EQUITY LIFE ASSURANCE KENYA DATA PROTECTION AND PRIVACY POLICY

DOCUMENT HISTORY

VERSION	DATE APPROVED	ACTION BY	BRIEF DESCRIPTION / COMMENT
V1.21.02	11/02/2021	Data Strategy and Analytics Risk & Compliance Legal	Initial Document
		ELAK Head of Risk and Compliance	Localise policy for ELAK

This Data Protection and Privacy policy was passed and endorsed as fit to run and support the businesses of Equity Life Assurance Kenya on this _____ day of November 2022.

Contents

1. INTRODUCTION

Equity Life Assurance Kenya (ELAK), is committed to the ethical and sustainable use of personal and sensitive data within the organization. This policy is designed to specify the essential elements in the management of risks relating to processing of both personal and sensitive data.

The purpose of this policy document is to describe ELAK's guidelines regarding how the bank processes data to ensure compliance to the General Data Protection & Regulation (GDPR) and Kenya Data Protection Act.

1.1. Objectives

- To ensure that all staff members are clear about how personal data is processed and ELAK's expectations for all those who process personal data on its behalf including third parties.
- To ensure that ELAK complies with both data protection laws and embeds global best practices.
- To ensure that ELAK's reputation is protected by ensuring personal data is processed lawfully and in line with the data subjects' rights.
- To protect ELAK from risks of personal data breaches and other breaches of the data protection law.

1.2. Applicability of Policy

- This policy applies to all personal data processed within ELAK regardless of the location where that personal data is stored and regardless of the data subject.
- This policy applies to all persons employed by or under contract with ELAK.

1.3. Definitions

Automated Decision Making	Decision made based solely on automated processing Decision-Making including profiling that produces legal effects or significantly affects an individual. The regulations prohibit Automated Decision-Making unless certain conditions are met.
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 analyze or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. Profiling is an example of automated processing.
Consent	Agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.
Data Controller	The person or organization that determines when, why and how to process personal data. It is responsible for establishing practices and policies in accordance with the Privacy and protection regulations. ELAK is the Data Controller of all personal data relating to its customers and used for conducting business or research any all other purposes connected with it.
Data processor	A company that processes personal data on behalf of the data controller.
Data Subject	A living, identified or identifiable individual about whom we hold personal data i.e. both customers and staff members.
Data Protection Impact Assessment (DPIA)	Privacy risk assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.

Data Protection Officer (DPO)	Person appointed and responsible for advising ELAK (including its employees) on their obligations under Data Protection Law, for monitoring compliance with data protection law, as well as with ELAK's polices, providing advice, cooperating and acting as a point of contact with any regulatory body enforcing the law.
Personal Data	Any information identifying a data subject (employees and customers) 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 pseudonymized personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location, or date of birth)
Data Breach	Any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data, where that breach results in a risk to the data subject.
Privacy by Design and Default	Technical measures embedded in the software development life cycle to ensure privacy is embedded in the solution design from the onset
Privacy Notices	Separate notices setting out information that shall be provided to data subjects when ELAK collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals or they may be stand-alone, one-time privacy statements covering processing related to a specific purpose.
Data Processing	Any operation or set of operations applied on data including organizing, 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.
Anonymization or Pseudonymized	Replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.
Special Catrgory/Sensitive data	Any data revealing: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs, • Genetic data • Biometric data for the purpose of uniquely identifying a natural person. • Health data

2. RESPONSIBILITIES

The administration and management of this policy shall be as follows

2.1. Data Protection Officer (Head of Risk & Compliance)

- Shall ensure that this policy is reviewed as frequently as prescribed in internal policy or, a formerly adopted best practice standard.
- Shall ensure that this policy is duly constituted and updated, in line with industry best practice and internal policy.

2.2. Chief Information Officer

- Shall ensure adoption and compliance to this policy.

2.3. Head of Risk & Compliance

- Shall test on compliance to this policy on a continual basis.

2.4. IT Security

- Shall support the enforcement of the policy through technical and organizational measures.

2.5. Head of Human Resources

- Shall ensure adoption of policy across all human resource processes across the bank.

2.6. Data Processor

- Shall Support the enforcement of the policy through technical and organizational measures.

3. POLICY STATEMENTS

3.1. Data Controller & Processor

3.1.1. As a Controller, ELAK shall maintain the below information:

- Names and contact details of any joint controllers, representatives and data protection office
- The purposes of the processing of personal data within ELAK
- A description of the categories of data subjects (Staff and Customers) and of the categories of personal data
- The categories of recipients, including recipients in third countries or international organizations
- Details of transfers of personal data to third countries where applicable
- Retention periods for different categories of personal data where possible
- A general description of the security measures employed by Equity across various domains within ELAK.

