Communication to Data Subjects
    (iv) Risk Assessment and Higher Risk
    (v) Accountability and Record Keeping
b) Protection of an important business asset — the personal information of KHL's stakeholders, including but not limited to Board of Directors, staff, Shareholders,

suppliers and relevant third-party business and implementation partners — as well as KHL's reputation.

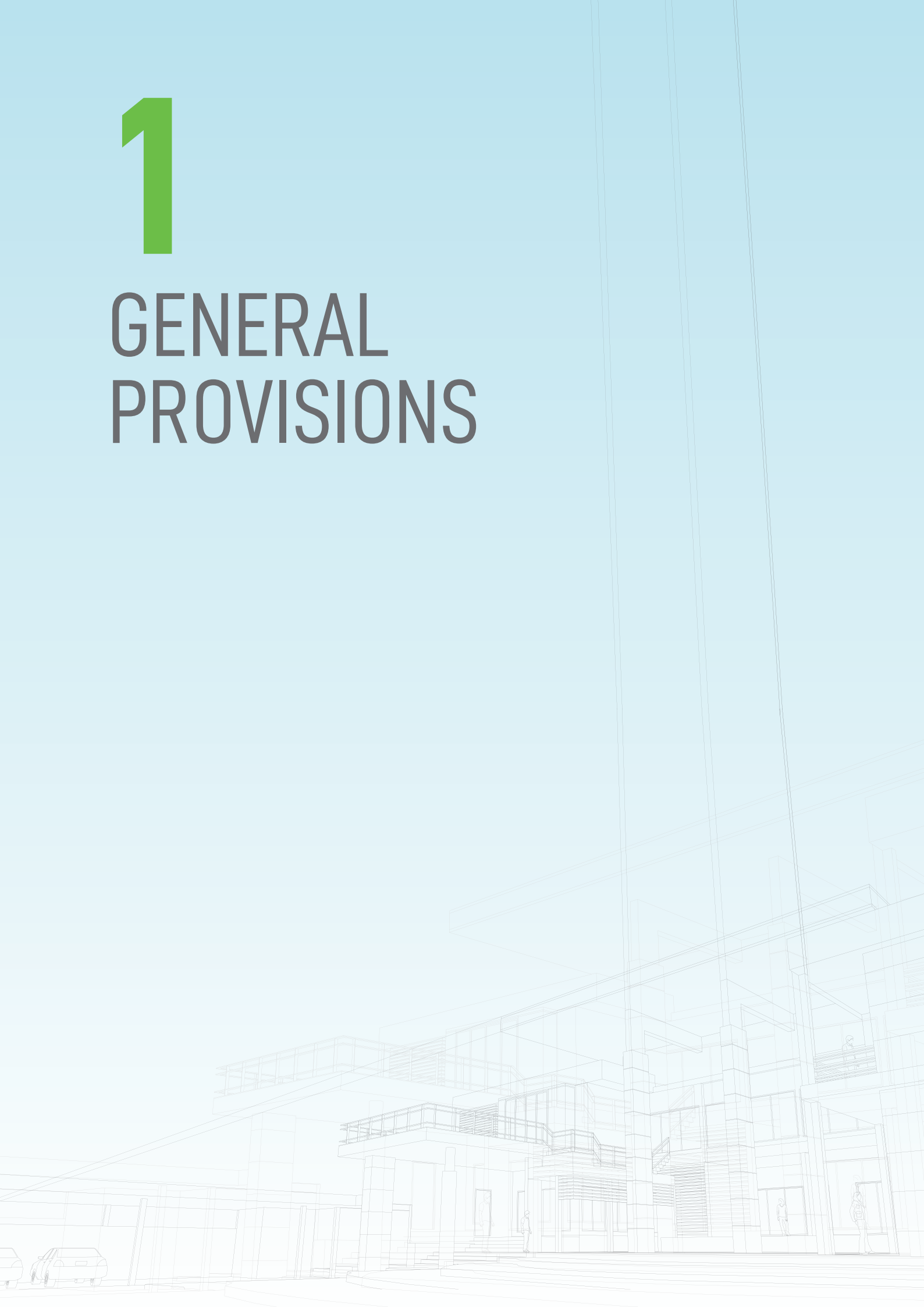
c) Dealing with adverse media or stakeholder attention from a breach or suspected breach.
d) Instilling public confidence by responding to a breach systematically and effectively, with the aim of meeting KHL'S obligations and protecting business and personal assets.

To enhance robust and effective privacy and Information Governance procedures, a Data Breach Management Procedure shall be developed within KHL's quality management framework. KHL takes protection of personal data as a key responsibility as a responsible corporate organization and therefore this policy illustrates our commitment, all employees are required to adhere to this policy.

This is an internal policy with lots of details however 'KHL has developed a data privacy policy which should be available to clients to read and understand how we intend to use and protect privacy and personal data.

# 1

# GENERAL PROVISIONS



## 1.0 INTRODUCTION

Information is a key corporate asset and as such ensuring the continued confidentiality, integrity and availability is essential to support the operations of KHL.

As a corporate organization KHL is also required to operate within the law, specifically the expectations set out in the Data Protection Act No.24 of 2019 and other reference international best practice such as the General Data Protection Regulation (GDPR).

Data security breaches are increasingly common occurrences whether these are caused through human or technical error or via malicious intent. As technology trends change and the volume of data and information created grows, there are more emerging ways by which data can be breached. KHL needs to have in place a robust and systematic process for responding to any reported potential data security breach, to ensure it can act responsibly, protect individual's data, and its organizational corporate information assets and reputation as far as possible.

Data security breaches will vary in impact and risk depending on the content and quantity of data involved, the circumstances of the loss and the speed of response to the incident. By managing all perceived data security breaches in a timely manner, it may be possible to contain and recover the data before it an actual breach occurs, reducing the risks and impact to both individuals and the organization.

Breaches can result in fines for loss of personal information and significant reputational damage, and may require substantial time and resources to rectify the breach. Current fines under the DPA No.24 of 2019 are up to Kenya Shillings Five Million. Breach reporting within 72 hours of identifying a breach is mandatory under the DPA No.24 of 2019, and additional fines can be levied against the organization by the Office of the Data Commissioner for failing to report a breach.

## 1.1 PURPOSE

Data breaches are increasingly common occurrences whether caused through human error or malicious intent. KHL operations rely on the proper use of Confidential Information and Personally Identifiable Information on a daily basis. Managing risk and responding in an organized way to Incidents and Breaches is key to operations and required by the law and the Office of Data Commissioner

The purpose of this policy is to outline the approach KHL takes towards personal data and ensuring the protection thereof and in the event a data protection breach should occur, this policy outlines our approach and steps that will be taken to resolve the breach and prevent a breach from happening again.

KHL must have a robust and systematic process for responding to reported data security Incidents and Breaches. This policy is designed to standardize the organization -wide response to any reported Breach or Incident, and ensure that they are appropriately logged and managed in accordance with best practice guidelines. Standardized processes and procedures help to ensure that KHL can act responsibly, respond effectively, and protect its

information assets to the extent possible. Consequently, a key element this policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner.

The expected results of this policy are to develop an institutional, organizational framework in line with the legal framework to govern the handling of data and privacy breaches of personal data.

## 1.2 AIM OF THE POLICY

The aim of this policy is to standardise the KHL's response to any data breach and ensure that they are appropriately logged and managed in accordance with the law and best practice, so that:

(a) incidents are reported swiftly and can be properly investigated
(b) incidents are dealt with in a timely manner and normal operations restored
(c) Incidents are handled by appropriately authorised and skilled personnel
(d) Appropriate levels of management staff are involved in response management.
(e) the impact of the incident is understood, and action is taken to prevent further damage
(f) incidents are recorded and documented and Evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny.
(g) The incidents are reviewed to identify improvements in policies and procedures
(h) the Office of the Data Commissioner and data subjects are informed as required in more serious cases
(i) incidents are reviewed, and lessons learned

## 1.3 OBJECTIVE OF THE POLICY

The objective of this policy is to enable staff to act promptly to contain any breaches that occur, minimising the risk associated with the breach and to act if necessary to secure personal data and prevent further breaches.

KHL expects its staff to embed security and prevention practices in their normal working day to ensure personal, or special category, data is protected for the purposes of college business and must take appropriate steps to safeguard this information.

## 1.4 RATIONALE

The rationale for having a Data Breach and Privacy policy is based on the legal compliance requirements outlined in the Data Protection Act No.24 of 2019.For example

i) ***Section 41*** of the Act requires corporate institutions to implement appropriate technical and organisational measures which are designed to inter alia to identify reasonably foreseeable internal and external risks to personal data under the person's possession or control; and to establish and maintain appropriate safeguards against the identified risks;

ii) ***Section 43*** of the Act introduces the requirement for a personal data breach (henceforth "breach") to be notified to the competent national supervisory authority (The Office of the Data Commissioner) within 72 hours of the breach;(or in the case of a cross-border breach, to the lead authority) and, in certain cases, to communicate the breach to the data subjects (individuals) whose personal data have been affected by the breach.

iii) ***Section 63 and 65*** of the Act-The focus of this policy is protecting individuals and their personal data. Consequently, breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data. At the same time, it should be noted that failure to report a breach to either an individual or a supervisory authority may mean that under Section 63 and 65 of the Act, a possible sanction is applicable to KHL.

## 1.5 SCOPE

This Data Breach and Privacy policy applies to

a) KHL, its controlled subsidiary Companies (hereinafter "subsidiaries") and its employees and members of the Board of Directors. "Controlled" in this instance means that KHL may enforce the adoption of this policy directly or indirectly, on the basis of its voting majority, majority management representation, or by agreement.
b) All who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personal data or sensitive personal data or corporate data of staff, clients or stakeholders.
c) All data subjects, whether resident in Kenya or not, whose data is or has been collected or processed by KHL and its subsidiaries.
d) Any Personal Data which is processed or controlled by KHL and its subsidiaries in Kenya or outside Kenya such as in cloud computing and hosting.
e) Whether processing takes place within one KHL or its subsidiaries office, between different KHL and its subsidiaries offices in the same or more than one country, or whether personal data is transferred to a strategic business Partners or third parties. The Policy continues to apply even after persons are no longer of concern to KHL or its subsidiaries.
f) This policy sets out the requirements for the procedure of how to treat breach of Personal Data and privacy whether the data occurred in fully or partially automated data, electronic data, manual processing in filing systems or any other form in relation to its employees, corporate data, suppliers, business partners, members,3rd Party and all stakeholders. It also applies where there is a loss of equipment with personal data.
g) This policy shall be the overarching guiding policy in relation to matters of Breach, Privacy, Security and Data Protection.
h) The policy covers all record level and aggregate level data collections within KHL, including those provided for by statute. It includes collections of corporate, financial and workforce information. For the purpose of this policy, a data collection includes both operational data collections and data repositories. Depending on the type and extent of the data breach, management of public relations may be required, including coordinating the timing, content and method of public announcements and similar activities. These activities are outside the scope of this policy, which is limited to the immediate internal responses of business units.
i) The policy does not apply to information that has been classified as Public.

## 1.6 DATA BREACH POLICY STATEMENT

This policy is mandatory to all members of staff and those of subsidiary companies. The policy also sets out mandatory procedures that staff must apply in the event that KHL experiences a data breach or suspects that a data breach has occurred.

All members of staff must familiarise themselves with this policy and comply with its terms. This policy supplements our other policies relating to internet and email use. KHL may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted. Supplemental policies and practices will be developed as needed to meet the legal or departmental requirements. Supplemental policies and practices may provide for more strict or specific privacy and protection standards than are set forth in this Policy.

KHL ***SHALL*** investigate and provide notice of data and/or information security breaches to affected individuals and/or relevant government agencies in accordance with applicable Data Protection Act No.24 of 2019 and other regulatory applicable requirements.

When dealing with personal data breaches or security incidences, KHL and its employees must focus on protecting the individuals and their personal data as well as protecting the interests of the organization.

## 1.7 POLICY DETAILS

KHL respects the privacy of its employees and third parties such as customers, business partners, vendors, service providers, suppliers, former employees and candidates for employment and recognizes the need for appropriate protection and management of Personal Information. KHL is guided by the following principles in Processing Personal Information:

### 1.7.1 Notice

When collecting Personal Information directly from individuals, KHL strives to provide clear and appropriate notice about the:

- Purposes for which it collects and uses their Personal Information,
- Types of non-Agent third parties to which KHL may disclose that information, and
- Choices and means, if any, KHL offers individuals for limiting the use and disclosure of their Personal Information.

### 1.7.2 Choice

Generally, KHL offers individuals a choice regarding how we Process Personal Information, including the opportunity to choose to opt-out of further Processing or, in certain circumstances, to opt-in. However, explicit consent from individuals is not required when Processing Personal Information for:

- Purposes consistent with the purpose for which it was originally collected or subsequently authorized by the individual,
- Purposes necessary to carry out a transaction relationship,
- Purposes necessary to comply with legal requirements, or
- Disclosure to an Agent.

### 1.7.3 Accountability for onward transfer

In regard to the transfer of Personal Information to either an Agent or Processor, KHL strives to take reasonable and appropriate steps to:

- Transfer such Personal Information only for specified purposes and limit the Agent or Processor's use of that information for those specified purposes,
- Obligate the Agent or Processor to provide at least the same level of privacy protection as is required by this Policy,
- Help ensure that the Agent or Processor effectively Processes the Personal Information in a manner consistent with its obligations under this Policy,
- Require the Agent or Processor to notify KHL if the Agent or Processor determines it can no longer meet its obligation to provide the same level of protection as is required by this Policy, and
- Upon notice from the Agent or Processor, take further steps to help stop and remediate any unauthorized Processing.

### 1.7.4 Security

KHL takes reasonable and appropriate measures to protect Personal Information from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the Processing and the nature of the Personal Information.

### 1.7.5 Data integrity and purpose limitation

KHL will only Process Personal Information in a way that is compatible with the purpose for which it has been collected or subsequently authorized by the individual. KHL shall take steps to help ensure that Personal Information is accurate, reliable, current and relevant to its intended use**.**

### 1.7.6 Access

KHL provides individuals with reasonable access to their Personal Information for purposes of correcting, amending or deleting that information where it is inaccurate or has been Processed in violation of the KHL data privacy principles.

**1.7.7 Recourse, Enforcement and Liability**

Violation of this Policy by an employee or contractor of KHL will result in appropriate discipline up to and including termination. Violation by an Agent, Processor or other third party of this Policy or KHL's privacy requirements will result in the exercise of appropriate legal remedies available at law or in equity including termination for material breach of contract.

## 1.8 ADMINISTRATION

This section spells out the roles and responsibilities, implementation and interpretation of this policy.

### 1.8.1 Roles and Responsibilities.

Responsibility for compliance with this Policy rests with the heads of the individual functions, business units and departments together with any individual employees collecting, using or otherwise Processing Personal Information. Business unit, function and department heads, in coordination with the Legal Department, are responsible for implementing further standards, guidelines and procedures that uphold this Policy, and for

assigning day-to-day responsibilities for privacy protection to specific personnel for enforcement and monitoring.

### 1.8.2 Implementation

This Policy is meant to be implemented in conjunction with supplementary data privacy policies. These supplementary data privacy policies will account for differences in data protection requirements by function and will specify individual roles and responsibilities. KHL business units, functions or facilities will implement supplementary data privacy policies as required to be in compliance with applicable laws.

### 1.8.3 Interpretation.

In the event of any conflict between this Policy and any supplemental data privacy policy, this Policy will supersede the supplemental data privacy policy to the extent that the supplemental data privacy policy is less restrictive. Specific procedures may provide for stricter data privacy and protection standards than are set forth in this Policy. In the event that the procedures pertaining data privacy provides for stricter data privacy and protection than this Policy, the procedures will supersede this Policy to the extent necessary to comply with the Data Protection Act No.24 of 2019.

# 2

# DATA PRIVACY POLICY

## 2.0 INTRODUCTION

KHL and its subsidiaries respects data privacy and is committed to protecting personal data.

