DATA PROTECTION POLICY

1. INTRODUCTION

AUTO SPRINGS EAST AFRICA PLC (ASEAP) collects and uses personal information about ASEAP staff, customers, partners, suppliers, visitors, and other interested parties (**YOU**), who come into contact with the company. This information is gathered in the process of ASEAP conducting its daily operations and assists in meeting its internal management system requirements. In light of this, ASEAP is committed to ensuring that it abides and remains compliant to the law in its entirety, in the collection and use of such data and/or information. ASEAP is therefore committed to processing personal data in its possession and/or under its control in such a manner that safeguards the privacy and confidentiality of the data and those persons and legal entities represented by it. ASEAP has implemented policies and procedures to assure security during the collection, retrieval, distribution, access, use, change, disclosure, storage, retention, and disposition of personal data provided to and approved by ASEAP, in compliance with the Kenya Data Protection Act 2019.

2. PURPOSE

This policy is developed to communicate to YOU how ASEAP implements data and information-related transactions on all personal soft and hard copy forms of data and information for legitimate business reasons by obtaining consent before any such data and information-related transactions are pursued. All ASEAP staff involved in the execution of all data and information-related transactions will be aware of their duties and responsibilities relating to this policy and as such are expected to exercise their mandate while strictly adhering to the guidelines prescribed herein per the Kenya Data Protection Act 2019, the regulations made under the act and any other related legislation.

3. DEFINATIONS

The following terms as used in this policy are defined below.

a) **Data Subject: -** means an identified or identifiable natural person who is the subject of personal data i.e. person whose data has been collected.

b) **Biometric data: -** means personal data resulting from specific technical processing based on physical, physiological, or behavioral characterization including blood type, fingerprint, deoxyribonucleic acid-DNA analysis, facial features recognition, retinal scanning, and voice recognition.

c) **Personal data: -** means any information relating to a data subject.

d) **Personal data breach: -** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure/transmission/access to personal data that is transmitted, stored, or otherwise processed.

e) **Sensitive personal data**: means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, gender, physical, physiological or behavioral characterization, property details, marital status, family details including names of the person's children, parents, spouse or spouses or sexual orientation of the data subject

4. COLLECTING AND USE PERSONAL DATA

4.1. ASEAP may collect personal data and/or information when performing one or several of the following services for and on behalf of **YOU** or when **YOU** choose to engage us through but not limited to the following channels:

a) Visiting the ASEAP company website and other social media platforms (through the use of cookies/mobile advertising IDs and other technologies) and leaving behind your contact and other relevant information that may be personal to you
b) Contacting ASEAP via their respective electronic business mail, letters through the postal service, or phone calls
c) Signing up for ASEAP news alerts or newsletters
d) Subscribing to the use of our products/Services either as a walk-in customer, an OEM (Original Equipment Manufacturer) and/or corporate customer or through opening a business account to purchase our product(s)
e) Participating in a survey
f) Taking part in a job application process by submitting your curriculum vitae and job application forms to ASEAP directly, through recruitment agencies working on behalf of ASEAP and/or through the company recruitment portal
g) As an interested party by visiting our facility/business premises to evaluate our business for specific industry and/or legal reasons
h) When engaged as an employee or a student under attachment/internship/apprenticeship. Data such as your name, name of your spouse, name of children, academic and professional certificate, contacts details, curriculum vitae, Birth certificate, National identity card/Passport or other identification documents, photographs and audio-visual recording provided to AEAP or taken by ASEAP, medical data, religion etc.
i) As a supplier of goods and services to ASEAP.

4.2. Use of personal data by ASEAP

ASEAP processes personal data on YOU in accordance with the data protection principles as outlined below.

a) The data is used for the purposes of managing staff, management of business transactions between ASEAP customers, suppliers, service providers, creditors and other parties as prescribed in the introduction paragraph.
b) ASEAP may make use of limited personal data (such as contact details) for marketing, to maintain relationships with YOU, and any other legitimate purpose, but only where consent has been provided for the use of their personal data.
c) Any wish to limit, object to any use of personal data or to exercise any of the data subject rights detailed in Section 5 of this Policy should be addressed to the school Data Protection Officer in writing, which notice will be acknowledged in writing. If, in the view of the Data Protection Officer, the objection or attempt to exercise the data subject's rights cannot be maintained, the individual will be given written reasons why the ASEAP cannot comply with their request.
d) Personal data shall be retained for a period no longer than is necessary for the purposes for which it is obtained and processed. Data retention will be done in line with legal requirements and ASEAP'S operational needs.

