AUTOMOTIVE PARTS MANUFACTURERS ASSOCIATION

Data Protection Policy

Date of Revision	Two years after approval
Policy Owner	Secretariat
Status	Public

Version Control

Version	Submitted	Reviewed	Approved
1-2025	27-05-2025	27-05-2025	12-07-2025

APMA Data Protection and Privacy Policy 2025

AUTOMOTIVE PARTS MANUFACTURERS ASSOCIATION

Table of Contents

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) operationalized 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, minimizing the collection of data, ensuring the accuracy of data and adopting security safeguards to protect personal data.

2 Policy Statement

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

APMA Kenya 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. APMA holds Personal Data about our employees, Members, Partners and Committee Members for a variety of purposes as detailed in clause 3 of this Policy.

3 Purpose

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

4 Scope

The policy applies to:

a) Employees of APMA Kenya and all APMA Kenya's associated parties such as Committee Members, APMA Members, Partners, vendors, contractors and any other third party who handle and use APMA Kenya information (where APMA Kenya 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 APMA Kenya;

b) All personal data processing APMA Kenya carries out for others (where APMA Kenya 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

"Consent" means that the Data Subject or as appropriate parent or the legal guardian has been fully informed of the clear intended processing and has signified their agreement, while being in a fit state of mind to do so and without pressure being exerted upon them. The Data Subject, parent, or legal guardian, as the case may be, must give Consent freely of his or her own accord.

"Data controller[1]" 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.

Data processor[1] means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

"Data Protection Officer" for the purpose of this Policy, the Data Protection Officer is

The Secretariat.

Data subject[1] means an identified or identifiable natural person who is the subject of personal data.

"Identifiable natural person[1]" means a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity;

"Partners" means donors, consultants, suppliers and any parties we have a contractual relationship with and their respective subcontractors.

Personal data[1] means any information relating to an identified or identifiable natural person

A personal data breach[1] means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed

Processing data[1] 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.

"Regulatory Requirements" refer to all relevant national and international laws on data protection applicable to APMA's operations that shall be in force at the time.

Sensitive personal data[1] 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 spouse's sex, or the sexual orientation of the data subject.

"Third Party" means any individual/organisation other than the Data Subject, APMA or Partners.

[1]Adapted from the Kenya Data Protection Act

6 Principles

APMA Kenya 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 unauthorized 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.
h) APMA shall inform Data Subjects of the reasons for Processing their Personal Data, how it uses such Personal Data, the legal basis for Processing and where required seek Consent from the Data Subject. It shall not process Personal Data of Data Subjects for other incompatible reasons.
i) Sensitive Personal Data shall be Processed with strict controls as set out in Section 17 of this Policy and within available technological constraints.

7 Data Protection Officer

APMA Kenya has designated the Secretariat to be the Data Protection Officer (DPO). Accordingly, the DPO will:

a) Advise APMA Kenya on requirements for data protection, including data protection impact assessments.
b) Ensure that APMA Kenya has complied with the legal requirements on data protection.
c) Facilitate capacity building in data processing operations.
d) Cooperate with external regulators on matters relating to data protection. APMA Kenya's DPO can be contacted via the email: apma.kenya@gmail.com.

8 Duty to notify

APMA Kenya has a duty to notify data subjects of their rights before processing data. APMA Kenya 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 APMA Kenya'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

All Processing undertaken by APMA must be lawful. It is only lawful to undertake the Processing of Personal Data where the Processing is in accordance with Regulatory Requirements and on the following basis:

a) With the informed consent of the data subject.
b) Processing is necessary for the performance of a contract with the Data Subject or to take steps to enter into a contract;
c) To comply with the APMA Kenya's legal obligations.
d) Processing is necessary to protect the vital interests of a Data Subject or another person;
e) Processing is necessary to protect the confidentiality, integrity and availability of APMA's information assets.
f) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller;
g) Necessary for the purposes of legitimate interests pursued by the Data Controller or a Third Party, except where such interests are overridden by the interests, rights or freedoms of the Data Subject or;
h) For historical, statistical, journalistic, literature and art or scientific research.