3.1.2. As a Processor, ELAK shall maintain the below information:

- Name and contact details of the data protection office
- The name and contact details of each data controller you acting on behalf including, where applicable, representatives and data protection officers
- The categories of processing carried out on behalf of each controller
- Details of transfers of personal data to third countries where applicable
- A general description of the security measures employed where possible
- Record of sub-processors used, approvals by the controller to use sub-processors and security measures of sub-processors

3.1.3. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

3.1.4. Personal data collected for specified, explicit and legitimate purposes shall not be further processed in a manner that is incompatible with the said purposes.

3.1.5. Data subjects shall be informed and their consent obtained should there be any intention to use their personal data for entirely new, different or incompatible purposes from those disclosed when it was obtained.

3.1.6. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

3.1.7. ELAK shall not amass large volumes of personal data that are not relevant for the purposes for which they are intended to be processed.

3.1.8. ELAK shall ensure that personal data collected shall be adequate to ensure that it can fulfil the purposes for which it was intended to be processed.

3.1.9. ELAK shall ensure that personal data is as accurate as possible and where necessary, kept up to date.

3.1.10. The GM Operations shall ensure that the accuracy of all personal data is checked at the point of collection and at regular intervals thereafter.

3.1.11. Where necessary the GM Operations shall take all reasonable steps to destroy or amend inaccurate records without delay.

3.1.12. The GM Operations shall ensure that personal data is stored in a form, which permits identification of data subjects for no longer that necessary for the purposes to which the data is processed.

3.1.13. Whenever possible, personal data shall be stored for longer periods insofar as the personal date will be processed solely for archiving purposes.

3.1.14. The GM Operations shall ensure that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

3.1.15. Processing of personal data shall be considered lawful if it satisfies at least one of the processing conditions highlighted below:

a) If the data subject has unambiguously given his consent

This implies that the individual has given their consent to the processing for one or more specific purposes. By definition, consent must be freely given, specific and informed. ELAK shall keep records in order to be able to demonstrate that consent has been given by the data subject.

b) If processing is necessary for the performance of a contract

Where processing is necessary for the performance of a contract, to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract that nature of processing is considered lawful. ELAK shall process personal data necessary for the provision of a service requested by a client or prospective client, in line with agreed terms and conditions aimed at regulating the relationship between the client and Equity, such processing is considered legitimate.

c) If processing is necessary for compliance with a legal obligation to which the controller is subject

This applies in situations involving data processing carried out to comply with statutory obligations imposed on ELAK e.g. reporting to the tax authorities, or reporting of suspicious transactions under the Prevention of Money Laundering Regulations.

d) If processing is necessary in order to protect the vital interests of the data subject

This is typically limited to processing needed for medical emergencies.

e) If processing is necessary for the performance of a task that is carried out in the public interest or in the exercise of official authority vested in the controller

This may also be utilized when processing of personal data is necessary for the performance of an activity that is carried out in the public interest e.g. census

f) If processing is necessary for a purpose that concerns a legitimate interest

If the processing is necessary for a purpose that concerns legitimate interest to the controller or of a third party, except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject, in particular where the data subject is a child.

3.2. Processing of Special Category/Sensitive Data

3.2.1. Any processing of special categories of personal data shall satisfy at least one of the conditions highlighted below:

a) Explicit consent - the individual has given explicit consent.

b) Legal obligation related to employment - The processing is necessary for a legal obligation in the field of employment or for a collective agreement.

c) Vital interests - The processing is necessary in order to protect the vital interests of the individual or of another natural person. This is typically limited to processing needed for medical emergencies.

d) Not for profit bodies - The processing is carried out in the course of the legitimate activities of a not-for profit body and only relates to members or related persons and the personal data is not disclosed outside that body without consent.

e) Public information - The processing relates to personal data which is manifestly made public by the data subject.

f) Legal claims - The processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity.

g) Substantial public interest - The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law.

h) Healthcare - The processing is necessary for healthcare purposes and is subject to suitable safeguards. Additionally, Health of a Data Subject under the data protection act can only be processed when is necessary for:

i. The purpose of preventive or occupational medicine
ii. Assessment of the working capacity of an employee
iii. Medical diagnosis
iv. Provision of health or social care
v. Treatment or the management of health or pursuant to a contract with a health professional.