This Privacy Policy will inform staff, clients and stakeholders as to how KHL and its subsidiaries collects, uses, discloses, transfers and stores personal data when they interact with us and inform clients about their privacy rights and how the law protects them. Since we want to empower stakeholders to make the best decisions about their privacy and personal data, we have made this Privacy Policy as clear and transparent as possible to let the public at large know how the law protects them. It is therefore important that clients and stakeholders are given a condensed version of the Privacy Policy through our websites, to read and understand what we intend to do with their personal data.

KHL is committed to maintaining robust privacy protections for its users. Our Privacy Policy is designed to help the public understand how it collects, uses and safeguards the information you provide and to assist them in making informed decisions when using our services.

## 2.1 IMPORTANT INFORMATION OF WHO WE ARE

KHL and its subsidiaries consist of Four different legal entities which provide various products or services including insurance, ICT solutions, advisory, consultancy, investment solutions and real estate investment solutions. The following are the legal entities in Kenya that form part of the KHL and its subsidiaries and are responsible for your personal data in terms of this Privacy Policy:

| No. | Entity | Contact Details |
|---|---|---|
| 1. | Karibu Homes Ltd | O Suite G, Springette,<br>Lower Kabete Road<br>P.O. Box 40063 - 00100, Nairobi, KENYA<br>Tel: + 254 705 151585<br>Mobile: + 254 705 151515<br>E-mail: frontdesk@karibuhomes.co<br>URL: www.karibuhomes.com |

This Privacy Policy is issued on behalf of the KHL LIMITED so when we mention "**KHL & its Subsidiaries**", **"KHL","we**", "**us**" or "**our**" in this Privacy Policy, we are referring to the relevant company i.e. KHL and its subsidiaries set out above responsible for processing your personal data when you purchase a product or service from us.

### 2.1.1 How to reach us

We have appointed a Data Protection Officer who is responsible for overseeing questions in relation to this Privacy Policy.

If you have any concerns about the use of your personal data, questions about this Privacy Policy including any requests to exercise your legal rights under the law, please contact us using the details set out below:

| No. | Entity | Contact Details |
|---|---|---|
| 1. | Karibu Homes Ltd | O Suite G, Springette,<br>Lower Kabete Road<br>P.O. Box 40063 - 00100, Nairobi, KENYA<br>Tel: + 254 705 151585<br>Mobile: + 254 705 151515<br>E-mail: frontdesk@karibuhomes.co<br>URL: www.karibuhomes.com |

We will respond to your questions or concerns within seven (7) days of receipt of the query.

## 2.2 PROTECTION OF PERSONAL DATA

KHL attaches great importance to the right to privacy and the protection of personal data. We want the public to feel secure that when dealing with KHL, their personal data are in good hands.

KHL protects personal data in accordance with applicable laws and our data privacy policies. In addition, KHL maintains the appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing and/or against accidental loss, alteration, disclosure or access, or accidental or unlawful destruction of or damage thereto.

Only authorized KHL personnel and third-party service providers are provided access to personal data, and these employees and service providers are required to treat this information as confidential. Despite these precautions however, KHL has data breach policy in place in the unfortunate event that there is a data and privacy breach.

## 2.3 HOW WE COLLECT YOUR PERSONAL DATA

We collect personal data of our employees, potential employees, clients, suppliers, business contacts, shareholders and website users. If the data we collect are not listed in this privacy statement, we will give individuals (when required by law) appropriate notice of which other data will be collected and how they will be used.

We also may derive inferences based on the information described above and also collect other information as described in this privacy statement. Where a client provides us with personal information of another person (for instance, a potential employee/referral), they take responsibility for ensuring that such person is made aware of the information contained in this privacy statement and that the person has given his/her consent for sharing the information with KHL.

In summary we may collect personal data directly from the clients and from other people and organisations that we ask to share information about the client. The list below shows you the various ways we may collect personal information:

### 2.3.1 We may collect personal data directly from the Client

In most instances, we collect personal data directly from you when you fill in forms or communicate with us through our contact details. This includes personal data clients provide when they:

- apply for our products or services;
- make enquiries;
- create an account on our website;
- register for our products offered through mobile and online platforms;
- request marketing to be sent to clients
- give us feedback or contact us;
- provide goods or services to us as a supplier or contractor; or
- interact with our website. We collect this personal data by using cookies and similar technologies. KHL has put in place an elaborate cookies and website policy to help clients better understand our privacy commitment.

### 2.3.2 We may collect your personal data from a number of third parties or publicly available sources

In some instances, we will receive personal data from various third parties or publicly available sources including:

- identity and contact data from the Government of Kenya's e-citizen and Integrated Population Registration Services platforms;
- identity and contact data from publicly available sources such as the Companies Registry and the Business Registration Service;
- contact, financial and transaction data from land registries, industry databases such as credit reference agencies, fraud prevention agencies and providers of technical, payment and delivery services;
- medical professionals and hospitals;
- social media;
- if you are a potential candidate for employment with KHL or any of its subsidiaries, we may have received your personal data from third parties such as recruiters or external websites;
- directly from an individual or employer (or your employer's service provider) who has a policy with us under which you are insured;
- directly from an employer which funds a cover that we administer where you are a beneficiary;
- directly from a person who is making a claim or application and they include information about you which is related to their claim or application;
- from family members when they make enquiries about purchasing a product for you or including you on their insurance, when you ask them to make a claim on your behalf, or where you may be incapacitated or otherwise unable to provide information yourself when we need it;
- insurance broker if you have one; or
- third parties who assist us in checking that claims are eligible for payment.

## 2.4 LAWFUL REASON FOR COLLECTING DATA

The law stipulates that personal data can only be processed if there is a lawful and legitimate reason to do so. KHL will only process data lawful in three instances

1. Where the Data Subject has consented – ***Under Section 30 (1) (a) of the DPA.***
2. To perform a contract which the data subject is party to-***Under section 30 (1) (b) (i) of the DPA***
3. To pursue a legitimate interest (commercial) -***Under Section 30 (1) (b) (vii) of the DPA.***

Legitimate interest means that KHL has reasonable grounds to process personal information. Where privacy policy states that we rely on our legitimate interests for a given purpose, we are of the opinion that our legitimate interests are not overridden by client's interests, rights or freedoms, given;

i. the transparency we provide on the processing activity,
ii. our privacy by design approach,
iii. our regular privacy reviews and
iv. the rights you have in relation to the processing activity.

We will also process personal information for the purposes mentioned above based on prior consent, to the extent that such consent is mandatory under applicable laws.

To the extent that visitors are asked to click on/check "I accept", "I agree" or similar buttons/checkboxes/functionalities in relation to a privacy statement, doing so will be considered as providing consent to process personal information, only where such consent is required by mandatory law.

We will not use personal information for purposes that are incompatible with the purposes of which you have been informed, unless it is required or authorized by law, or it is in your own vital interest (e.g. in case of a medical emergency) to do so.

## 2.5 THE TYPES OF DATA THAT WE COLLECT

Personal data means any information relating to an identified or identifiable natural person. The personal data that we collect will depend on the context of our relationship with the client.

The below-mentioned categories of personal data have been obtained either directly from our website users (for example, when you provide information to sign up for a newsletter or register to comment on a forum website) or indirectly from certain third parties (for example, through our website's technology). Such third parties include our affiliates, public authorities, public websites and social media, suppliers and vendors. Except where certain information is required by law or by KHL's policies (including management of an employment relationship with KHL), the decision to provide any personal data to us is voluntary.

### 2.5.1 Type of Data collected - Generally

Generally, we may collect, use, store and transfer different kinds of personal data about you or persons connected to the client which we have grouped together as follows:

i. identification information such as name, date and place of birth, national identity card number, passport number, Kenya Revenue Authority personal identification number (PIN), photo, marital status, title, nationality, gender and specimen signature;
ii. contact information such as email address, postal address, physical address, residential address and telephone number;
iii. financial information such as bank account details, payment card details, mobile money statements, income, credit history, credit worthiness, bank statements, details about payments to or from the client and other details of products and services purchased from us;
iv. information relevant to client's insurance policy or relevant to client's claim or his/her involvement in the matter giving rise to a claim;
v. information about the nature of client's business and commercial assets;
vi. employment information such as the name of the employer, position in the organization and office address;
vii. children's personal data such as the name, date of birth and gender;
viii. sensitive personal information such as marital status, property details, health status and family details (such as next of kin and beneficiaries);
ix. marketing and communications information including preferences in receiving marketing information from us and communication from us;
x. online data whenever clients use our products and services through our website, mobile applications such as cookies, login data, IP address (your computer's internet address), browser type and version, ISP or operating system, domain name, access time, page views, location data, how clients frequently use our online insurance, banking and other services, our mobile applications or visit our website; or
xi. profile data such as username and password, purchases or orders made, interests, preferences, feedback and survey responses.

If we need information about other people connected to the client, we may request the client to provide the information in relation to those people. If the client is providing information about another person, we expect the client to ensure that the concerned party is made aware and are content with their information being provided to us. It might be helpful for clients to show the other party this Privacy Policy and if they have any concerns, please contact us on the same.

### 2.5.2 Types of Data Collected- Specifically, Use and Lawful Basis for use

We collect personal data of our employees, potential employees, clients, suppliers, business contacts, shareholders and website users. If the data we collect are not listed in this privacy statement, we will give individuals (when required by law) appropriate notice of which other data will be collected and how they will be used.

Specifically, we may collect, use, store and transfer different kinds of personal data about you or persons connected to you which we have grouped together as follows:

#### 2.5.2.1 Member and Client Data

When one joins KHL or one of its subsidiaries as a member or a client or subscribes to our Mailing list, we collect business contact data in the form of the following data from you:

i. First and last name
ii. Job title
iii. Company
iv. Work email address
v. Phone number
vi. Area of interest depending on the service you require e.g interest in a project
vii. Nationality
viii. Locality (County, location, sub-location and division)
ix. Next of Kin details (Name, Relationship, Contacts etc).
x. Property information (for mortgage or collateral)

All personal data collected will only be used to process your property purchase application and send client's product information and occasional special offers or announcements from KHL and/or its subsidiaries, if you have subscribed to the KHL's Mailing List. We do not sell personal data to anyone and only share it with third parties who are facilitating the delivery of KHL services. (For example, when you apply for a mortgage we can send the form to your financial services provider for authentication

We rely on the performance of a contract and pursuing a legitimate interest as provided for under section a ***Section 30 (1) (b) (i) and Section 30 (1) (b) (vii) of the Data Protection Act No.24 of 201 of the Data Protection Act No.24 of 2019*** respectively as lawful and legal basis for the processing of members or clients data.

**2.5.2.2 Human Resources Data**
KHL and its subsidiaries is always looking for new employees, and we are always pleased to receive solicited job applications. If one wishes to apply for a position with us, they apply directly through our website. Sometimes hard copy and e-mail resume attachments are also considered.

When one submits their application for employment with KHL or its subsidiaries we process personal data in accordance with applicable personal data regulations. This implies that:
i. The personal data will be treated confidentially
ii. We only use your personal data for recruitment purposes
iii. We do not disclose the personal data, except for the data processors (e.g. if we use a recruitment agency) we use in our recruitment procedure.

KHL and its subsidiaries shall ensure that applicants have expressly authorized personal information to be transmitted to KHL and/or its subsidiaries for position consideration. Access to this personal data is restricted to relevant employees within KHL and/or its subsidiaries only.

KHL and/or its subsidiaries shall store employee details and performance data on its own servers or with security-cleared data processors, who are assisting us with these data management or HR services. Personal data are stored on secure servers in Kenya

Any personal data received from applicants will only be used for the purpose of processing the application and will not be disclosed, except to KHL's security-cleared data processors in connection with the recruitment procedure.

If an applicant is offered employment or in the case of an existing employee of KHL then the following information shall be collected for the purpose of providing you with an employment contract.

a) the name, age, permanent address and sex of the employee;
b) the name of the employer;
c) the job description of the employment;
d) the date of commencement of the employment;
e) the form and duration of the contract;
f) the place of work;
g) the hours of work;
h) the remuneration, scale or rate of remuneration, the method of calculating that remuneration and details of any other benefits;
i) the intervals at which remuneration is paid; and
j) the date on which the employee's period of continuous employment began, considering any employment with a previous employer which counts towards that period; and
k) entitlement to annual leave, including public holidays, and holiday pay (the particulars given being sufficient to enable the employee's entitlement, including any entitlement to accrued holiday pay on the termination of employment, to be precisely calculated);
l) incapacity to work due to sickness or injury, including any provision for sick pay; and
m) pensions and pension schemes;
n) the length of notice which the employee is obliged to give and entitled to receive to terminate his contract of employment;
o) where the employment is not intended to be for an indefinite period, the period for which it is expected to continue or, if it is for a fixed term, the date when it is to end;
p) either the place of work or, where the employee is required or permitted to work at various places, an indication of that place of work and of the address of the employer;
q) any collective agreements which directly affect the terms and conditions of the employment including, where the employer is not a party, the person by whom they were made; and

If an applicant provides Personal information of another person (for instance, a potential employee/referral), it is their responsibility to ensure that such person is made aware of the information contained in this privacy statement and that the person has given you his/her consent for sharing the information with KHL and/or its subsidiaries.

We rely on performance of contract and pursuing a legitimate interest as provided for under Section ***30 (1) (b) (i) and (vii) of the Data Protection Act No.24 of 2019*** respectively, and ***Section 10 (2) and (3) of the Employment Act No.11 of 2007*** as lawful and legal basis for the processing of HR data. Potential employees and existing employees 'data is protected under the constitution under Article 31 and other relevant Privacy and Data Protection Laws, regulations and guidelines.

**2.5.2.3 KHL Exhibitions, Events, Seminars, and Conference Data**

KHL sometimes participates in exhibitions, events and conferences which are open to the public. Members of the public interested in these events provide their corporate information to register for an event. During Conference and event registration, where information is voluntarily provided during event signup, we collect the following information from you:

a) First and last name

b) Job title
c) Company/organization
d) Work e-mail address
e) Phone number
f) Area of interest
g) Locality (County, town etc)
h) Conference or events feedback

KHL events may be photographed and/or video/audio recorded for the purpose of reflecting the events in KHL'S publications and on the KHL's website. We focus our efforts solely on the key note speakers and other voluntary participants from the audience, as well as the audience as a whole.

We rely on legitimate interest as the lawful and legal basis under ***Section 30 (1) (b) (vii) of the Data Protection Act No.24 of 2019*** for the processing of KHL's events and conference data.

**2.5.2.4 Physical Facilities, System and Application access data and Internet and Electronic network activity information.**

For security of our facilities and our systems; there can be places where employees might be required to or be given access credentials some may be biometric (for example as when fingerprint authentication to access some parts of the facility.) or simple access cards, some places in the facility might also be under 24-Hour CCTV surveillance and the footage stored.

Where an employee is provided with access to KHL's systems, KHL may collect information required to access such KHL systems and applications such as System ID, LAN ID, e-mail account, instant messaging account, mainframe ID, system passwords, and internet or other electronic network activity information, including access logs, activity logs, and electronic content produced using KHL systems

We rely on legitimate interest of protecting and securing facilities/systems as the lawful and legal basis under ***Section 30 (1) (b) (vii) of the Data Protection Act No.24*** of 2019 for the processing of KHL's facility and systems access logs collected.

KHL has a comprehensive biometric data privacy policy in place to further safe guard user's privacy rights.

**2.5.2.5 Website Visitors' Data**

In general, website visitors do not need to provide personalized information to KHL. We do collect "aggregate data," that is, group data with no personal identifiers. We use this aggregate data to help us understand how the site is being used and to improve its usability. We also use it to enhance the quality and availability of products and services we offer.

We also, with explicit permission, use aggregate data from online surveys clients choose to fill out for research and publication purposes.

If personal data is provided, and retained, it is only name, business contact email, and business contact phone number, which allow KHL to contact the visitor at his or her organization. KHL solely holds the information and engages in no contact-sharing program with other organizations.