10 Roles and responsibilities

APMA's Responsibilities

a) APMA is a Data Controller and/or Data Processor under the data privacy regulations. Where APMA engages a Third Party to process Personal Data (such as payroll), an agreement that is compliant with Regulatory Requirements shall be set up with the supplier/service provider. APMA must require sufficient guarantees under data privacy laws from Data Processors including sufficient guarantees that the rights of Data Subjects shall be respected and protected.
b) Regularly review and only retain Personal Data relevant to the purpose it was provided for.
c) Document the type of Personal Data APMA Processes, the Processing purposes and the lawful basis for Processing.
d) Comply with data protection principles as detailed in clause 6 of this policy.
e) Enable the Data Subjects to exercise their rights as described in clause 8 of this policy.
f) Receive appropriate training on data protection requirements.
g) Implementing and reviewing procedures to detect, report and investigate Personal Data breaches.
h) Store Personal Data in safe and secure ways.
i) Assess the risk that could be posed to individual rights and freedoms should Personal Data be compromised.

Responsibilities of APMA Secretariat.

a) The Secretariat should ensure they are familiar with this Policy in the Processing of all Personal Data to which they have access in the course of their duties.
b) The Secretariat is are expected to:
    i. Use Personal Data responsibly and in accordance with the Data Protection Principles;
    ii. Exercise caution before disclosing Personal Data both within and outside APMA, or before using it in email, through the internet or intranet;
    iii. Report any loss or compromise of their own or others' Personal Data to the Data Protection Advisory Committee;
    iv. Take all necessary action to keep Personal Data secure, no matter its form or format, including by the proper management of electronic devices, including mobile devices and computer access; implementing and complying with rules on access to APMA premises and secure electronic and hard copy file storage and destruction, and in accordance with corporate policies and guidance.
    v. Where Personal Data is to be disposed of, the Data Protection Officer should ensure that it is destroyed securely subject to retention requirements. It must be remembered that the destruction of Personal Data is of itself Processing and must be carried out in accordance with the data protection principles;
    vi. The Secretariat must not send other people's Personal Data from an APMA device including laptop, desktop, tablet or mobile phone to a personal email account such as an account not owned or controlled by APMA, except where it is legally permitted to do so;
    vii. Where employees' Personal Data needs to be taken off site the Secretariat must ensure that appropriate steps are taken to protect it; be it in hard copy, stored on a laptop or other electronic device. For the removal of hard copy information, prior consent should be obtained from the Data Protection Advisory Committee.
    viii. Care must also be taken when observing Personal Data in hard copy or on-screen so that such information is not viewed by anyone who is not legitimately privy it.
    ix. If the Secretariat is in any doubt about what they may or may not do with Personal Data, they should seek advice from the Data Protection Advisory Committee before taking any action; and
    x. Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this Policy or Regulatory Requirements without delay.

Responsibility for this Policy;

a) The Data Protection Officer, who is the General Counsel for the purpose of this Policy, has overall responsibility for APMA's Personal Data protection compliance and the day-to-day implementation of this Policy.
b) A Data Protection Advisory Committee that shall be appointed by the board from time to time.

11 Minimization of collection

a) APMA Kenya 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.

b) APMA Kenya will collect and process data that is adequate, relevant, and limited to what is necessary. APMA Kenya Secretariat must not access data which they are not authorized to access nor have a reason to access.

c) 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.

d) The Secretariat must ensure that they delete, destroy, or anonymize any personal data that is no longer needed for the specific purpose for which they were collected.

12 Accuracy of data

APMA Kenya 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.

13 Safeguards and security of data

APMA Kenya has instituted data security measures to safeguard data. These measures serve to safeguard personal data and must be complied with accordingly.

14 Processing data relating to a child

APMA Kenya 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 APMA Kenya Safeguarding policy.

APMA Kenya will institute adequate mechanisms to verify the age and obtain consent before processing the data.

15 Data protection impact assessment

APMA Kenya 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.

Data Protection Impact Assessments will be undertaken when a new business process or processing activity is developed that involves the use of Personal Data.

16 Processing sensitive personal data

APMA Kenya 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 APMA Kenya, and the personal data is not disclosed outside that APMA Kenya 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 defense 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 Procurement

Data protection issues must be considered at the point of procurement where the goods or services being procured have an impact on data protection and involve the handling of Personal Data.

Before a new supplier can be involved in the processing of Personal Data held by APMA, a contract must exist which sets out the obligations and requirements of the supplier to the processing of the Personal Data. The supplier must be subject to appropriate due diligence in regard to their data protection practices.