3.3. Processing of Personal Data Relating to Children

3.3.1. ELAK shall ensure that it processes personal data of children in a manner that protects and advances their rights and best interests.

3.3.2. ELAK shall incorporate appropriate mechanisms for age verification and parental consent in order to process personal data of children in a lawful manner. Such mechanisms as per the data protection law shall be determined on the basis of:

a. Volume of personal data processed
b. Proportion of such personal data likely to be that of children
c. Possibility of harm to children arising out of processing of personal data

3.4. Processing of personal data relating to criminal convictions and offences

3.4.1. Information about criminal convictions, offences or related security measures shall be processed only as outlined in the various data Protection laws within the jurisdictions that ELAK operates in.

3.4.2. Consent from an individual shall not provide a justification to process personal data relating to criminal convictions and offences.

3.4.3. Equity shall process personal data relating to criminal convictions and offences under the below conditions.

a) ELAK Customers

- ELAK shall maintain relevant information to alert its operations team to the risks of making new or policy endorsements to individuals who clearly do not qualify for such new or additional policy covers.
- ELAK shall retain, on a particular customer file, press cuttings or other information relating to court proceedings, convictions against a customer and similar information on any other person (e.g. a debtor of the customer) where such information may affect the relationship between ELAK and the customer. This shall be on the basis of Know Your Customer' principle outlined in the Insurance Regulatory Authority guidelines.

3.5. Processing of Employee Data

3.5.1. Employees shall consent to the processing of personal information by ELAK and Equity Group.

3.5.2. All employees shall be fully informed of the nature and scope of the processing, including understanding fully how the information will be processed, used and transmitted to third parties. A read and sign approach should be adopted where possible.

3.5.3. Without consent the other conditions that ELAK shall use to process employee data are as outlined below.

a) Legitimate interest - For ELAK to rely on legitimate interest as the legal basis of processing HR shall perform a privacy impact assessment balancing ELAK's legitimate interest against the employees' privacy interests. This has to be documented to clearly show that ELAK's interest outweighs the employee's privacy needs. The processing must also be proportionate to the business needs, i.e. the purpose, it is meant to address. The employee however retains the right to object to the processing on compelling grounds.

b) Performance of a Contract - When meeting obligations under an employment contract, such as paying the employee, the employer shall be required to process some personal data.

c) Legal Obligation - Employment law imposes legal obligations on the employer, which necessitate the processing of personal data (e.g. for the purpose of tax calculation and salary administration).

3.5.4. ELAK in the process of recruiting shall conduct due diligence on potential employees under consideration. This will generally include obtaining professional references, confirming employment history, qualifications and requesting a recent police good conduct certificate.

3.5.5. ELAK shall be allowed to process and keep copies and records of the collected data sets for selected candidates for the duration that the employee stays in employment

3.6. Restriction of Processing

3.6.1. ELAK at the request of a data subject or customer shall restrict the processing of personal data where:

a) Accuracy of the personal data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the data

b) Personal data is no longer required for the purpose for which it was collected but the data subject requires the personal data for the establishment, exercise or defense of a legal claim.

c) Processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of its use.

d) Data subject has objected to the processing, pending verification as to whether the legitimate grounds of the data controller or data processor overrides those of the data subject.

3.7. Data Subject Rights

3.7.1. Right of Access by the Data Subject

A data subject shall have the right to obtain from the data controller confirmation as to whether or not personal data concerning him or her is being processed. Additional information that the data subject shall have access to includes:

a) The purposes of the processing

b) The categories of personal data concerned

c) The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations

d) Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period

e) The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing

f) The right to lodge a complaint with a supervisory authority

g) Where the personal data has not been collected from the data subject, any available information as to their source

h) The existence of automated decision-making, including profiling, referred to in Article and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

i) Where personal data is transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

3.7.2. The Right to Rectification

i. A data subject shall have the right to obtain from ELAK without undue delay the rectification of inaccurate personal data concerning him or her.

ii. The data subject shall have the right to have incomplete personal data completed and inaccurate data corrected.

3.7.3. Right to Erasure ('Right to be forgotten')

i. The data subject shall have the right to obtain from ELAK the erasure of personal data concerning him or her without undue delay.

ii. ELAK shall have the obligation to erase personal data without undue delay where one of the following rules applies:

a) The personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed.
b) The data subject withdraws consent on which the processing is based or where there is no other legal ground for the processing.
c) The personal data has been unlawfully processed.
d) The personal data has to be erased for compliance with a legal obligation within the country to which the controller is subject.

3.7.4. Right to Restriction of processing

The data subject shall have the right to obtain from ELAK restriction of processing where one of the following applies:

a) The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
b) The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead.
c) The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims.