Many websites create Cookies (small text files) when a user visits a website, and these Cookies are used to analyze aggregate user behaviour on a website. In compliance with the ePrivacy international best practice, KHL websites ask permission of the visitor prior to setting Cookies. Should the visitor agree, KHL's server MAY only collect the following information:

i. The visitor's IP address (including the domain name associated with the IP address, i.e. using reverse look-up).
ii. The date and time of the visit to the website.
iii. The pages visited on the website.
iv. The browser being used.

In addition, where this is available, KHL will also collect:

i. The country from which the visitor is accessing the website (only the ending is saved, e.g., de, since this indicates the relevant country).
ii. The language of the browser being used.
iii. The website from which the visitor is accessing the KHL website.
iv. The search word used (if the site is accessed via a search engine)
v. The type of connection and operating system.

We only use this data to improve the visitor's website experience. KHL has a comprehensive website use terms and conditions and cookies policy which visitors can review before using our websites. It is advisable for visitors to review our Website Terms and Condition and Cookie Policy to learn more about how we use Cookies.

When it comes to use our website and use of Cookies, we rely on consent given as the lawful basis under ***Section 28 (2) (c) and Section 30 (1) (a) of the Data Protection Act No.24 of 2019.***

**2.5.2.6 Inquiries**

When one sends an inquiry to us through our contact form, we use the personal data provided in the contact form to answer the inquiry. Any personal data received from will not be used for any other purpose without prior consent and knowledge of the inquirer and will not be disclosed. In some cases, the forms may be printed and retained in hard copy as well. There can be some information that can also be verified from the third party; e.g. your employer or credit details; in such instances the inquirer is responsible for ensuring that such person is made aware of the information contained in this privacy statement and that the person has given you his/her consent for sharing the information with KHL and/or its subsidiaries.

We rely on consent and legitimate interest as the lawful and legal basis under ***Section 30 (1) (a) and 30 (1) (b) (vii) of the Data Protection Act No.24 of 2019*** respectively for the processing your inquiries.

**2.5.2.7 Surveys**

In order to ensure that the services we offer meet clients' requirements, we may ask for feedback in form of surveys and polls. Any feedback received from you will only be used for the purpose of improving our services and will not be disclosed.

We rely on consent as the lawful basis under **Section 30 (1) (a) of the Data Protection Act No.24 of 2019,** for the processing of data in connection with surveys.

**2.5.2.8 Interviews**
Any personal data received from stakeholder's interviews will not be used for any other purpose without prior consent. We rely consent as the lawful basis **under Section 30 (1) (a) of the Data Protection Act No.24 of 2019**, for the processing of data in connection with stakeholders' interviews.

**2.5.2.9 eCommerce**
KHL may use ecommerce portal in a limited way for example to sell some services such as on-going projects. Taking an event as an example; KHL's use of ecommerce is limited to registration for a limited number of projects each year. Individuals within companies provide their corporate information to register for an event. We use the data collected in order to process billing and orders for products/services you choose to purchase on our website.

We rely on fulfilment of contract as the lawful basis under ***Section 30 (1) (b) (ii) of the Data Protection Act No.24 of 2019*** for the processing of eCommerce Data.

## 2.6 HOW DO WE USE PERSONAL DATA?

We will only use personal data when the law allows us. Most commonly, we will use personal data in the following circumstances:

- where we need to perform the contract, we are about to enter into or have entered into with you;
- to assess whether clients are eligible for our products and services;
- where you consent to our use of your personal data;
- where we need to comply with or fulfil legal or regulatory obligations and protecting ourselves and our clients against fraud;
- where we need to protect client's vital interests and the vital interests of third parties (for example when paying out sums to beneficiaries under your policies);
- where it is necessary for our legitimate interests (or those of a third party) such as maintaining our records, developing, assessing and improving our products and services, risk evaluation, underwriting, managing arrangements with reinsurers, managing claims, improving our customer administration and engagement as well as complying with our Know Your Customer (KYC) requirements;
- to establish, exercise or defend our legal rights such as when we are faced with any legal claim or where we want to pursue any legal claims;
- to advertise and market to the public our latest products and services (please note that if someone does not want to receive our marketing information they may opt-out anytime by contacting us at any time);
- to send important notices such as changes to our terms, conditions and policies or unusual activity with respect to any of your accounts with us;
- if one applies for an employment position at KHL or any of its subsidiaries or we note that they are a potential candidate for employment, we may use their personal data in evaluating their candidacy and to contact them about the employment opportunity;
- where we receive personal data from third parties, we may use it to validate the information provided to us or for fraud prevention purposes;
- to enable clients to use the services available through our website and mobile and online applications including registering them for our services and verifying their identity and authority to use our services;

- to address fraud or safety concerns, or to investigate complaints or suspected fraud or illegality;
- to monitor and analyse the use of our products and services for system administration, operation, testing and support purposes;
- to cooperate with, respond to requests from, and to report transactions and/or other activity to, government, tax or regulatory bodies, financial markets, brokers or other intermediaries or counterparties, courts or other third parties;
- to conduct compliance activities such as audit and reporting, assessing and managing risk, maintenance of accounting and tax records, fraud and anti-money laundering (AML) prevention and measures relating to sanctions and anti-terrorism laws and regulations and fighting crime. This includes know your customer (KYC) screening (which involves identity checks and verifying address and contact details), politically exposed persons screening (which involves screening client records against internal and external databases to establish connections to 'politically exposed persons' (PEPs) as part of client due diligence and onboarding) and sanctions screening (which involves the screening of clients and their representatives against published sanctions lists); or
- to record and/or monitor telephone conversations so as to maintain service quality and security, for staff training and fraud monitoring and to deal with complaints, disputes and potential and/or actual criminal activity. To the extent permitted by law, these recordings are our sole property.

Clients have the right to withdraw their consent to our processing of their personal data at any time, however, withdrawal of consent will not affect the lawfulness of our processing which was based on prior consent before your withdrawal or which is based on other legal basis for processing of your personal data. In cases where consent has been withdrawn we will not be able to provide our products and services if you withdraw your consent.

## 2.7 WHAT HAPPENS IF CLIENTS FAIL TO PROVIDE THE REQUESTED PERSONAL DATA?

Where clients do not provide certain information, we may not be able to accomplish some or all of the purposes outlined in this privacy statement, and you may not be able to use certain tools and systems which require the use of such personal data.

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with an insurance policy or to provide you with advisory or training services). In this case, we may have to cancel a product or service the client have with us but we will notify the client if this is the case within reasonable time.

### 2.7.1 How to change personal data

It is important that the personal data we hold about a client is accurate and the most recent. We encourage you to keep us informed in case of any changes of your personal data during your relationship with us. KHL has put in place secure procedures in place to ensure accuracy and data quality is achieved.

## 2.8 SHARING PERSONAL DATA WITH THIRD PARTIES?

We may transfer personal data to our service providers and professional advisors, public and governmental authorities, Accenture companies/affiliates or third parties in connection with KHL's operation of its business, including any (potential) corporate or commercial transaction. Such third parties may be located in other countries.

Before we do so, we shall take the necessary steps to ensure that your personal data will be given adequate protection as required by relevant data privacy laws and KHL's internal policies. KHL may also transfer your personal data to any of its global affiliates/partners.

For example, we may disclose personal information to third parties for other business purposes as follows:

i. We share personal information with third-party service providers that provide services to us, including billing, payment processing, customer service, email deployment, advertising and marketing, security and performance monitoring, maintaining or servicing accounts, processing or fulfilling orders and transactions, verifying customer information, research, data hosting, auditing, and data processing;
ii. To protect and defend the legal rights, safety, and security of KHL , our subsidiaries, affiliates, users, or the public, including to protect against fraud and malicious activity; and
iii. For other business purposes described in this privacy statement or for any other purpose disclosed to you at the time we collect the information or pursuant to your consent.

Subject to client's rights and the applicable laws, we may also share personal data with the third parties set out below:

- entities comprising KHL and its subsidiaries or their affiliates;
- public authorities or governments when required by law, public interest, national security, regulation, legal process or enforceable governmental request;
- our third-party service providers who help us manage our products and services including those service providers who maintain our IT and office systems and provide marketing and advertising services;
- to service providers that provide application processing, fraud monitoring, call centre and/or other customer services, hosting services and other technology and business process outsourcing services;
- persons or entities that the client explicitly request us to transfer your personal data to them;
- relatives, guardians or persons acting on client's behalf where the client is incapacitated or for the purposes of paying out claims to their beneficiaries;
- financial advisers, business partners and third-party administrators who help us manage our products and services;
- banks or financial institutions within the country and outside the country where you either transfer or receive payments from the said banks or financial institutions;
- insurers, reinsurers and brokers who help us manage and underwrite our products and provide us with reinsurance and insurance services;

- our professional advisers such as auditors, tax advisers, insurers, reinsurers, medical agencies, legal advisers who act on our or your behalf, or who represent another third party;
- loss adjusters and claims experts who help us handle claims;
- medical institutions and professionals where we may require to access your health records and assessments for the purpose of arranging or facilitating your claim;
- third parties connected with the sale, transfer or disposal of our business;
- to counterparty banks, payment infrastructure providers and other persons from whom we receive, or to whom we make, payments on our clients' behalf; or
- debt collection agencies, credit reference agencies, fraud detection agencies and other agencies that we will contract to provide services to us.

## 2.9 CROSS-BORDER TRANSFER OF PERSONAL DATA

Where we will make a transfer of personal data outside Kenya, we will ensure that adequate steps are taken to protect your privacy rights and your personal data.
These include:

i. providing proof to the Data Protection Commissioner of the appropriate safeguards taken to protect your personal data;
ii. where personal data is transferred to our affiliates located outside the country, we have entered into agreements governing transfers of personal data with our affiliates to ensure that your personal data receives an adequate and consistent level of protection;
iii. we will only transfer sensitive personal data outside Kenya where we have obtained your consent and on confirmation of appropriate safeguards. Such safeguards may include placing the third party to whom the personal data is transferred under contractual commitments to protect the personal data as well as transferring the personal data to jurisdictions with commensurate levels of protection to ours.

## 2.10 SENSITIVE DATA

"Sensitive personal data" refers to data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.

We do not generally seek to collect sensitive data as defined above through our website, forms or otherwise. In the limited cases where we do seek to collect such data, we will do this in accordance with data privacy law requirements and/or ask for consent.

## 2.11 SECURITY OF PERSONAL DATA

We have put in place appropriate security measures to prevent personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to personal data to those employees, agents, contractors and other third

parties who have a business need to know. They will only process personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

## 2.12 THE RETENTION AND STORAGE OF YOUR PERSONAL DATA

We will retain personal data only for as long as is necessary. We maintain specific records management and retention policies and procedures, so that personal data are deleted after a reasonable time according to the following retention criteria:

i. We retain your data as long as we have an ongoing relationship with you (in particular, if you have an account with us).
ii. We will only keep the data while your account is active or for as long as needed to provide services to you.
iii. We retain your data for as long as needed in order to comply with our global legal and contractual obligations.

As a policy rule we retain your personal data for as long as may be reasonably necessary to fulfil the purpose we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting information.

We may retain your personal data for a longer period if the retention is:

i. required or authorised by law;
ii. reasonably necessary for a lawful purpose;
iii. authorised or consented by you;
iv. is necessary for purposes of responding to a complaint or if we reasonably believe there is a prospect of litigation in respect of our relationship with you; or
v. for historical, statistical, journalistic, literature and art or research purposes.

We have developed a data retention policy which guides us to determine the appropriate retention period for your personal data. Clients are free to request data retention policy by contacting us.

## 2.13 DATA SUBJECTS LEGAL RIGHTS

Data subjects are entitled (in the circumstances and under the conditions, and subject to the exceptions, set out in applicable law) to:

- Request access to the personal data we process about them: this right entitles data subjects to know whether we hold personal data about them and, if we do, to obtain information on and a copy of that personal data.
- Request a rectification of their personal data: this right entitles them to have your personal data be corrected if it is inaccurate or incomplete.
- Object to the processing of their personal data: this right entitles data subjects to request that KHL no longer processes their personal data.
- Request the erasure of data subject's personal data: this right entitles them to request the erasure of their personal data, including where such personal data would no longer be necessary to achieve the purposes.

- Request the restriction of the processing of data subject personal data: this right entitles the data subject to request that KHL only processes their personal data in limited circumstances, including with consent.
- Request portability of data subject's personal data: this right entitles data subject to receive a copy (in a structured, commonly used and machine-readable format) of personal data that the data subject has provided to KHL, or request KHL to transmit such personal data to another data controller.

To the extent that the processing of personal data is based on the data subject's consent, they have the right to withdraw such consent at any time by contacting KHL's Data Protection Officer. Please note that this will not affect KHL's right to process personal data obtained prior to the withdrawal of the consent, or its right to continue parts of the processing based on other legal bases than your consent.

If, despite our commitment and efforts to protect personal data, the data subject still believe that their personal data privacy rights have been violated, we encourage and welcome individuals to come to KHL first to seek resolution of any complaint.

If the complaint is not satisfactorily addressed the data subjects have the right at all times to register a complaint directly with the relevant supervisory authority or to make a claim against KHL with a competent court. Data subjects are welcome to Contact KHL to exercise any of their rights.

## 2.14 UPDATES AND CHANGES TO OUR PRIVACY POLICY

We regularly review our Privacy Policy. This version was last updated on 1st February 2021. Please note however that in case of any changes to the privacy policy, we will inform all our stakeholders of the same. KHL and its subsidiaries has established a mechanism of notifying all our stakeholders of updates to its privacy policy.

We recognize that data protection and privacy is an ongoing responsibility, so we reserve our right to make changes to this Privacy Policy from time to time as we undertake new personal data practices or adopt new privacy policies, etc. If such changes are substantial, we will notify you via email, provided that we have your email address.

KHL reserves the right to change this policy and Terms of Service at any time. We will notify you of significant changes to the Privacy Policy by sending a notice to the primary email address specified in your account or by placing a prominent notice on the site. Significant changes will go into effect 30 days following such notification. Non-material changes or clarifications will take effect immediately. Clients and all our stakeholders should periodically check the Site and this privacy page for updates.

# 3

# WEBSITE & COOKIES PRIVACY POLICY

## 3.0 INTRODUCTION

Global best practice dictates that if you collect any personal information from any website users, such as email addresses, GPS location, phone numbers, or mailing addresses, you are required to have a legal statement available for users to review that discloses the privacy practices of your business.

People care a lot about their privacy, especially when it comes to the use of their personal information online. Most users want to feel secure before providing private information, such as the home address.

A Privacy Policy is not only the legally required document to disclose your practices on protecting personal information, but it's also great way to show users that you can be trusted, and that you have procedures in place to handle their personal information with care.

## 3.1 PURPOSE AND AIM

The purpose of this policy is to offer assurance to our stakeholders who use our website that the information shared is protected by relevant data protection /privacy laws and international best practice.

## 3.2 RATIONALE

The Data Protection Act No.24 of 2019, defines data in very broad terms and includes any data shared or processed by any equipment, machine or system. In this age of internet, a lot of information is shared though web-based systems and the website of an organization is the get way to such systems.

It therefore prudent and best practice to have a policy covering the website and internet. Lastly websites come with various analytic tools offered by third parties and it is important to protect user's data.

## 3.3 SCOPE

This policy applies to data shared in our websites and website links available in KHL and/or its subsidiary websites. This policy also covers terms and conditions for the use of our website and the cookies and other analytics policy.

## 3.4 HOW DO WE USE PERSONAL DATA IN KHL WEBSITE

The following policy gives guidance to which personal data we gather, third party links and programs, how we use the personal data that is collected from the websites and how we use

cookies and other analytics available in websites e.g. CRM (customer relationship management) systems.

### 3.4.1 Personal data collected by websites

KHL collects personal data at its websites in two ways:

1. Directly (for example, when you provide personal data to sign up for a newsletter or register to comment on a forum website); and
2. Indirectly (for example, through our website's technology).

