# Data Protection Policy

**Contents of this policy**

## 1. Introduction

Recent concerns about the security of personal data stored in institutions have led to Governments enacting data protection regulations. In 2018 the European Union (EU) operationalised the General Data Protection Regulations (GDPR) that govern how companies handle personal data. Consequently, in 2019 Kenya enacted its own Data Protection Act. The regulations seek to protect the privacy of individuals by enforcing responsible processing of personal data. This includes embedding principles of lawful processing, minimising the collection of data, ensuring the accuracy of data and adopting security safeguards to protect personal data.

## 2. Policy statement

Apex Steel Ltd is committed to complying with all relevant Kenyan legislation and applicable global legislations. Apex Steel Ltd recognises that the protection of individuals through lawful, legitimate, and responsible processing and use of their personal data is a fundamental human right.

Apex Steel Ltd will ensure that it protects the rights of data subjects and that the data it collects, and processes is done in line with the required legislation. Apex Steel Ltd staff must comply with this policy, breach of which could result in disciplinary action.

## 3. Purpose

The policy provides guidance on how Apex Steel Ltd will handle the data it collects. It helps Apex Steel Ltd comply with the data protection law, protect the rights of the data subjects and protects Apex Steel Ltd from risks related to breaches of data protection.

## 4. Scope

The policy applies to:

a) Employees of Apex Steel Ltd and all Apex Steel Ltd's associated parties such as implementing partners, vendors, contractors and any other third party who handle and use Apex Steel Ltd information, where Apex Steel Ltd is the '**Controller**' for the personal data being processed, be it in manual and automated forms or if others hold it on their systems for Apex Steel Ltd;

b) All personal data processing Apex Steel Ltd carries out for others (where Apex Steel Ltd is the **'Processor'** for the personal data being processed) and,

c) All formats, e.g., printed and digital information, text and images, documents and records, data and audio recordings.

## 5. Definitions[1]

**Data controller** means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data.

[1] Adapted from the Kenya Data Protection Act

**Data processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

**Data subject** means an identified or identifiable natural person who is the subject of personal data.

**Personal data** means any information relating to an identified or identifiable natural person

**A personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed

**Sensitive personal data** means data that reveals 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.

**Processing data** means any operation or sets of operations performed on personal data whether or not by automated means, such as (a) collection, recording, organisation, structuring; (b) storage, adaptation or alteration; (c) retrieval, consultation or use; (d) disclosure by transmission, dissemination, or otherwise making available; or (e) alignment or combination, restriction, erasure or destruction.

## 6. Principles

Apex Steel Ltd will ensure that data is:

a) Processed lawfully, fairly and in a transparent manner and in line with the right to privacy.

b) Collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with that purpose.

c) Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is to be processed.

d) Accurate and where necessary kept up to date.

e) Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed.

f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction, or damage.

g) Not transferred out of Kenya unless there is proof of adequate data safeguards/ measures or consent from the data subject.

## 7. Data protection officer

Apex Steel Ltd has designated the **IT Executive** to be the Data Protection Officer (DPO). Accordingly, the DPO will:

a) Advise Apex Steel Ltd staff on requirements for data protection, including data protection impact assessments.

b) Ensure that the Apex Steel Ltd has complied with the legal requirements on data protection.

c) Facilitate capacity building of staff involved in data processing operations.

d) Cooperate with external regulators on matters relating to data protection. Apex Steel Ltd's DPO can be contacted via the email:

s.darji@apex-steel.com

**8. Duty to notify**

Apex Steel Ltd has a duty to notify data subjects of their rights before processing data. Apex Steel Ltd will therefore inform the data subjects of their right:

a) To be informed of the use to which their personal data is to be put.
b) To access their personal data in Apex Steel Ltd's custody.
c) To object to the processing of all or part of their personal data.
d) To the correction of false or misleading data.
e) To deletion of false or misleading data about them.

**9. Lawful and fair processing of data**

Apex Steel Ltd will only process data where they have a lawful basis to do so. Processing personal data will only be lawful where the data subject has given their consent for one or more specific purposes or where the processing is deemed necessary:

a) For the performance of a contract to which the data subject is a party (for instance a contract of employment).
b) To comply with the Apex Steel Ltd's legal obligations.
c) To perform tasks carried out in the public interest or the exercise of official authority.
d) To protect the vital interests of the data subject or another person.
e) To pursue Apex Steel Ltd's legitimate interests where those interests are not outweighed by the interests and rights of data subjects.
f) For historical, statistical, journalistic, literature and art or scientific research.

**10. Minimisation of collection**

Apex Steel Ltd will not process any personal data for a purpose for which it did not obtain consent. Should such a need arise, then consent must be obtained from the data subject.

Apex Steel Ltd will collect and process data that is adequate, relevant, and limited to what is necessary. Apex Steel Ltd staff must not access data which they are not authorised to access nor have a reason to access.

Data must only be collected for the performance of duties and tasks; staff must not ask data subjects to provide personal data unless that is strictly necessary for the intended purpose.