3.7.5. Right to data portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

a) The processing is based on consent.
b) The processing is carried out by automated means.

In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3.7.6. Right to Object Automated Individual Decision-Making, including profiling

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her.

This shall not apply if the decision is necessary for entering into, or performance of, a contract between the data subject and ELAK or if the data subject has given explicit consent.

a) Request that the decision be reconsidered other than in a manner based solely on automated processing.
b) Obtain information from ELAK about what has controlled the automated processing that resulted in the negative decision.

However, such obligations would not apply in those cases where the decision is necessary for entering into, or the performance of, a contract between the controller and data subject.

3.8. Information Communication

3.8.1. ELAK shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with the law.

3.8.2. ELAK shall take appropriate measures to provide any information referred to relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

3.8.3. Information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

3.8.4. Where personal data relating to a data subject is collected from the data subject, the controller shall, at the time when personal data is obtained, provide the data subject with all of the following information:

a) The identity and the contact details of the controller and where applicable, of the controller's representative
b) The contact details of Equity's data protection office
c) The purposes of the processing for which the personal data are intended as well as the legal basis for the processing
d) The recipients or categories of recipients of the personal data, if any
e) Where applicable, the fact that the controller intends to transfer personal data to a third country.

3.8.5. Where personal data has not been obtained from the data subject, the controller shall provide the data subject with the following information:

a) The identity and the contact details of the controller and, where applicable, of the controller's representative;
b) The contact details of Equity's data protection office.
c) The purposes of the processing for which the personal data was intended as well as the legal basis for the processing
d) The categories of personal data concerned
e) The recipients or categories of recipients of the personal data, if any.

3.9. Data Retention & Archiving

3.9.1. ELAK shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless the retention is

a) Required or authorized by law
b) Reasonably necessary for a lawful purpose
c) Authorized or consented by the data subject
d) For historical, statistical or research purposes

3.9.2. ELAK shall delete, erase, anonymize or pseudonymised personal data not necessary to be retained.

3.9.3. ELAK shall develop and maintain a data retention policy that highlights the various retention periods for different classes of data assets within Equity to ensure proper retention and archiving practices are maintained.

3.10. Data privacy by Design or Default

3.10.1. Equity shall ensure that all departments involved when deploying systems, processes, applications, products and services that rely on the processing of personal data to fulfil their tasks, design products and services containing technical measures which are data protection friendly embedded in their design.

3.10.2. The Head of Risk & Compliance shall be consulted whenever possible to provide their input on how best to achieve this.

3.10.3. Privacy by design measures to be employed during development shall include:

a) Data minimization and pseudonymization
b) Transparency both in relation to processing and the functions within an organization
c) Default settings, which limit the processing of personal data to what is strictly necessary
d) Features enabling data subjects to have more control on their personal data including its access and further usage
e) Measures protecting data subjects' rights
f) Strong access controls including audit trails and flagging systems
g) Data segregation mechanisms
h) Automated deletion or anonymization of personal data upon expiry of the storage period.

3.11. Data Protection Impact Assessments (DPIAs)

3.11.1. ELAK shall conduct data protection impact assessments for any processing that is likely to create "high risks" for customers. Activities which can be considered to involve high risk processing, include conducting due diligence and especially enhanced due diligence in relation to any potential or existing customer as well as profiling of clients. Profiling activities, which may lead to decisions including those by automated means, which have significant effects on data subjects, such as for example credit scoring, are considered to create high risk and would require an impact assessment.

3.11.2. ELAK shall conduct Data Protection Impact assessments in respect of high-risk processing as a result of new technology being employed.

3.11.3. A DPIA shall be conducted early into the life of a project and will run alongside the planning and development process.

3.11.4. A checklist shall be maintained to enable proper assessment to be done within the project management life cycle.

3.12. Direct and Electronic Marketing

3.12.1. ELAK shall obtain a data subject's prior consent for electronic direct marketing for example, by email, text or automated calls.

3.12.2. The limited exception for existing customers e.g. current existing to ELAK customers known as "soft opt in" shall be used by ELAK to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar services and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message. iii. The right to object to direct marketing shall explicitly be offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information. iv. A data subject's objection to direct marketing shall be promptly honored.

3.12.3. If a data subject opts out at any time, their details shall be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

3.13. Reporting a Personal Data Breach

3.13.1. Any Data breaches shall be reported immediately to IT security and Data Governance which will serve as the data protection office.