We may collect and process the following personal data:

- Personal data that you provide by filling in forms on our website. This includes registering to use the website, subscribing to services, newsletters and alerts, registering for a conference or requesting a white paper or further information. Pages that collect this type of personal data may provide further information as to why your personal data are needed and how it will be used. It is completely up to you whether you want to provide it.
- If you contact us, we may keep a record of that correspondence.
- We may ask you to complete surveys that we use for research purposes, although you do not have to respond to them.
- Any postings, comments or other content that you upload or post to an KHL website.
- Our website collects personal data about your computer, including (where available) your IP address, operating system and browser type, for system administration, to filter traffic, to look up user domains and to report on statistics.
- Details of your visits to our website, the pages you view and resources you access or download, including but not limited to, traffic data, location data, weblogs and other communication data. KHL has a comprehensive cookies policy which shall be shared to users in our website.

### 3.4.2 Links to websites and programs of third parties

Our websites may include:

- Links to and from the sites of our partner networks, advertisers and affiliates
- Certain programs (widgets and apps) of third parties. Where this is the case, note that such third parties may process your personal data collected through such programs for their own purposes.

KHL does not accept any responsibility or liability for such third parties' sites or programs. KHL shall advise visitors of such third-party sites and programmes to check such third parties' terms of use and privacy statements before using and providing any information to such third parties' sites and programs.

### 3.4.3 KHL use of personal data collected from the websites

KHL uses personal data for legal and legitimate purposes only (see Section 2.7) as well as to provide clients and stakeholders with information they request, process online job applications, and for other purposes that KHL would describe to its clients and stakeholders at the point where it is collected. For example:

- Links to and from the sites of our partner networks, advertisers and affiliates.
- Certain programs (widgets and apps) of third parties. Where this is the case, note that such third parties may process personal data collected through such programs for their own purposes.

- We may analyse IP and browser information to determine what is most effective about our website, to help us identify ways to improve it and make it more effective.

KHL has in place a comprehensive cookies policy which clients and website users can refer to get more guidance and information.

### 3.4.4 How do we use cookies (and other tracking technologies)?

In addition to the information set out above, this section describes how we use cookies and other tracking technologies.

We analyze website user's IP and browser information to determine what is most effective about our website, to help us identify ways to improve it and, eventually, to determine how we can tailor our website to make it a more positive and relevant user experience.

Our Cookies policy is very comprehensive and it has details including for information about client's choices with respect to advertising and social media cookies and for access to our cookie consent manager. By using our website, users agree that we can place cookies and other similar technologies on their devices as explained in our Cookies policy.

### 3.4.5 How do we use personal data for marketing purposes?

In addition to the information set out above, the following sections describe how we use personal data for marketing purposes:

#### 3.4.5.1 What are the sources of marketing data?

The bulk of the personal data we collect and use for marketing purposes relates to individual employees of our clients and other companies with which we have an existing business relationship. We may also obtain contact information from public sources, including content made public at social media websites, to make an initial contact with a relevant individual at a client or other company. Or any one who has visited our website and subscribed to newsletters, questionnaires or other promotional material found in our website

#### 3.4.5.2 Do we send targeted e-mails?

We nay send commercial e-mail to individuals at our client or other companies with whom we want to develop or maintain a business relationship in accordance with applicable laws. Our targeted e-mail messages typically may include web beacons, cookies, and similar technologies that allow us to know whether users have opened, read, or delete the message, and links you may click. When user click a link in a marketing e-mail from KHL, we may also use a cookie to log what pages the user views and what content they download from our websites, this may happen even if the users are not registered at or signed into our site.

Targeted e-mails from KHL may include additional data privacy information, as required by applicable laws. KHL shall put mechanisms in place to seek clients and users consent before sending them marketing e-mails.

#### 3.4.5.3 Do we maintain Customer Relationship Management (CRM) databases?

Like most companies, KHL may use customer relationship management (CRM) database technology to manage and track our marketing efforts. CRM databases may include personal data belonging to individuals at our client and other companies with whom we already have a business relationship or want to develop one.

The personal data used for these purposes includes relevant business information, such as: contact data, publicly available information (e.g. board membership, published articles, press releases, your public posts on social media sites if relevant for business purpose), responses to targeted e-mail (including web activity following links from our e-mails), website activity of registered users of our website, and other business information included by KHL professionals based on their personal interactions with clients.

KHL will put mechanisms in place to inform clients and data subjects whether their information will be stored in a CRM.

**3.4.5.4 Do we combine and analyze personal data?**
We may combine data from publicly available sources, and from our different e-mail, website, and personal interactions with clients or website users (this includes information collected across our different websites such as our careers and corporate sites and information collected when clients/users sign-up or log on to our sites or connect to our sites using social media credentials (such as LinkedIn). We combine this data to better assess clients/users experience with KHL and to perform the other activities described throughout our privacy policy.

**3.4.5.5 What are Data Subjects rights regarding marketing communications?**
Clients and users of KHL websites can exercise their rights as data subjects to prevent marketing communications by opting out through checking certain boxes on the forms we use to collect personal data, or by utilizing opt-out mechanisms in e-mails available every time KHL sends marketing e-mails to clients.

Clients and website users can also exercise the right to discontinue marketing communications or to have their personal data removed from our customer relationship management (CRM) databases at any time by using provided links. In such cases, we will retain minimum personal data to note that the client or user opted out in order to avoid contacting them again.

## 3.5 COOKIES POLICY

The following information may be collected through cookies or similar technology: unique device identifier, mobile device IP address, information about your device's operating system, mobile carrier and your location information (to the extent permissible under applicable law).

### 3.5.1 What are cookies?
Cookies are text files containing small amounts of information which are downloaded to user's computer or mobile device when they visit a site and allow a site to recognize the specific device. Cookies managed by KHL only are called "first party cookies" whereas cookies from third parties are called "third party cookies" as explained below.

### 3.5.2 Why do we use cookies and similar technologies?
Cookies do a lot of different jobs, such as letting you navigate between pages efficiently, remembering preferences and generally improving the user experience. They can also help to ensure that the advertisements users see online are more relevant to their interests. In addition, cookies can help corporate websites to analyze the use of the websites and online

content (analytics cookies) and they can also facilitate/track the interaction on the websites and online content with social media (e.g. links to social media sites, like buttons, etc.).

### 3.5.3 Does KHL use cookies for marketing and analytics?

KHL may use information collected from first party cookies to identify user behavior and to serve content and offers based on user's profile, and for the other purposes described below, to the extent legally permissible in certain jurisdictions.

In other cases, KHL can associate cookie information (including information from cookies placed via our advertisements on third party sites) with an identifiable individual. For example:

- If we send users a targeted email which includes web beacons, cookies or similar technologies we will know whether users open, read, or delete the message.
- When users click a link in a marketing e-mail they receive from KHL, we will also use a cookie to log what pages users view and what content they download from our websites, even if they are not registered at or signed into our site.
- Combining and analyzing personal data – As described above, KHL may combine data from publicly available sources, and from our different e-mail, website, and personal interactions with users (this includes information collected across our different websites such as our careers and corporate sites and information collected when you sign-up or log on to our sites or connect to our sites using your social media credentials (such as LinkedIn). We combine this data to better assess user experience with KHL and to perform the other activities described throughout our privacy policy.

### 3.5.4 Do you use any cookies from third party companies?

Some cookies, web beacons and other tracking and storage technologies that we use are from third party companies (third party cookies), such as Facebook, Google Analytics, Microsoft, Twitter, YouTube, Instagram, and Linkedin Analytics to provide us with web analytics and intelligence about our sites which may also be used to provide measurement services and target ads.

These companies use programming code to collect information about users interaction with our sites, such as the pages users visit, the links they click on and how long they are on our sites. This code is only active while users are on KHL website. This that party cookies also have their own privacy policies which users may familiarize with.

### 3.5.5 Does KHL use any tracking technologies similar to cookies?

KHL may also use web beacons (including conversion pixels) or other technologies for similar purposes as above and we may include these on our sites, in marketing e-mail messages or our newsletter, affiliated websites, to determine whether messages have been opened and links clicked on. Web beacons do not place information on your device, but they may work in conjunction with cookies to monitor website activity. The information provided about cookies also applies to web beacons and similar technologies. Conversion pixels are small codes located on a particular web page which are triggered when someone visits a page resulting in an increase in the conversion count.

### 3.5.6 Opting out of cookies or similar tracking technologies?

Clients and users can adjust their cookie settings through a cookie consent manager. If a user or client wants to remove existing cookies from their device, they can do this using the browser options. Clients and web users can also block future cookies being placed on their

device using the cookies consent manager. However, deleting and blocking cookies may have an impact on user experience.

### 3.5.7 What types of cookies does the site use?

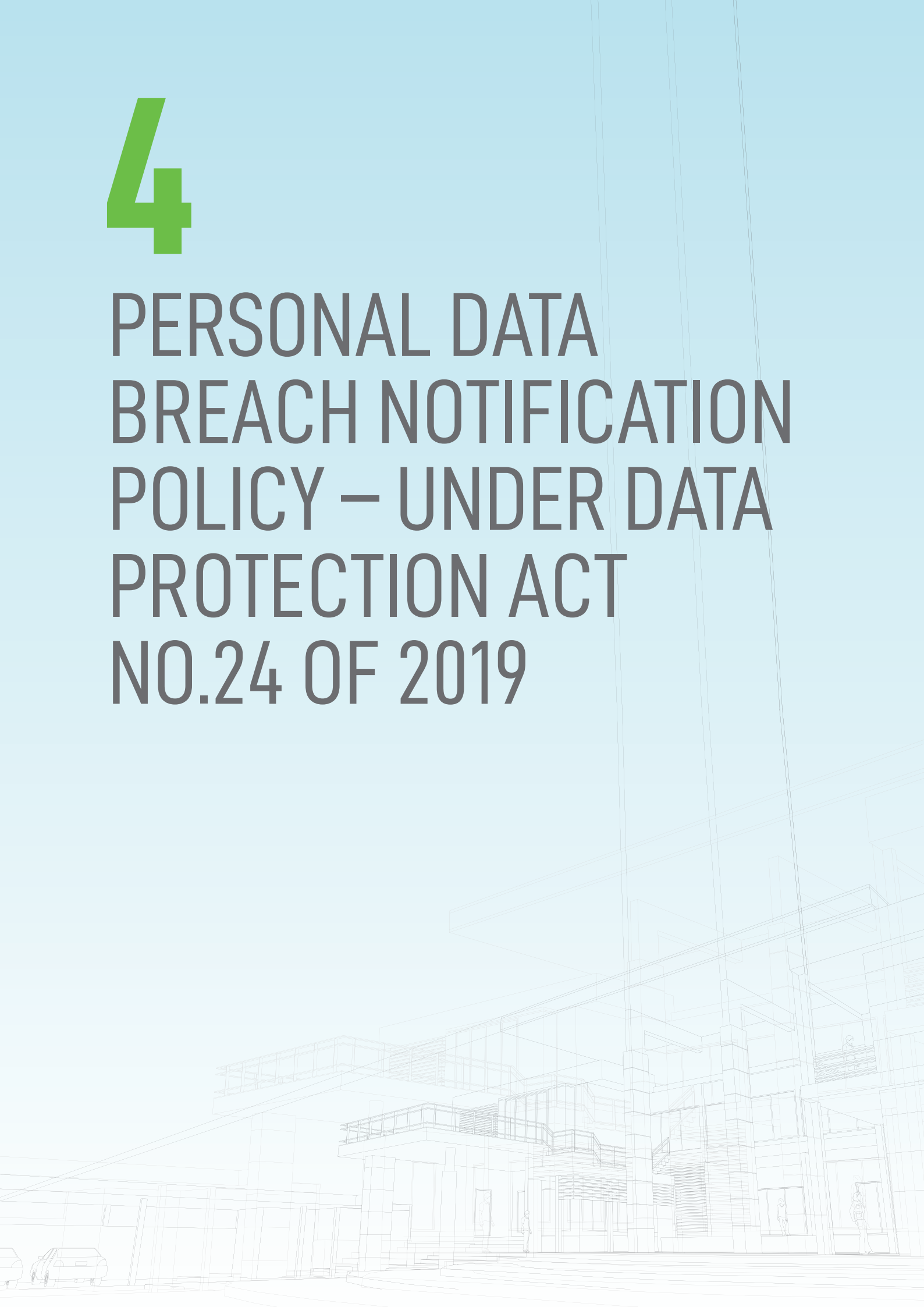
The cookies used on Accenture sites have been categorized as per the table below.

| Category | Description |
|---|---|
| **Strictly Necessary cookies** | These cookies are essential in order to enable users to move around the site and use its features, such as accessing secure areas of the site. Without these cookies, services asked for cannot be provided |
| **First party analytics cookies** | These cookies allow users to employ data analytics so we can measure and improve the performance of our site and provide more relevant content to users.<br><br>These cookies don't collect information that identifies a visitor down to an individual level that is available to us. These cookies are not passing personally identifiable information to any external third party other than in limited cases when we engage a service provider to act on our behalf but who is then unable to use the data for their own purposes. These include, Adobe's Analytics, Target and Audience Manager; Content square and Demand base |
| **Performance cookies** | Performance cookies are generally third-party cookies from vendors we work with or who work on our behalf that collect information about your visit and use of the KHL website, for instance which pages users visit the most often, and if users get error messages from web pages.<br>These cookies don't collect information that identifies a visitor. All information these cookies collect is anonymous and is only used to improve how the website works. Third party vendors may have access to this data and may use it to improve their overall services and offerings. |
| **Functionality cookies** | These cookies allow a site to remember choices users make (such as their username, language or the region you are in) and provide more enhanced, personal features.<br><br>These cookies cannot track user's browsing activity on other websites. They don't gather any information about users that could be used for advertising or remembering where you've been on the Internet outside our site. |
| **Advertising and social media cookies** | Advertising and social media cookies (including web beacons and other tracking and storage technologies) are used to<br>1. Deliver advertisements more relevant to users and their interests;<br>2. Limit the number of times users see an advertisement;<br>3. Help measure the effectiveness of the advertising campaign;<br>4. Retargeting to KHL websites/information and<br>5. Understand people's behavior after they view an advertisement. They are usually placed on behalf of advertising networks with the site operator's permission. They remember that a user has visited a site and quite often they will be linked to site functionality provided by the other organization. This may impact the content and messages you see on other websites you visit. |

KHL will provide together with the web privacy policy a condensed version of the cookies policy and seek users consent before using cookies on their devices.

# 4

# PERSONAL DATA BREACH NOTIFICATION POLICY – UNDER DATA PROTECTION ACT NO.24 OF 2019



## 4.0 INTRODUCTION

The new Data Protection Act No.24 of 2019 (herein after referred to as "DPA" or the "Act"), which was assented on 8th August 2019 and come into effect on 25th November 2019; introduces new legal requirements to corporate organizations on how to handle data breach. A data or privacy breach can be defined as a breach of security leading to the unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

This policy describes the principles for responding to a breach of KHL held data including managing a data breach and notification of persons whose privacy may be affected by the breach. Effective breach management assists KHL in avoiding or reducing possible harm to both the affected individuals and KHL and may prevent future breaches.

This policy also sets out the key legal elements and considerations of responding to a Personal Data breach, principally the obligation to notify Supervisory Authority and/or data subjects in accordance with the law.

## 4.1 PURPOSE AND AIM

KHL must have a robust and systematic process for responding to reported data security Incidents and Breaches. This policy is designed to standardize the KHL organizational -wide response to any reported Breach or Incident, and ensure that they are appropriately logged and managed in accordance with best practice guidelines. Standardized processes and procedures help to ensure the KHL can act responsibly, respond effectively, and protect its information assets to the extent possible. This policy is also in compliance with section 41 and 43 of the Data Protection Act No.24 of 2019

### 4.1.1 Aim of the policy

The aim of this procedure is to standardise KHL's response to any data breach and ensure that they are appropriately logged and managed in accordance with the law and best practice, so that:

- Incidents are reported in a timely manner and can be properly investigated
- Incidents are handled by appropriately authorized and skilled personnel
- Appropriate levels of management are involved in response management
- Incidents are recorded and documented
- Organizational impacts are understood and action is taken to prevent further damage
- Evidence is gathered, recorded, and maintained in a form that will withstand internal and external scrutiny
- External agencies, customers, and data users are informed as required
- Incidents are dealt with in a timely manner and normal operations are restored
- Incidents are reviewed to identify improvements in policies and procedures • the Data Commissioner's office and data subjects are informed as required in more serious cases
- incidents are reviewed, and lessons learned

## 4.2. RATIONALE

Having a data breach response plan is part of establishing robust and effective privacy and information governance procedures, at KHL this is included in the Data Breach Management Procedure. And having clear roles and responsibilities is the foundation to a comprehensive and well-managed privacy and information governance program.

Breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data. At the same time, it should be noted that failure to report a breach to either an individual or a supervisory authority may mean that under Section 63 and 65 of the Data Protection Act No.24 of 2019 of a possible sanction is applicable to KHL by the Data Commissioner and compensation by way of damages to the data subject respectively.

## 4.3 REASONS FOR THE POLICY

This Policy defines the steps that personnel must use to ensure that information security incidents are identified, contained, investigated, and remedied. It also provides a process for documentation, appropriate reporting internally and externally, and communication so that organizational learning occurs. Finally, it establishes responsibility and accountability for all steps in the process of addressing information security incidents.

## 4.4 SCOPE

This policy applies to

- All personal and sensitive personal data processed by KHL or anyone acting on behalf of the KHL.
- Breaches that only affect personal data.
- All persons employed in KHL (including contractors and external agency personnel).
- External organisations and their personnel who have been granted access to KHL Information and Communication Technology (ICT) infrastructure, services and data.
- Data held in any format or medium (paper based or electronic) that has been assigned a classification of protected (internal use) or confidential.
- All record level and aggregate level data collections within KHL, including those provided for by statute. It includes collections of corporate, financial and workforce information. For the purpose of this policy, a data collection includes both operational data collections and data repositories.
- For the purposes of this policy, data security breaches include both confirmed and suspected incidents

### 4.4.1 Applicability of this Policy

This Policy applies to all users of Protected Personal Data (PPD), whether faculty, staff, student, contractor, consultant, or agent thereof. This Policy further applies to any computing or data storing devices owned or leased by the University that experience a Security Incident, as well as any computing or data storing device, regardless of ownership, which is used to store Protected Personal Data, or which, if lost, stolen, or compromised,

and based on its privileged access, could lead to the unauthorized disclosure of Protected Personal Data.

### 4.4.2 Exclusions

This policy has two exclusions worth mentioning

1. Depending on the type and extent of the data breach, management of public relations may be required, including coordinating the timing, content and method of public announcements and similar activities. These activities are outside the scope of this policy, which is limited to the immediate internal responses of business units.
2. The policy does not apply to information that has been classified as Public.

### 4.4.3 Supplemental Policies and Procedures

This Policy sets the minimum standard and shall guide all KHL employees and subsidiaries and agents even if they are not KHL's data processors. Supplemental policies and practices will be developed as needed to meet legal or departmental requirements. Supplemental policies and practices may provide for more strict or specific privacy and protection standards than are set forth in this Policy.

## 4.5 POLICY STATEMENT

---

i) KHL is committed to the protection of all personal data and special category personal data for which we are the data controller.

ii) KHL is committed to protecting the privacy and confidentiality of Personal Information about its employees, customers, business partners and other identifiable individuals.

iii) KHL's policies, guidelines and actions support this commitment to protecting Personal Information.

iv) The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

v) All members of our staff must comply with this policy when processing personal data on our behalf. Each employee therefore bears a personal responsibility for complying with this Policy in the fulfillment of their responsibilities at KHL. Any breach of this policy may result in disciplinary or other action.

### 4.5.1 Training and Induction

The steps to be taken in the event of an actual or suspected breach, including the immediate necessity of informing the DPO or the nominated person, must be included in any introductory briefing on information management and security procedures delivered to all new staff. It must be made clear at this early stage that failure to comply with these requirements may result in disciplinary action.

## 4.6 LEGISLATIVE FRAMEWORK

---

Section 41 of the Data Protection Act No.24 of 2019 requires institutions to implement appropriate technical and organisational measures which are designed-inter alia to

implement the data protection principles in an effective manner; and to integrate necessary safeguards for that purpose into the processing. Section 43 of the
Data Protection Act No.24 of 2019 further states that where personal data has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, a data controller shall—inter alia notify the Data Commissioner and the data subject although the communication to the data subject shall not be required where the data controller or data processor has implemented appropriate security safeguards which may include encryption of affected personal data.(Section 43 (6)).

## 4.7 TERMINOLOGY

Section 2 of the Data Protection Act No.24 of 2019 and Article 4 (12) of the General data protection Regulation ("GDPR") defines a data breach as: "a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

In addition personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. (See Recital No.5 of the General Data Protection Regulations-GDPR)

It is important to note that a potential data breach does not always involve technical systems or IT devices. Breaches can also involve paper-based and verbal information, for example a diary with personal details left in a coffee shop, or inappropriate disclosure of someone's information through conversation.

What is meant by "destruction" of personal data should be quite clear: this is where the data no longer exists, or no longer exists in a form that is of any use to the controller. "Damage" should also be relatively clear: this is where personal data has been altered, corrupted, or is no longer complete. In terms of "loss" of personal data, this should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession. Finally, unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the law.

What should be clear is that a breach is a type of security incident. However, as indicated under Section 2 of the Data Protection Act No.24 of 2019, the law only applies where there is a breach of personal data. This highlights the difference between a security incident and a personal data breach – in essence, whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches. It should also be noted that a security incident is not limited to threat models where an attack is made on an organisation from an external source, but includes incidents from internal processing that breach security principles.

### 4.7.1 Data Security Breach

A data security breach is considered to be any loss of, or unauthorised access to, KHL data, normally involving Personal or Confidential information including intellectual property. Data security breaches include the loss, modification, or theft of data or equipment on which data is stored, inappropriate access controls allowing unauthorised use, human error (e.g. information sent to the incorrect recipient), hacking attacks and 'blagging' where information is obtained by deception.

### 4.7.2 Data Security Incident

A data security incident is where there is the risk of a breach but a loss or unauthorised access has not actually occurred. It is not always clear if an incident has resulted in a breach; by reporting all perceived data breaches quickly, steps can be taken to investigate, secure the information and prevent the incident becoming an actual breach (e.g. by reporting an email IT can remove the email before it has been read and therefore the data has been contained and not been seen by the incorrect recipient)

### 4.7.3 "Near Miss" Incident

A 'near miss' can be described as an unplanned event that did not lead to a data breach but had the potential to. It can also be described as a 'data incident' which requires some investigation to identify whether an actual breach has occurred: the initial investigation may change the status from incident to breach and invoke the full breach investigation procedure.

Near misses should be reported in the same way as breaches, using the procedures below. Once further information is gathered it will be determined whether an incident was a 'near miss' or is escalated as an actual breach.

In any situation where staff are uncertain whether an incident constitutes a full data breach or might be a 'near miss' it should be reported anyway using the procedures below. It is better to report something that can be acknowledged and that we can learn from than not report something that then escalates into a major issue.

## 4.8 CLASSIFICATION OF DATA, INCIDENTS AND BREACHES

Incidents vary in impact and risk depending on a number of mitigating factors including the content and quantity of the data involved. It is critically important that KHL's management respond quickly and identify the data classification of the Incident. This allows staff to respond accordingly in a timely and thorough manner. The purpose of the various classifications is to assist the organization to make an assessment on the cause of action to take after a breach or incident.

Incidents can occur locally, in the cloud, or through third party service providers. Reporting and management of Incidents shall occur similarly. Third party providers shall also be governed by contract terms and liability as defined in their operational agreements.

### 4.8.1 Classification of Data

All reported Incidents shall be classified as below in order to assess risk and approaches to mitigate the situation. Data classification shall refer to the following KHL's data categories:

i) **Public Data** - Information intended for public use or information that can be made public without any negative impact on KHL or its customers. Personal data can never be considered public

ii) **Confidential/Internal Data** - Information of a more sensitive nature to the business and operations of KHL. This data represents basic intellectual capital, applications, and general knowledge. Access shall be limited to only those people that need to know as part of their role within the KHL. Employee, customer and financial information, or other critical information falls within this classification.

iii) **Highly Confidential Data**- Information that, if breached, causes significant damage to KHL's operations, reputation, and/or business continuity. Access to this information should be highly restricted. Organization's Financial Information and other critical information also fall into this classification.

### 4.8.2 Classification of Personal Data Breaches

Breaches can be categorised according to the following three well-known information security principles

i) **"Confidentiality breach"** - where there is an unauthorised or accidental disclosure of, or access to, personal data.

ii) **"Integrity breach"** - where there is an unauthorised or accidental alteration of personal data.

iii) **"Availability breach"** - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

**NB:** It should also be noted that, depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

Whereas determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.

### 4.8.3 Classification of Incidents

i) **Critical/Major Breach or Incident –** Incidents or Breaches in this category deal with Confidential Information or personal data and are on a large scale organizational-wide. All Incidents or Breaches involving client or employee's information will be classified as Critical or Major. They typically have the following attributes:

- Any Incident that has been determined to be a Breach
- Significant Confidential Information or personal data loss, potential for lack of business continuity, KHL exposure, or irreversible consequences are imminent
- Negative media coverage is likely and exposure is high
- Legal or contractual remedies may be required
- Requires significant reporting beyond normal operating procedures
- Any breach of contract that involves the misuse or unauthorized access to personal data by a KHL's Service Contract Provider.

ii) **Moderately Critical/Serious Incident** – Breaches or Incidents in this category typically deal with Confidential Information and are on a medium scale (e.g. less than 50 users on the internal network, application or database related, limited exposure). Incidents in this category typically have the following attributes:

- Risk to KHL is moderate
- Third party service provider and subcontractors may be involved
- Data loss is possible but localized/compartmentalized, potential for limited business continuity losses, and minimized KHL exposure
- Significant user inconvenience is likely
- Service outages are likely while the breach is addressed
- Negative media coverage is possible but exposure is limited
- Disclosure of client or Employee personal data is contained and manageable

iii) **Low Criticality/Minor Incident** – Incidents in this category typically deal with personal or internal data and are on a small or individualized scale (e.g. <10 users on the internal network, personal or mobile device related). Incidents in this category typically have the following attributes:

- Risk to KHL is low
- User inconvenience is likely but not damaging to KHL
- Internal data released but data is not student, employee, or confidential in nature
- Loss of data is totally contained on encrypted hardware
- Incident can be addressed through normal support channels

### 4.8.4 Other criteria of classification

**i) Information Security Breach**

An information security breach is any incident that results in unauthorised access of data, applications, services, networks and/or devices through bypassing their underlying security mechanisms (e.g. firewalls). An information security breach occurs when an individual or an application illegitimately enters a private, confidential or unauthorised information technology perimeter.

An information security breach may also be caused by any software attempts to subvert the confidentiality, integrity or availability of a system and may be the result of external intrusion. The method of intrusion needs to be identified to stop further access and mitigate damage to servers.

Some causes of an information security breach are:

- databases containing personal information being illegally accessed by individuals outside of KHL;
- abuse of privileges in a network environment;
- unauthorised changes to network profiles or access control lists.

**ii) Personal Information Breach**

A breach of personal information is considered to be an incident whereby information has potentially been viewed, shared, stolen, removed, destroyed or used by an individual unauthorised to do so.

A personal information breach occurs when there is unauthorised access or disclosure of KHL information, whether intentional or unintentional. Some causes of a personal information breach are:

- improper handling of classified KHL information
- KHL, its subsidiary or agent or data processor inadvertently providing personal information to the wrong person, for example, sending details out to the wrong address
- an individual deceiving KHL into improperly releasing the personal information of another person
- lost or stolen laptops, removable storage devices or paper records containing personal information
- hard drive and other storage media being disposed without the contents first being erased
- unauthorised publishing of classified information to an uncontrolled environment e.g. internet or social media
- unauthorised access to records or electronic databases
- unauthorised disclosure of information that has the potential to cause an adverse event
- any unforeseen event that has or may affect the ethical acceptability of the use of the personal information provided by KHL.

**iii) Corporate, Financial or Workforce Information Breach**

Corporate, financial or workforce information breach occurs when there is unauthorised access or disclosure of information, whether intentional or unintentional. Some causes of corporate, financial or workforce breach are:

- unauthorised access to human resource systems
- improper handling of staff bank account details or payslip details
- a person inadvertently disclosing staff contact details such as mobile phone number or home address
- unauthorised publishing of budget related information
- unauthorised disclosure of staff professional development documentation or assessment results.

## 4.9 RISK ASSESSMENT

Some data breaches may not lead to risks beyond possible inconvenience to those who need the data to undertake their role. Following immediate containment, the risks must be assessed which may be associated with the breach, potential adverse consequences to the individuals, as well as, the college itself, and the seriousness of the breach must be considered, further to immediate containment.

Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that KHL is able to quickly identify the classification of the data and assess the risk to data subjects or to KHL

For the purposes of this policy data security breaches include both confirmed and suspected incidents. The following must be considered upon discovering a data breach:

- The type of data involved.
- Its sensitivity.

- If data has been lost or stolen, whether data has been protected by encrypted devices or software.
- What has happened to the data, such as the possibility that it may be used to cause harm to the individual(s).
- Who the individuals are, number of individuals involved and the potential effects to those data subject(s).
- Whether there are wider consequences to the breach.
- Whether any actions have been taken during the breach that contravene the policies, procedures and training in place.

## 4.10 CAUSES AND EXAMPLES OF PERSONAL DATA BREACHES AND INCIDENTS

Data breaches can occur for different reasons. They may be caused by employees, parties external to the organisation or computer system errors. Possible ways in which a data breach may occur, and KHL employees should be thoroughly aware of, are:

### 4.10.1 Human error:

- Loss of laptop, phone, data storage devices or paper records containing client and/or personal data;
- Sending client and/or personal data to a wrong e-mail or physical address, or disclosing data to a wrong recipient; (either internally or externally) who does not have a legitimate need to see it;
- Unauthorised access or disclosure of client and/or personal data by employees; e.g. staff accessing or disclosing personal data outside the requirements or authorisation of their job; or verbally
- Sharing of computer ID's and passwords.
- Not updating records when we are notified of a change
- Improper disposal of client and/or personal data (e.g. hard disk, storage media or paper documents containing client and/or personal data sold or discarded before data is properly deleted); Poor disposal of confidential waste;
- paper records containing personal data being left unprotected for anyone to see, for example: -
    - files left out when the owner is away from their desk and at the end of the day;
    - papers not properly disposed of in secure disposal bins that can then be extracted or seen by others;
    - papers left at photocopying machines;

### 4.10.2 Malicious activities:

- Hacking incidents / illegal access to databases containing client and/or personal data; e.g. databases containing personal data being compromised, for example being illegally accessed by individuals outside the KHL; social engineering, phishing or other subversive attacks where information is obtained by deceitful practice.
- Theft of laptop, phone, data storage devices or paper records containing client and/or personal data;

- Scams that trick organisations into releasing client and/or personal data; e.g. 'Blagging' offences where information is obtained by deceiving the organisation that holds it.

### 4.10.3 Computer system error:

- Errors or bugs in the programming code of websites, databases and other software which may be exploited to gain access to personal data stored on computer systems.
- the los Failure of cloud services, cloud computing or cloud storage security / authentication / authorization systems
- loss of personal data due to unforeseen circumstances such as a fire or flood.
- Successful attempts to gain unauthorized access to a KHL's system or client or employee information regardless of where such information is located.
- Equipment failure;
- Inappropriate access controls allowing unauthorised use;
- Unwanted disruption or denial of service
- The unauthorized use of KHL's system for the processing or storage of Confidential Information or Personal Information
- Changes to KHL's system hardware, firmware, or software characteristics without the KHL's knowledge, instruction, or consent.