APMA shall maintain a register of organizations whose data protection practices have been verified and approved and a record of the contract that is in place.

18 Data Sharing

APMA shall ensure that no Personal Data is transferred to a country or organization unless that country or organization ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data, unless such transfer is for compliance with APMA's data protection policy.

APMA shall in some circumstances have to share Personal Data with Third Parties, including service providers and other statutory bodies. APMA shall require Third Parties to fully comply with this Policy.

APMA shall ensure that Personal Data held in organizational ICT resources that traverse national boundaries are shared across systems (such as websites, integrated information systems among others) in compliance with this Policy and/or applicable Regulatory Requirements.

19 Data Protection Breaches

Failure to observe the Data Protection Principles within this Policy may result in the employee and Third Parties incurring personal criminal liability. It may also result in disciplinary action up to

and including dismissal of an employee where there are significant or deliberate breaches of this Policy, such as accessing Personal Data without authorization or a legitimate reason to do so.

Employees must immediately report to the Data Protection Officer and the Data Protection Advisory Committee any actual or suspected data protection breaches.

If APMA discovers that there has been a breach of employee-related Personal Data that poses risk to the rights and freedoms of individuals, it shall inform affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken to address the breach.

Where APMA engages Third Parties to process personal data on its behalf, such parties do so based on written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organizational measures to ensure the security of data.

APMA shall not be held responsible for disclosure of Personal Data in its possession that is also held in other public or private systems.

20 Training and awareness

APMA Kenya will train staff on the contents and implementation of this policy. Staff who join APMA Kenya will be required to go through an induction process that entails familiarization with this policy.

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

21 Grantees and partners

Grantees and partners of APMA Kenya must report breaches of APMA Kenya'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.

22 Independent assurance

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

23 Data retention and Disposal

Personal Data should not be retained longer than is required for the lawful processing of the Personal Data. Once the Personal Data is no longer required for a specific purpose then it must be disposed of in a way that protects the rights and privacy of Data Subjects or Anonymized Personal Data and maintains a trail of activity on the Personal Data for compliance purposes.

There are a range of different legal and statutory obligations requiring the retention of information that impact APMA's activities as a Data Controller. Personal Data must be retained in accordance with all applicable Regulatory Requirements.

24 Routine Publication of Information

APMA publishes a number of items that include Personal Data which includes but is not limited to:

a) Names of all members of the Committee.
b) Names of APMA members.
c) Names and job titles of employees
d) Internal telephone directory
e) Information in prospectuses (including photographs), brochures, annual and other reports, and newsletters.
f) Employee, Committee Members and APMA Members information on APMA website and social media pages, including photographs.
g) Information about stakeholders that interact with APMA in its day-to-day activities.

It is recognised that there might be occasions when a Data Subject, requests that their Personal Data in some of these categories remain confidential or are restricted to internal access. The individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, APMA should endeavor to comply with the request where possible and ensure that appropriate action is taken. However, where the Personal Data is published for regulatory reasons or where the Personal Data is published because of a legal, compliance or security obligation then the information shall continue to be published.

25 Compliance

APMA complies with all Regulatory Requirements. It is the responsibility of all APMA employees and stakeholders to ensure, by taking legal advice, that they are aware of all laws, regulations and policies which may affect the area of work in which they are engaged.

Likewise, APMA complies with obligations placed on us by our development partners. It is the responsibility of all APMA employees to ensure that they understand and comply with requirements of Partners.

Where there is any doubt about compliance requirements related to Regulatory Requirements or obligations from Partners, further guidance should be sought from the office of the General Counsel.

26 Review of this policy

The Secretariat 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 Committee.

27 Privacy Complaints or Breaches

If an individual wishes to access or change their personal information, or to lodge a complaint about a possible breach of privacy or has any query on how personal information is collected or handled, they should contact the Data Protection Officer by mail through:

The Secretariat

Automotive Parts Manufacturers Association of Kenya

P.O BOX 18628 – 00500

Nairobi, Kenya

apma.kenya@gmail.com

Signed by and on behalf of APMA

.....

Mr. Pavit Kenth

Secretary

Date 14/07/2025

.....

Mr. Ashit Shah

Chairman

Date 16/7/25