3.13.2. ELAK shall report to the Information Commissioner's Office (ICO) any personal data breach where there is a risk to the rights and freedoms of the data subject.

3.13.3. Where the Personal data breach results in a high risk to the data subject, he/she shall be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialize such as anonymization.

3.13.4. In the latter circumstances, a public communication shall be made or an equally effective alternative measure shall be adopted to inform data subjects, so that they themselves can take any remedial action.

3.13.5. Records of personal data breaches must also be kept, setting out.

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

3.14. Security of Processing

3.14.1. ELAK shall ensure that personal data is secure at all time.

3.14.2. ELAK has and shall keep investing in security measures that shall improve its security posture at all times.

3.14.3. Technical and organizational measures that Equity shall employ are as outlined below.

a) The pseudonymisation and encryption of sensitive data
b) Entrenchment of (CIA) confidentiality, integrity, availability and resilience to all bank information technology systems.
c) Ensure the ability to restore availability and access to personal data in the event of a physical or technical incident.
d) Develop processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing.

3.15. Processor Outsourcing

3.15.1. Choosing a processor

a) ELAK shall only use processors who have or can provide sufficient guarantees to implement appropriate technical and organizational measures so that the processing meets world-class privacy and protection requirements. This way fundamental rights of customers shall be protected.
b) ELAK shall conduct broader due diligence exercise when selecting a processor.
c) ELAK as a controller shall consider whether it is necessary, or good practice, to carry out a data protection impact assessment (DPIA) before entering into a major new processing arrangement.

3.15.2. Negotiating a processor contract

ELAK shall enter into written agreements with third parties intending to process data on its behalf. The agreement shall clearly abide by the below requirements.

Processing by a processor shall be governed by a contract that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data, categories of individuals whose data is being processed and the obligations and rights of the controller.

The contract shall stipulate, in particular, that the processor will:

a) Process only on documented instructions, including with regard to transfers of personal data to a third country or to an international organization (unless, subject to certain restrictions, legally required to transfer to a third country or international organization) ensure those processing personal data are under a confidentiality obligation (contractual or statutory)
b) Take all measures required under the security provisions which includes pseudonymizing and encrypting personal data as appropriate.
c) Only use a sub-processor with the controller's consent (specific or general, although where general consent is obtained processors must notify changes to controllers, giving them an opportunity to object) flow down the same contractual obligations to sub-processors.
d) Assist ELAK/controller in responding to requests from individuals (data subjects) exercising their rights
e) Assist ELAK/controller in complying with the obligations relating to security, breach notification, DPIAs and consulting with supervisory authorities

f) Delete or return at ELAK/controller's choice all personal data at the end of the agreement.

g) Make available to the controller all information necessary to demonstrate compliance allow/contribute to audits (including inspections) and inform the controller if its instructions infringe data protection law.

3.16. Cross Border Data Transfer

a) Cross border data transfer of customer sensitive data shall be prohibited.

b) The Regulator based on strategic interests shall categorize data classes as sensitive and hence shall only be processed within the country of origin.

c) ELAK shall be expected to have on premise copy of all data that may be sitting in a different jurisdiction.

d) Consent shall be obtained upon application from the ordering customer for crossborder credit transfers via SWIFT. By signing the transfer order, the ordering customer would also be implicitly giving his consent to the transfer of the personal data contained in the transfer order to the jurisdiction where recipient of such transfer is located.

3.17. Conditions of Cross Border Transfer

ELAK as a data controller and a data processor shall transfer personal data to another country when the following conditions are met:

a) ELAK has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data.

b) ELAK customer has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer such as the absence of appropriate security safeguards.

c) The transfer is necessary for

- The performance of a contract between the customer and Equity or Equity's data processor or implementation of pre-contractual measures taken at the customer's request.
- For the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person
- For the establishment, exercise or defense of a legal claim
- In order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
- For the purpose of compelling legitimate interests pursued by Equity which are not overridden by the interests, rights and freedoms of the data subjects.

4. Appendix

Typically, the nature of the information maintained for legitimate interest would include

a) Individuals (both customers and non-customers) who are known or suspected of having engaged in fraudulent activities. Such information would need to be supported by a police report or other reliable sources (e.g. Equity's security officer who would have conducted the necessary investigations).

b) Information received from Credit Reference bureaus on credit ratings of customers

c) The 'Know Your Customer' principle is particularly relevant to the business, and ELAK shall seek to have maximum knowledge of all its customer's affairs, including details of their backgrounds, means, etc. This is also necessary for ELAK to comply with the due diligence procedures which are called for under the anti-money laundering legislation.