## 4.11 RESPONSIBILITIES

All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage. But this are the specific roles and responsibilities:

**4.11.1 All staff**

All staff have a responsibility for reporting suspected or actual data breaches as soon as possible. Staff are also responsible for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

**4.11.2 Managers**

Senior managers, managers, departmental heads, unit heads or leadership Team members are responsible for ensuring that staff in their area comply with this policy and assist with investigations as required.

**4.11.3 Data Protection Officer and ICT Manager**

DPO shall be responsible for ensuring any reported breach is investigated, following these procedures. The Data Protection Officer (DPO) will be responsible for overseeing management of data security breaches in line with the Data Security Breach Management Plan; suitable delegation may be appropriate in some circumstances. The DPO shall work with members of the Senior Management Team to respond appropriately to data breach incidents.

The ICT Manager is responsible, along with the DPO for ensuring reported security breaches are investigated, following these procedures, and that appropriate remedial action is taken, where required. Suitable further delegation may be appropriate in some circumstances.

### 4.11.4 Marketing and Communications Manager

Responsible for providing all professional advice in relation to the management of communications in relation to any data breach and for managing all internal and external communications.

### 4.11.5 Data Breach Management Committee

The CEO and the Board may form and constitute a Data Breach Management Committee which will be tasked with coming up with a Data Breach Response Plan for KHL. The membership of such a committee may be drawn from various relevant departments:

Membership of the Data Breach Management Committee may include (but is not limited to):

- Data Protection Officer
- Head of Data Analytics (Or Planning)
- Head of ICT or Information Security Officer.
- Head of Risk Management (Division of Enterprise)
- Head of Customer Service or Delivery
- Head of Legal or Privacy Officer (Legal)
- Head of PR or Head of External Relations or Corporate Communications.
- Head of Digital Marketing

The Committee may be responsible for decisions, in consultation with Data Owners/Processors, regarding notification of individuals who have been impacted in the data breach. The Committee will consider the following factors:

- The risk of harm to the individual/organisation.
- Steps that KHL has taken to date to avoid or remedy any actual or potential harm.
- The ability of the individual/organisation to take further steps to avoid or remedy harm.
- Whether the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual/organisation.
- Whether there are any applicable legislative provisions or contractual obligations that require KHL to notify affected individuals.

## 4.12 DATA BREACH MANAGEMENT PLAN

A Data Breach Management Plan enables KHL to respond quickly to a data breach. It is a framework which sets out the roles and responsibilities for managing an appropriate response to a data breach as well as describing the steps to be taken by KHL in managing a breach if one occurs.

The KHL Data Breach Management Plan is established by the Data Breach Management Committee. Where a data breach is suspected it is required that KHL personnel contact the immediate supervisor or the data protection officer advising of the suspected data breach. The supervisor or Data Protection Officer will inform the committee, the committee will then initiate the Data Breach Management Plan using KHL's Data Breach Response Procedure.

The Data Breach Management Committee shall take appropriate action to handle a data security breach efficiently utilising its data breach management plan which consists of the following elements:

A. **Identification, Reporting and classification**: Where staff who witness a suspected data breach report to either their supervisor or data protection officer who does the initial assessment
B. **Containment and recovery**: where
    i. Action is taken to contain and investigate the breach.
    ii. Action is taken to recover data and limit the damage the breach can cause.
    iii. The police are informed if appropriate
C. **Risk assessment**: where there is an assessment of the ongoing risk and a risk assessment is undertaken of the breach and the potential adverse consequences for individuals concerned to determine next steps necessary further to immediate containment.
D. **Notification of breach:** where Individuals concerned, the Data Commissioner Office (DCO) and third parties are notified of the breach as appropriate depending on the nature of the breach.
E. **Evaluation of the response & recovery to prevent future breaches**: where
    i. The effectiveness of KHL's response to the breach is considered through action planning and monitoring.
    ii. Improvements to existing procedures are identified to enhance data security.

### 4.12.1 Identification, Reporting and Classification

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows KHL to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority of any compliance failures that are material either in their own right or as part of a pattern of failures

The following process shall be followed when responding to a suspected Incident:

A. Confirmed or suspected Incidents shall be reported promptly to the departmental head or directly to the Data Protection Officer. A formal report shall be filed that includes full and accurate details of the Incident including who is reporting the Incident and what classification of data is involved. (KHL in line with the QMS shall develop a data incident reporting forms and procedures for incident reporting). In general, a data incident reporting form shall be comprised of two parts, Part I and II. Part I is to be completed immediately, by the person who discovers or suspects the breach. The following details must be recorded:
    i. the date, time, duration and location of the breach
    ii. how the breach was discovered or is suspected
    iii. description of the incident and the type of data involved in the breach
    iv. the cause and extent of the breach
    v. other staff members that either witnessed the event or were notified at the time of the incident
    vi. an initial breach impact severity rating.

    The Data Protection Officer must complete Part II of the Data Breach Incident Reporting Form by providing the following details:
    i. details of who is affected by the data breach and the estimated number of individuals affected
    ii. a description of the immediate actions taken to contain the breach

iii. details of anyone else notified of the incident and, if so, how and when they were notified
iv. whether any evidence has been preserved
v. if any further investigation is considered necessary
vi. if any steps have been taken to prevent the data breach from occurring again.

NB: Staff who witness data security incidents are advised not to share the incident with fellow staff members to mitigate and limit the level of the breach or further breach. All cases should only be reported to Departmental Head or the Data Protection Officer

B. Once an Incident is reported, the Data Protection Officer shall conduct an initial assessment (See Table 1 Annex B) to establish the severity of the Incident, next steps in response, and potential remedies and solutions. Based on this assessment, the matter shall be passed to the Data Breach Management Committee to determine if this Incident remains an Incident or if it needs to be categorized as a Breach. The DPO assessment shall entail the following
    i. Ascertain if the problem is still ongoing and, if so, take the necessary steps to stop the breach from continuing.
    ii. Make an initial assessment of the extent of the breach.
    iii. Decide, in consultation with the organisation's data breach management committee, who will carry out further investigation of the causes and likely impact of the incident.
    iv. Decide if it is of a level of seriousness that requires notification to the Data Commissioner (is there a risk to people's rights and freedoms?) or the police (has the data been compromised/stolen by a criminal act?).
    v. Establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

C. All Incidents and Breaches will be centrally logged and documented to ensure appropriate documentation, oversight, and consistency in response, management, and reporting. (KHL in line with the QMS shall develop a Data Breach Security Log See Annex C)
D. Once a matter has been reported to the Data Breach Management Committee the committee shall initiate the Data Breach Management Plan described above.

### 4.12.2 Containment and Recovery

All data security incidents or breaches shall have immediate analysis of the Incident and an Incident report completed by the data protection officer or their designee. This analysis shall include a determination of whether this Incident should be characterized as a Breach. This analysis shall be documented and shared with the data breach management committee, the affected parties, and any other relevant stakeholders. Following a reporting of a data security incident, at a minimum, the DPO shall initiate an analysis that will generally involve

a) Identify a member of the Senior Management Team who is independent of the department where the breach occurred to take the lead on investigating the breach.
b) Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise, e.g. isolate or close a compromised section of the network, find a lost piece of equipment or change access codes of doors or IT equipment.
c) Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause, e.g. as well as the physical recovery of

equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.

d) Where appropriate, inform the police.

All actions and decisions should be recorded on the Data Security Breach Management Timeline of Appendix B.

**4.12.2.1 Containment and Recovery Procedure**

KHL will develop a containment and recovery procedure within the wider Data Breach Management procedure in line with the company's QMS. At a minimum the DPO shall do the following within the procedure.

| Step | Action | Notes |
|---|---|---|
| **B** | **Containment and Recovery:** | **Contain the breach, limit further organizational damage, seek to recover/restore data.** |
| 1 | Breach Determination | Determine if the Incident needs to be classified as a Breach. |
| 2 | Ascertain the severity of the Incident or Breach and determine the level of data involved. | See Incident Classification (See Section 4.8.3) |
| 3 | Investigate the Breach or Incident and forward a copy of the Incident report to the Data Breach Management Committee | Ensure investigator has appropriate resources including sufficient time and authority. If Personal Data or confidential data has been breached, also contact the data subject. In the event that the Incident or Breach is severe, KHL'S executive management, general counsel and the Data Commissioner Office shall be contacted |
| 4 | Identify the cause of the Incident or breach and whether the situation has been contained. Ensure that any possibility of further data loss is removed or mitigated as far as possible. If this loss cannot be mitigated, any Incident will be characterized as a Breach. | Compartmentalize and eliminate exposure. Establish what steps can or need to be taken to contain the threat from further data loss. Contact all relevant departments who may be able to assist in this process.<br><br>This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the Incident. |
| 5 | Determine depth and breadth of losses and limit exposure/damages | Can data be physically recovered if damaged through use of backups, restoration or other means? |
| 6 | Notify authorities as appropriate | For criminal activities where property was stolen or fraudulent activity occurred, contact the appropriate authorities and general counsel. Should the Breach involve Personal Data that involves KHL'S Service Contract Provider, notify the CEO and Data Commissioners Office where applicable. |

| Step | Action | Notes |
|---|---|---|
| 7 | Ensure all actions and decisions are logged and recorded as part of incident documentation and reporting. | Complete Incident Report and file with Data Breach Management Committee and Data Commissioners Office where applicable. |

### 4.12.3 Risk Assessment (Continuing Risk)

All Incidents or Breaches shall have a risk and scope analysis completed by the DPO or their designee. This analysis shall be documented and shared with the Data Breach Management Committee, the affected parties, and any other relevant stakeholders.

The DPO while carrying out the investigation into a data breach will, within the first 24 hours (if possible), carry out an initial assessment of the extent of potential harm. This will focus on:

- the type of data involved and its level of sensitivity
- the volume of data stolen, copied or compromised
- the number of data subjects involved (that is, the persons affected or likely to be affected)
- the individuals/organisations that carried out the breach (if known)
- the extent to which the files involved were encrypted or password-protected.

Knowing the risks and impact of data breaches will help KHL determine whether there could be serious consequences to affected individuals, as well as the steps necessary to notify the individuals affected.

#### 4.12.3.1 Risk and Impact on Individuals

- How many people were affected? -A higher number may not mean a higher risk, but assessing this helps overall risk assessment.
- Whose personal data had been breached? -Does the personal data belong to employees, customers, or minors? Different people will face varying levels of risk as a result of a loss of personal data.
- What types of personal data were involved? This will help to ascertain if there are risk to reputation, identity theft, safety and/or financial loss of affected individuals.
- Any additional measures in place to minimize the impact of a data breach? e.g.: a lost device protected by a strong password or encryption could reduce the impact of a data breach.

#### 4.12.3.2 Risk and Impact on organizations

- What caused the data breach? -Determining how the breach occurred (through theft, accident, unauthorized access, etc.) will help identify immediate steps to take to contain the breach and restore public confidence in a product or service.
- When and how often did the breach occur? -Examining this will help KHL better understand the nature of the breach (e.g. malicious or accidental).
- Who might gain access to the compromised personal data? -This will ascertain how the compromised data could be used. In particular, affected individuals must be notified if personal data is acquired by an unauthorized person.
- Will compromised data affect transactions with any other third parties? -Determining this will help identify if other organizations need to be notified.

At a minimum, the DPO shall:

| Step | Action | Notes |
|---|---|---|
| **C** | **Risk Assessment** | **Identify and assess ongoing risks that may be associated with the Incident or Breach.** |
| 1 | Determine the type and breadth of the Incident or Breach | Classify Incident or Breach type, data compromised, and extent of breach |
| 2 | Review data sensitivity | Determine the confidentiality, scope and extent of the Incident or Breach. |
| 3 | Understand the current status of the compromised data | If data has been stolen, could it be used for purposes that harm the individuals whose identity has been compromised; If identity theft is involved, this poses a different type and level of risk. |
| 4 | Document risk limiting processes or technology components that contain and manage the Incident | Does encryption of data/device help to limit risk of exposure? |
| 5 | Determine what technologies or processes will mitigate the loss and restore service | Are there backups of the compromised data? Can they be restored to a ready state? |
| 6 | Identify and document the scope, number of users affected, and depth of Incident or Breach | How many individuals' personally identifiable information were affected? |
| 7 | Define individuals and roles whose data was compromised | Identify all students, staff, districts, customers or vendors involved in the Incident or Breach |
| 8 | If exploited, what will the compromised data tell a third party about the individual? Could it be misused? | Confidential Information or Personal Information could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a criminal build up a detailed picture associated with identity theft or fraud. |
| 9 | Determine actual or potential harm that could come to any individuals | Identify risks to individuals:<br>• Physical Safety<br>• Emotional Wellbeing<br>• Personal or Business Reputation<br>• Financial Implications<br>• Identity Concerns<br>A combination of these and other private aspects of their life? |
| 10 | Are there wider consequences to consider? | Is there risk to another organization, the government, or loss of public confidence? |
| 11 | Are there others who might provide support or advise on risks/courses of action? | Contact relevant service providers, agencies, or companies impacted by the breached data, notify them about the Incident, and ask for assistance in limiting the scope of the Incident. |

The lead investigating the data security breach shall undertake a risk assessment associated with the breach to assess potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen. KHL in line with the internal QMS shall develop risk assessment tools. A sample Appendix D shall be used to carry out this assessment and to record their findings.

### 4.12.4 Notifications of Data Breach and Incident Communication.

Each security Incident or Breach determined to be "moderately critical" or "critical" shall have communication plans documented by the Data Breach Management Committee, senior leadership, and their designees to appropriately manage the Incident and communicate progress on its resolution to all effected stakeholders.

When deciding whether a breach is sufficiently serious to be notified to the data subject and the Data Commissioner's Office, the following points should be borne in mind.

- Is there a high risk of it adversely affecting the rights of data subjects?
- Would notification enable them or others on their behalf to take mitigating action?
- Would notification help to prevent the unauthorised or unlawful use of the data concerned?
- Does this organisation have a contractual duty to take such action?

[Note: Not all breaches will merit being reported to the authorities, but in all cases the persons affected should be informed of how and when the breach occurred, what has been done to correct the situation and what they may wish to do to further safeguard themselves. A contact within the organisation must be provided so that those affected have access to further information.]

The DPO and lead investigating the data security breach shall determine whether data subjects or other organisations should be informed of the breach to enable those whose data has been compromised to take steps to protect themselves, to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints using the Notification of a Data Breach Checklist (Appendix E) to determine this.

If the risk to individuals' rights and freedoms is unlikely, the breach does not have to be reported to the individual or the Data Commissioner's Office but shall still be documented in the Personal Data Security Breach Log (Appendix C) by the DPO.

**NB: Under no circumstance is any member of staff do the notification. Only the DPO after consultation with the Data Breach Management Committee is allowed to issue notification. Secondly all decision to notify or not to notify an individual, the data commission or third party shall be documented and logged in for future evidence. Lastly as part of the QMS KHL will develop notification templates.**

At a minimum, the DPO shall:

| Step | Action | Notes |
|---|---|---|
| **D** | **Notification and Communications** | **Notification enables affected stakeholders to take precautionary steps and allow regulatory bodies to act on the Incident or Breach.** |
| 1 | Are there legal, contractual or regulatory notification | Review vendor contracts and compliance terms, assure government reporting and notifications are understood. |

| Step | Action | Notes |
|---|---|---|
| | requirements associated with the Incident or Breach? | Contact legal department as necessary to begin contractual adherence. Should the Breach include Personal Data or Sensitive Personal Data initiate the Data Breach Management Committee hearing process. |
| 2 | Notify impacted individuals of Incident or Breach remedies. | Provide individuals involved in the Incident or Breach with mitigation strategies to re-secure data (e.g. change user id and/or passwords etc.) |
| 3 | Determine Internal Communication Plans | Work with senior leadership and provide regular internal updates on status of Incident or Breach, remedies underway, and current exposure and containment strategies.This messaging should be provided to all internal stakeholders and management. Messaging shall be coordinated through the CEO office in conjunction with the Data Breach Management Committee |
| 4 | Determine Public Messaging | Prepare and execute a communication and follow-up plan with Data Breach Management Committee and senior leadership. Communication strategies need to define audience(s), frequency, messaging, and content. |
| 5 | Execute Messaging Plan | Working through the Data Breach Management Committee and appropriate senior management leadership, execute the public and internal communication plans. Depending on the nature and scope of the Incident or Breach, multiple messages may need to be delivered as well as press and public communiques. Minimally notifications should include:<br>• A description of the Incident or Breach (how and when it occurred)<br>• What data was involved and whose data was compromised<br>• Details of what has been done to respond to the Incident or Breach and any associated risks posed<br>• Next-steps for stakeholders<br>• KHL or DPO's contacts for the Incident or Breach, any follow-, and other pertinent information<br>• When notifying individuals, provide specific and clear advice on the steps they can take to protect themselves and what KHL and/or third-party vendor will do to help minimize their exposure<br>Provide a way in which they can contact KHL or DPO for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page). |

#### 4.12.4.1 Notifications to Individual/s Affected (Data Subject/s)

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, they shall be informed without undue delay. KHL is legally required to notify affected individuals if their personal data has been breached. This will encourage individuals to take preventive measures to reduce the impact of the data breach, and also help KHL rebuild consumer trust

This shall normally by the responsibility of the DPO who shall provide individuals affected with the following information using the Notification of a Data Breach template provided in Appendix F:

- The name and contact details of the DPO or other contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

The DPFIO shall record this in the Personal Data Security Breach Log (Appendix C).