Staff must ensure that they delete, destroy, or anonymise any personal data that is no longer needed for the specific purpose for which they were collected.

**11. Accuracy of data**

Apex Steel Ltd must ensure that the personal data it collects and processes is accurate, kept up to date, corrected or deleted without delay. All relevant records must be updated should staff be notified of inaccuracies. Inaccurate or out of date records must be deleted or destroyed.

**12. Safeguards and security of data**

Apex Steel Ltd has instituted data security measures which are laid out in the Information security policy and procedures. These measures serve to safeguard personal data and must be complied with accordingly.

**13. Consent**

Where necessary, Apex Steel Ltd will maintain adequate records to show that consent was obtained before personal processing data. Data will not be processed after the withdrawal of consent by a data subject.

**14. Processing data relating to a child**

Apex Steel Ltd will not process data relating to a child unless consent is given by the child's guardian or parent and the processing is in such a manner that protects and advances the rights and best interests of the child in line with Apex Steel Ltd Safeguarding policy.

Apex Steel Ltd will institute adequate mechanisms to verify the age and obtain consent before processing the data.

**15. Data protection impact assessment**

Apex Steel Ltd will undertake a data protection impact assessment whenever they identify that the processing operation will likely result in a high risk to the rights and freedoms of any data subject. The data protection impact assessment will be done before processing the data. It is the responsibility of the DPO to carry out the impact assessment.

**16. Processing sensitive personal data**

Apex Steel Ltd will process sensitive personal data only when:

a) The processing is carried out in the course of legitimate activities with appropriate safeguards and that the processing relates solely to the staff or to persons who have regular contact with Apex Steel Ltd, and the personal data is not disclosed outside that Apex Steel Ltd without the consent of the data subject.

b) The processing relates to personal data that has been made public by the data subject.

c) Processing is necessary for:

   i. The establishment, exercise or defence of a legal claim.

   ii. The purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject.

   iii. Protecting the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.

## 17. Transferring personal data out of Kenya

Apex Steel Ltd will transfer personal data out of Kenya only when they have:

a) Proof of appropriate measures for security and protection of the personal data, and the proof provided to the Data Protection Commissioner in accordance with Kenya's Data Protection Act, 2019, such measures include that data is transferred to jurisdictions with commensurate data protection laws.

b) The transfer is necessary for the performance of a contract, implementation of pre-contractual measures such as:

   i. For the conclusion or performance of a contract to which the data subject is part of.
   ii. For matters of public interest.
   iii. For legal claims.
   iv. To protect the vital interests of data subjects.
   v. For compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

Apex Steel Ltd will process sensitive personal data out of Kenya only after obtaining the consent of a data subject and on receiving confirmation of appropriate safeguards.

## 18. Onward reporting

In line with regulatory requirements, Apex Steel Ltd will report to the Data Protection Commissioner any data breach within 72 hours of being aware.

Apex Steel Ltd will also communicate the data breach to the data subject as soon as is practical unless the identity of the data subject cannot be established.

## 19. Training and awareness

Apex Steel Ltd will train staff on the contents and implementation of this policy. Staff who join Apex Steel Ltd will be required to go through an induction process that entails familiarisation with this policy.

Apex Steel Ltd will ensure that the requirements of this policy form part of its agreement with its grantees, contractors and third parties who process Apex Steel Ltd's data.

## 20. Grantees or partners

Grantees and partners of Apex Steel Ltd must report breaches of Apex Steel Ltd's data in their custody within 48 hours using the emails provided above.

Grantees and partners must also abide by this policy and institute adequate mechanisms to safeguard the privacy of individuals data.

## 21. Roles and responsibilities

**All staff** must:

a) Read, understand and comply with the contents of this policy
b) Report suspicions of breaches promptly

**All project leads and managers** must

a) Ensure staff and third parties they work with are aware of the contents of this policy
b) Conduct risk assessments, and update controls and procedures to mitigate the risk of data breaches

**The IT Executive** is responsible for ensuring employees, consultants, vendors, and partner organisations are aware of the policy and are supported to implement and work by it, as well as creating a management culture that encourages a focus on data protection.

**The Board of Directors** will provide governance oversight of activities under this policy and will ensure that there are adequate and effective systems and process in place to safeguard data.

## 22. Independent assurance

The adequacy and effectiveness of Apex Steel Ltd's data protection procedures is subject to the regular internal audit reviews where necessary Apex Steel Ltd may call an external review provide assurance over the integrity.

## 23. Data retention

The Data retention period in Apex Steel Ltd is determined by legitimate needs. Adequate records of decision making will be maintained to show cause.

## 24. Review of this policy

The IT Exectuive is responsible for ensuring that this policy is reviewed on a timely basis. This policy will be reviewed after every two years and accordingly approved by the Board of Directors.

## 25. Related policies

This policy should be read in conjunction with:

a) Code of conduct
b) Misconduct, disciplinary and grievance policy
c) Information security policy