At a minimum the DPO shall be guided as follows:

**a) Who to Notify:**

- Notify individuals whose personal data have been compromised.
- Notify other third parties such as banks, credit card companies or the police, where relevant.
- Notify Data Commissioner's Office especially if a data breach involves sensitive personal data.
- The relevant authorities (e.g.: police) should be notified if criminal activity is suspected and evidence for investigation should be preserved (e.g.: hacking, theft or unauthorized system access by an employee.)

**b) When to Notify:**

- Notify affected individuals immediately if a data breach involves sensitive personal data. This allows them to take necessary actions early to avoid potential abuse of the compromised data.
- Notify affected individuals when the data breach is resolved

**c) How to Notify:**

- Use the most effective ways to reach out to affected individuals, taking into consideration the urgency of the situation and number of individuals affected (e.g. media releases, social media, mobile messaging, SMS, e-mails, telephone calls).
- Notifications should be simple to understand, specific, and provide clear instructions on what individuals can do to protect themselves.

**d) What to Notify:**

- How and when the data breach occurred, and the types of personal data involved in the data breach.
- What KHL has done or will be doing in response to the risks brought about by the data breach.
- Specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused.

- Contact details and how affected individuals can reach the organization for further information or assistance (e.g. helpline numbers, e-mail addresses or website).

**4.12.4.1.1 Data Breaches Received as Complaints from Individuals**

There are occasions when a data subject may make KHL aware of a data breach by using the KHL's complaints procedure. If this is the case, the Head of Customer Service will forward the complaint to the Data Protection Officer to be dealt with as a data breach.

The complainant will receive acknowledgement from the KHL informing them that this will be handled in line with the KHL's Breach Reporting Procedure. The data protection officer inbox will be copied into all communications with the complainant. The complaint will be sent to the DPO and this will not be counted in the complaint reporting process.

**4.12.4.1.2 The Danger of Notifying too many Individuals**

There will be data security incidents in which a large number of individuals will need to be notified. However, there will be other incidents in which notifying a large number of individuals may have the potential to cause disproportionate enquiries. The DPO and the Data Breach Management Committee should always balance the method of notification and the people to be notified against the business interest and reputation of KHL.

Whenever we notify an individual whose personal data has been affected by an incident or breach, that notification must include a description of when the breach occurred, how the breach occurred and what data was involved. Notifications must also include explicit guidance concerning what said individual can do to protect themselves. We should also outline to concerned individuals what steps our company has already taken to mitigate risks.

**4.12.4.2 Notifying the Data Commissioner's Office**

Unless the breach is unlikely to impact on data subjects or result in a risk to the rights and freedoms of individuals, we must notify the breach to the Data Commissioner's Office within 72 hours of becoming aware of the breach. (See Section 43 (1) (a) of the Data Protection Act No.24 of 2019).

We must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms. The content of the notification will be drafted by our DPO, and any notification to the DCO must only be made by the DPO.

The DPO and the Data Breach Management Committee shall make the determination of who needs to be notified of the breach. At a minimum

i) Ultimately, the DPO will decide whether the DCO should be notified of the breach within the required 72 hours
ii) Use of the Risk matrix (See Section 4.8.3) will help determine the risk to people's rights and freedoms and will aid the decision to notify the DCO (and the data subject(s)).
iii) Every incident will be assessed on a case by case basis, considering:
    - Whether there are any legal/contractual notification requirements
    - Whether notification would assist the individual affected – could they act on the information to mitigate risks?
    - Whether notification would help prevent the unauthorised or unlawful use of personal data?
    - Would notification help KHL meet its obligations under the data protection principles?

- The dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

iv) The DPO will need to keep the DCO up to date about the data breach. If anything changes from the time the initial notification to the DCO was sent, the DPO will consider whether there is need to update the DCO about the data breach.

When deciding whether a breach is sufficiently serious to be notified to the DCO, the following points should be borne in mind.

- Is there a high risk of it adversely affecting the rights of data subjects?
- Would notification enable them or others on their behalf to take mitigating action?
- Would notification help to prevent the unauthorised or unlawful use of the data concerned?
- Does this organisation have a contractual duty to take such action?

[Note: Not all breaches will merit being reported to the authorities, but in all cases the persons affected should be informed of how and when the breach occurred, what has been done to correct the situation and what they may wish to do to further safeguard themselves. A contact within the KHL must be provided so that those affected have access to further information.]

If it is decided that a serious breach has occurred that must be reported to the DCO, the following information will be made available.

- A description of the nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of the DPO or the person chosen to liaise with the authorities.
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

[Note: It is accepted that KHL may not be able to carry out all the necessary checks, or to supply all the required information, within the laid-down legal requirement 72-hour period. It is important, however, that initial contact is made within that period, even if it is only to explain why there will be a delay in supplying full details. In this event, KHL should emphasise that it has made dealing with the breach a priority and is devoting all possible resources to the investigation.]

[Note: The Data Commissioner's Office may provide further guidelines on the procedures to be followed for the purpose of notification to either Data Subjects or The Commissioner's office if this is the case then KHL shall amend the policy and procedures to adhere to the guidelines issued by DCO]

**4.12.4.3 Notifying other Relevant Third Parties**

KHL may also consider that it is necessary to notify other third parties about the data breach depending on the nature of the breach for example this would be appropriate where illegal activity is known or believed to have occurred, or there is a risk of illegal activity happening in the future. The parties to be notified could include:

- Regulators
- Other government agencies

- Media
- Insurers
- Police
- Employees
- Sponsors
- Banks
- Contract counterparties.

The decision as to whether any third parties need to be notified will be made by our DPO, Data Breach Management Committee and senior management. They will decide on the content of such notifications and act within 5 days of becoming aware of the data breach; save for notification to the media and general public where marketing and communications department must be involved in the notification drafting.

### 4.12.5 Evaluation & Monitoring (Responses Post-Mortem)

The key to preventing further incidents is to ensure that KHL learns from previous incidents. It is extremely important to identify the actions that KHL needs to take to prevent a recurrence of the incident. The DPO, The Data Breach Management Committee and other members of the Senior Leadership Team will carry out an evaluation as to the effectiveness of KHL's response to the data breach and document this in our Data Breach Register. Senior management may then make changes to college procedures to minimise the likelihood of incidents occurring again.

After the data breach or data security incident has been contained by carrying out all necessary measures, KHL will conduct an extensive review of the causes of the breach, the effectiveness of the response and determine whether any changes to systems, policies or procedures should be made detailing:

- The cause(s) of the breach
- The effectiveness of any responses.
- Whether changes to existing IT systems, company procedures or policies must be implemented.
- Where and how personal data is held and where and how it is stored.
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures.
- Whether methods of transmission are secure; sharing minimum amount of data necessary.
- Identifying weak points within existing security measures.
- Staff awareness.
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches.
- If deemed necessary the Data Breach Incident Report recommending any actions or changes to systems, policies and procedures shall be considered and monitored by Data Breach Management Committee, KHL's Senior Management Team, Audit & Risk Committee and in more serious cases it may be appropriate to report to the KHL's Board or appropriate Committee.

Without limiting the generality mentioned above the following more specific and strategic issues should be considered while doing an evaluation review to a serious data breach

a) **Operational and Policy Related Issues:**
   - Were audits regularly conducted on both physical and IT-related security measures?
   - Are there processes that can be streamlined or introduced to limit the damage if future breaches happen or to prevent a relapse?
   - Were there weaknesses in existing security measures such as the use of outdated software and protection measures, or weaknesses in the use of portable storage devices, networking, or connectivity to the Internet?
   - Were the methods for accessing and transmitting personal data sufficiently secure, e.g.: access limited to authorized personnel only?
   - Should support services from external parties be enhanced, such as vendors and partners, to better protect personal data?
   - Were the responsibilities of vendors and partners clearly defined in relation to the handling of personal data?
   - Is there a need to develop new data-breach scenarios?

b) **Resource Related Issues:**
   - Were sufficient resources allocated to manage the data breach?
   - Should external resources be engaged to better manage such incidents?
   - Were key personnel given sufficient resources to manage the incident?

c) **Employee Related Issues:**
   - Were employees aware of security related issues?
   - Was training provided on personal data protection matters and incident management skills?
   - Were employees informed of the data breach and the learning points from the incident?

d) **Management Related Issues:**
   - How was management involved in the management of the data breach?
   - Was there a clear line of responsibility and communication during the management of the data breach?

All existing protocols must be reviewed to analyse their adequacy. Any necessary amendments to protocols must be identified and carried out as soon as possible. The DPO shall review any recommended actions to enhance information security and liaise with the appropriate staff members to discuss and implement these actions as appropriate.

In summary each Incident or Breach determined to be "moderately critical" or "critical" shall have a post mortem analysis completed by the DPO and the Data Breach Management Committee and their designees to appropriately document, analyze, and make recommendations on ways to limit risk and exposure in the future.

At a minimum, the DPO and the Data Breach Management Committee shall:

| Step | Action | Notes |
|---|---|---|
| **E** | **Evaluation and Response** | **To evaluate the effectiveness of the University's response to the Incident or Breach.** |
| 1 | Establish where any present or future risks lie. | Assess and evaluate the root causes of the Incident or Breach and any ways to mitigate and/or prevent a similar occurrence. |

| | | |
|---|---|---|
| 2 | Consider the data and security measures employed. | Evaluate, analyze, and document the use cases and technical components of the Incident or Breach. Document areas for improvement in environment, technology, or approach that limit future security exposures. Make recommendations as appropriate. |
| 3 | Evaluate and identify areas of weakness in existing security measures and procedures. | Document lapses in process, procedure, or policy that may have caused the Incident or Breach. Analyze and document solutions and remedies to reduce future risks. |
| 4 | Evaluate and identify areas of weakness related to employee skills. | Assess employee readiness, education, and training. Document and plan for updates in education or procedural changes to eliminate potential for future Incidents. |
| 5 | Report on findings and implement recommendations. | Prepare report and presentation to KHL's Senior Leadership Team or in some cases the Board for major Incidents or Breaches. |

An activity log recording the timeline of Incident management shall also be completed. Reporting and documentation shall be filed and managed through the office of the DPO.

### 4.12.6 Records and Retention (Further Action)

Throughout the breach management process a record should be kept of actions taken and by whom. An activity log recording the timeline of the incident management will also be completed. Appendix 4 provides an activity log template to record this information. Copies of any correspondence relating to the breach should also be retained.

During the aftermath of a breach, in the reporting and investigation stages, the required information should not only be gathered and supplied as appropriate but should also be recorded. This should form the basis of a final report into the breach, to be prepared by the DPO or the person responsible for data protection, which will be considered at the highest level within the organisation (board, senior management, owner, etc).

This report should include recommendations for remedial action and improvements in the organisation's data protection policy as appropriate and should consider the need for further training of relevant staff.

Once a data breach has been investigated, any related documentation must be kept by the Data Protection Officer and maintained in accordance with the requirements of the Data Protection Act No.24 of 2019.Data Breach documentation should be classified as confidential and access must be managed in accordance with the KHL Data Privacy Policy, Information Security Policy and other organizational policies and procedures.

### 4.12.7 Miscellaneous Provisions of the Policy

There are few miscellaneous provisions that should be adhered to in this policy

**a) Compliance, Sanctions and Enforcement**

- Compliance with this policy and operational directive outlined herein is mandatory.
- Those who fail to comply with this policy may face disciplinary action and, in serious cases, termination of their employment or engagement.

Unauthorised access, use, disclosure and destruction of confidential information is misconduct pursuant to KHL's Code of Conduct and may be subject to disciplinary action.

- Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

**b) Audits, Controls and Management,**

On-demand documented procedures and evidence of practice should be in place for this operational policy. Examples of appropriate audit controls and management practice includes:

- Archival completed Incident Reports demonstrating compliance with reporting, communication and follow-through.
- Executed communication plans for Incident management.
- Evidence of cross-departmental communication throughout the analysis, response and post-mortem processes.

**c) Monitoring and Distribution**

- Everyone must observe this policy.
- The DPO has overall responsibility for this policy.
- The DPO will review and monitor this policy regularly to make sure it is effective, relevant, and adhered to.
- We take compliance with this policy very seriously. Failure to comply puts both you and the organization at risk.
- The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.
- This policy is to be distributed to all KHL staff.

**d) Review and Updates**

We regularly review our Data Breach Policy. This version was last updated on 1st February 2021. Please note however that in case of any changes to the privacy policy, we will inform all our stakeholders of the same. KHL and its subsidiaries has established a mechanism of notifying all our stakeholders of updates to its privacy policy.

We recognize that data protection and privacy is an ongoing responsibility, so we reserve our right to make changes to this Data Breach Policy from time to time as we undertake new personal data practices or adopt new privacy policies, etc. If such changes are substantial, we will notify you via email, provided that we have your email address.

KHL reserves the right to change this policy and Terms of Service at any time. We will notify you of significant changes to the Data Breach Policy by sending a notice to the primary email address specified in your account or by placing a prominent notice on the site. Significant changes will go into effect 30 days following such notification. Non-material changes or clarifications will take effect immediately. Clients and all our stakeholders should periodically check the Site and this privacy page for updates.

# ANNEXURES & APPENDICES

## APPENDIX A: DRAFT JOB DESCRIPTION OF DATA PROTECTION OFFICER

**JOB TITLE** : DATA PROTECTION OFFICER

**REPORTING** : HEAD OF LEGAL/HEAD OF AUDIT/ HEAD COMPLIANCE/ OR CEO

**OTHER REPORTING:** DATA BREACH MANAGEMENT COMMITTEE

**Objectives of this Role**

- Lead KHL's data protection and privacy led projects
- Ensure the company's policy is in accordance with the Data Protection Act No.24 of 2019 and the attendant regulations and General Data Protection Regulation (GDPR) and codes of practice. Follow evolution of regulation and promote KHL's adequacy.
- Ensure respect of data subject rights concerning their personal data (right to information, access, rectification, erasure, restriction, portability, objection, decision making)
- Represent KHL vis-viz the Data Commissioner's Office and act as the primary point of contact within the organization for members of staff, regulators, and any relevant public bodies on issues related to data protection
- Evaluate the existing data protection framework and identify areas of non or partial compliance and rectify any issues
- Devise training plans and provide data protection advice and support for members of staff
- Inform and advise KHL as a Data Controller or Data Processor on all matters related to data protection
- Promote a culture of data protection compliance across all units of the organization

**Responsibilities**

- Inform and advise KHL as a data controller or data processor and employees how to be Data Protection Act No.24 of 2019 and GDPR compliant and how to comply with other data protection laws. Provide expert advice and educate employees on important data compliance requirements, including giving advice and recommendations to the company about the interpretation or application of the data protection rules.
- Enable compliance with GDPR and foster a data protection culture within the organisation by proactively conduct audits and monitoring to ensure compliance with Data Protection Act No.24 of 2019 and GDPR or other data protection law, addressing any potential issues and reporting any failure to comply.
- Drive implementation of essential elements of the GDPR, such as the principles of data processing, data subjects' rights, data protection by design and by default, records of processing activities, security of processing, and notification and communication of data breaches.
- Draft new and amend existing internal data protection policies, guidelines, and procedures, in consultation with key stakeholders including managing these internal policies and make sure the company is following them through.
- Manage a program of awareness-raising and training to deliver compliance and to foster a data privacy culture by holding training with staff members across different

business units who are involved in data handling or processing including raising awareness and provide staff training for any employees involved with processing activities.

- Manage the assignment of responsibilities to deliver compliance with data protection laws and policies of KHL including through departmental or regional managers, teams and champions.
- Supervise and advise on data protection impact assessments and provide advice regarding the data protection impact assessment and monitor its performance.
- Handle complaints or requests by the institutions, the data controller, data subjects, or introduce improvements on their own initiative.
- Identify and evaluate the company's data processing activities.
- Serve as the point of contact between the company and the data protection authorities and Cooperate with the supervisory authority.
- Maintain records of all data processing operations and activities carried out by the company and oversee the maintenance of records required to demonstrate data protection compliance.
- Provide updates on the data protection compliance programme KHL senior management team and Data Breach Management Committee and other relevant parties.

**Skills and Qualifications**

- Minimum of three years' experience working in data protection compliance or a related field.
- Expertise in Kenya's and International data protection laws and practices including an in-depth understanding of Data Protection Act N0.24 of 2019 and the GDPR and understanding their requirements.
- Experience within a Legal, Compliance, ICT, Information Security or Audit and/or Risk function department.
- Relevant work experience of monitoring compliance with regulatory requirements and engaging with regulatory bodies.
- Experienced in the operational application of privacy law.
- Familiarity with computer security systems.
- Experience in managing data breaches.
- Experience in cooperation with supervisory authorities of any kind.
- Understanding the environment in which business operates and associated data protection risks.
- Experience in conducting data protection impact assessments.
- Good understanding of the data processing operations carried out, as well as the information systems, and data security and data protection needs of the controller/Insurance
- Ability to make good judgements regarding data privacy risks and to prioritize resources and activity around managing those risks
- Able to conduct the role independently and with integrity and high professional ethics
- Ability to plan, organize and prioritize tasks and projects
- Good personal communication skills capable of dealing with wide range of stakeholders, including senior management
- Proven ability to establish and maintain a high degree of confidentiality, respect, trust and credibility at all levels
- Strong team player and proven ability to lead and manage a team
- Enthusiastic and positive

- The ability to remain calm, controlled and resilient
- Strong project management skills.
- Ability to work well under pressure and manage sensitive and confidential information
- Excellent verbal and written communication skills, with strong attention to detail.
- Great interpersonal skills and ability to work well both independently and as part of a team.

.

## APPENDIX B: DATA BREACH SEVERITY TABLE FOR INITIAL ASSESSMENT OF A DATA BREACH

| SEVERITY OF THE BREACH | CRITERIA (ONE OF THE FOLLOWING) |
|---|---|
| MINOR BREACH | ▪ The breach involves data classified as Internal Use or Restricted.<br>▪ The breach involves a small number of individuals (less than 10).<br>▪ The breach incurs a low risk to KHL<br>▪ Inconvenience may be suffered by individuals impacted.<br>▪ The breach involves data that is contained / encrypted / password protected.<br>▪ The breach can be responded to during working hours.<br>Examples:<br>▪ An email being sent to a wrong recipient.<br>▪ Loss of an encrypted mobile device. |
| MAJOR BREACH | ▪ The breach involves data classified as Highly Restricted / Restricted.<br>▪ The breach involves more than 10 but less than 25 individuals.<br>▪ External third-party data is involved.<br>▪ There are significant or irreversible consequences.<br>▪ The breach is likely to result in media coverage.<br>▪ An immediate response is required regardless of whether it is contained or not.<br>▪ The breach requires a significant response beyond normal operating procedures. |
| SERIOUS BREACH | ▪ The breach involves data classified as Restricted.<br>▪ The breach is not contained within KHL<br>▪ The breach involves personal data of more than 25 individuals.<br>▪ A significant inconvenience will be experienced by individuals impacted.<br>▪ The breach may not yet be contained.<br>▪ The breach does not require an immediate response.<br>▪ The response to the breach may require notification to KHL's senior management. |

## APPENDIX C: DATA SECURITY BREACH INCIDENT REPORT FORM

- This form must be completed to report suspected and actual data breach incidents such as data loss.
- This form can be completed by anyone with knowledge of the incident.
- This form should be completed as soon as a data breach has been identified.
- You must email the completed form to the Data Protection Officer immediately.

| **DATA SECURITY BREACH INCIDENT REPORT FORM** | |
|---|---|
| **1.SUMMARY OF INCIDENT**<br>***To be completed by the person reporting the data breach*** | |
| Person Reporting the breach | |
| Date and Time of the Incident | |
| Number of Persons whose data is affected | |
| Department | |
| Nature of breach e.g. theft / disclosed in error / technical problems: | |
| Description of how breach occurred: | |
| **Signed by the person reporting the breach:** | |
| **Date:** | |
| **2. REPORTING**<br>***To be completed by DPO*** | |
| When was the breach reported? | |
| How did you become aware of the breach? | |
| Severity of Breach identified by Initial Assessment | In accordance with the Initial Assessment as described in Appendix B (delete as applicable):<br>a) Major Breach<br>b) Serious Breach<br>c) Minor Breach |
| Who will be leading the investigation of the breach? | Normally a Senior Management Team member managing an area not involved in the breach. |
| **Signed by the DPO** | |
| **Date** | |
| **3. PERSONAL DATA**<br>***To be completed by the Lead Investigator*** | |
| Full description of personal data involved (without identifiers): | |

| | |
|---|---|
| Number of individuals affected: | |
| Have all affected individuals been informed? | |
| If not, state why not: | |
| Is there any evidence to date that the personal data involved in this incident has been inappropriately processed or further disclosed? If so, please provide details: | |
| **4. DATA RETRIVAL**<br>***To be completed by the Lead Investigator*** | |
| What immediate remedial action was taken? | |
| Has the data been retrieved or deleted? If yes, state the date and time. | |
| **5. IMPACT**<br>***To be completed by the Lead Investigator*** | |
| Describe the risk of harm to the individual as a result of this incident: | |
| Describe the risk of identity fraud as a result of this incident: | |
| Have you received a formal complaint from any individual affected by this breach? If so, provide details. | |
| **6. MANAGEMENT**<br>***To be completed by the Lead Investigator.*** | |
| Do you consider the employee(s) involved has breached information governance policies and procedures? | |
| Please inform of any disciplinary action taken in relation to the employee(s) involved. | |
| Had the employee(s) completed regular data protection training? If so when? If not, why? | |
| As a result of this incident, do you consider whether any other personal data held may be exposed to similar vulnerabilities? If so, what | |

| | |
|---|---|
| steps have been taken to address this? | |
| Has there been any media coverage of the incident? If so, please provide details. | |
| What further action has been taken to minimise the possibility of a repeat of such an incident? Please provide copies of any internal correspondence regarding any changes in procedure. | |
| Were you aware of weaknesses in the systems, policies or procedures breached? Either by audit recommendations or anecdotal evidence? | |

**7. ACTION PLAN**
***To be completed by the Lead Investigator & DPO & monitored by the Data Breach Management Committee***

| ACTION | RESPONSIBILITY | DEADLINE | PROGRESS |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**8. TIMELINE**
***To be completed by the DPO & Lead Investigator throughout the investigation.***

| Date | Time | Action Taken/Decision | Authority |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| **9. SIGN OFF to Confirm Case has been Concluded**<br>***To be completed by the DPO & monitored by the Data Breach Management Committee*** | | | |
| Completed Date: | | | |
| Signed: | | | |
| Signed off by Data Management Committee as all actions completed: | | | |

## APPENDIX D: DATA SECURITY BREACH LOG

| Ref | Details of Breach | | | | | Potential/Actual Consequences of the Breach | Measures taken /to be taken following implementation of Data Breach Management Plan | | |
|---|---|---|---|---|---|---|---|---|---|
| | Date of Breach | No. of People Affected | Description of Breach | How you become aware of the Breach | Description of Data | | Remedial Action | Action Responsibility Deadline | Regulators required to be informed |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## APPENDIX E: ASSESSMENT OF ON-GOING RISK

This form should be completed by the senior member of staff identified as the lead on investigating a data security breach.

| **Senior member of staff identified to lead on investigating the breach:** | Name & Role |
|---|---|
| **What type of data is involved?** | Describe the data involved in the breach and include the classification of data involved in accordance with the Information Asset Classification System described in the Information Security Policy (delete as applicable):<br>a) Highly Restricted<br>b) Restricted<br>c) Internal Use<br>d) Public |
| **How sensitive is the data?** | E.g. Data may be defined as sensitive if it is of a personal nature (such as health records) or could be misused (such as bank account details). |
| **What has happened to the data?** | Has the data been lost, damaged or stolen?<br>If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk. |
| **Is the data involved encrypted or password protected?** | Describe whether the data is protected in any way or were there protection in place to mitigate its loss, e.g. backups or copies? |
| **What could the data tell a third party about an individual?** | E.g. Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people. |
| **How many individuals' personal data are affected by the breach?** | E.g. It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment. |
| **Who are the individuals whose data has been breached?** | E.g. Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks |
| **What harm can come to those individuals?** | E.g. Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life? |
| **Are there wider consequences to consider?** | E.g. Is there a risk to public policy or loss of public confidence in an important service the |

| | |
|---|---|
| | KHL provides? |
| **Who else could help to inform the assessment of ongoing risk?** | E.g. If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use. |
| **Record the date and time that this assessment has been completed on the Data Security Breach Management Timeline in Appendix B.** | See Appendix B |

## APPENDIX F: NOTIFICATION OF DATA BREACH CHECK LIST

| QUESTION | ANSWER |
|---|---|
| Has personal data been breached and will this have a significant adverse impact on the individuals affected? | The individual's affected should be informed without undue delay in accordance with the process outlined in Notifying Individuals Affected.<br><br>The DCO should be informed within 72 hours of the KHL being aware of the personal data breach through their reporting process: |
| Does the DCO need to be contacted for advice in how to handle the data breach? | Check with the DPA or the DCO's website for guidance. |
| Are there any legal or contractual requirements to notify individuals or an organisation of a data breach? | Affiliates/Partners/Service Providers/Regulatory Body |
| Can notification help us meet our security obligations with regard to the seventh data protection principle? | E.g. Prevent unauthorised access, loss or damage to the data? |
| Can notification help the individual? | Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example by cancelling a transaction card (Debit/Credit/ Wallet) or changing a password? |
| Is there a risk of 'over notifying'? | E.g. Notifying a whole customer base consisting of 1000's of customers of an issue affecting only 20 customers may well cause disproportionate enquiries and work. |
| Does the notification need to be made appropriate for particular groups of individuals? | E.g. Children or vulnerable adults? |
| Do third parties also need to be notified? | E.g. the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals, and trade unions. |

## APPENDIX G: NOTIFICATION OF DATA BREACH TEMPLATE

Dear <Name>,

This is to inform you that KHL confirms that a data breach has occurred as described below. We are making every effort to recover the data and to enhance our information security to prevent similar incidences as described below.

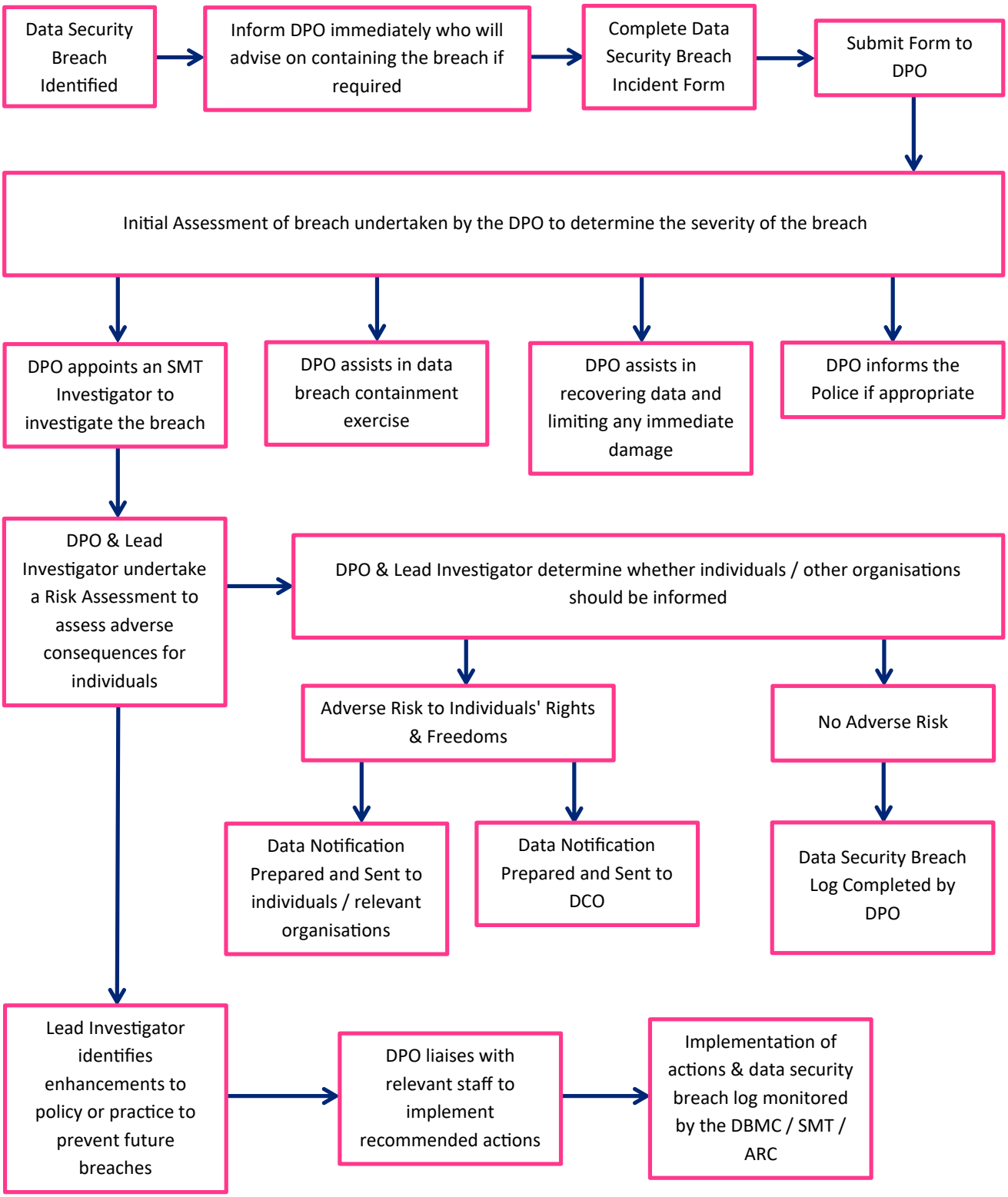
| | |
|---|---|
| Date of data breach: | |
| What happened: | |
| What data was involved: | |
| What KHL has done to respond to the risks posed by the breach: | |
| Action you may wish to take to protect yourself further as a result of this breach: | |

If you have any questions regarding the above data breach, please do not hesitate to contact me.

Yours faithfully,
XXXX

Data Protection Officer (DPO)
dpo@karibuhomes.com

## APPENDIX H: DATA BREACH MANAGEMENT FLOW CHART



KARIBU
HOMES

O Suite G, Springette, Lower Kabete Road
P.O. Box 40063 - 00100, Nairobi, KENYA
T: + 254 705 151585 / M: + 254 705 151515
E: frontdesk@karibuhomes.co
W: www.karibuhomes.com