Where personal data has satisfied the purpose for which it was obtained and processed, ASEAP may still retain the data if the retention is required or authorized by law, where the retention is reasonably necessary for a lawful purpose, where the retention is consented to by the data subject, or where the retention is necessary for historical, statistical, or research purposes.

5. DATA PROTECTION PRINCIPLES

In general,records containing information about individual members of staff or students on attachment/internship/apprenticeship are kept indefinitely by the Human Resource Manager. Other information relating to individual members of staff will be kept by Human Resources Manager.

ASEAP will ensure that the following principles governing data protection are adhered to at all times.

5.1. That personal data is: processed in accordance with the right to privacy;
5.2. Processed lawfully, fairly and in a transparent manner;
5.3. Collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
5.4. Data minimization; Adequate, relevant and limited to what is necessary;
5.5. Accurate and where necessary, kept up to date with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
5.6. Kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected.
5.7. Non-transferrable to third party or outside Kenya, unless there is proof of adequate data protection or consent from the data subject

6. DATA SUBJECT RIGHTS

6.1. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act, 2019 and all the Regulations made under the Data Protection Act 2019. Data subjects from whom ASEAP collects personal data shall have the right:

a) To be informed of the use to which their personal data is to be put;
b) To access their personal data;
c) To object to the processing of all or part of their personal data;
d) To correct false or misleading data; and;
e) To delete on of false or misleading data about them.

6.2. The above rights shall be subject to the requirements and limitations set out in the Data Protection Act 2019 and the Regulations made under the Data Protection Act 2019.

7. GENERAL STATEMENT

7.1. ASEAP is committed to maintaining the above principles at all times. ASEAP will strive to ensure:

a) That individuals are informed why the information is being collected when it is collected;
b) That individuals are informed when their information is shared, and why and with whom it was shared;
c) That the quality and accuracy of the information collected is of the highest standards;
d) That when obsolete information is destroyed that it is done so appropriately and securely;
e) That clear and strong safeguards are in place to protect personal information from loss, theft and unauthorized disclosure;
f) That information with others is only shared when it is legally and professionally appropriate to do so;
g) That ASEAP staff are aware of, and understand, policies and procedures related to Data protection.

7.2. ASEAP will be taking reasonable steps to ensure that personal data is relevant to its intended use, accurate, complete and current, they will rely on their data subjects to assist in providing accurate updates of their personal data.

8. DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

The following list includes the most usual reasons that ASEAP will authorise disclosure of personal data to a third party:

8.1. To give a confidential reference relating to a current or former employee, students on attachment/internship/apprenticeship or volunteer;
8.2. For the prevention or detection of crime;
8.3. where it is necessary to exercise a right or obligation conferred or imposed by law upon ASEAP (other than an obligation imposed by contract);
8.4. For the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
8.5. For the purpose of obtaining legal advice;
8.6. For research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);
8.7. To disclose details of a staff's medical condition where it is in the staff's interests to do so and there is a legal basis for doing so, for example for medical advice or insurance purposes
8.8. All requests for the disclosure of personal data must be sent to the ASEAP Data Protection Officer who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

9. DATA PROTECTION IMPACT ASSESSMENT

9.1. ASEAP will strive to perform an annual Data Protection Impact Assessment which will include:
   a) A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by ASEAP;
   b) An assessment of the necessity and proportionality of ASEAP's data processing operations in relation to the purposes of the processing;
   c) An assessment of the risks to the rights and freedoms of the data subjects governed by this Policy; and
   d) The measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Data Protection Act, considering the rights, and legitimate interests of data subjects.
9.2. Strathmore School will also conduct Data Protection Impact Assessment on a case-to-case basis where the processing of personal data is likely to result in a high risk to the rights and freedoms of data subjects.

10. INCIDENCE RESPONSE

10.1. Where there is a data breach caused by the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed, ASEAP will implement immediate incident response mechanisms to prevent any such actions.
10.2. ASEAP's incident response will be done in the following four steps:
   a) **Step 1:** Report and notify the data subject of sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach;
   b) **Step 2:** Detection of breach and analysis;
   c) **Step 3:** Containment, eradication and recovery;
   d) **Step 4:** Post incident investigation and report
10.3. To mitigate or address any such incidents, ASEAP will notify and work with the Office of the Data Protection Commissioner to take any actions required of ASEAP under the Data Protection Act 2019 and the Regulations made under the Data Protection Act 2019.
10.4. Any suspected or actual data breaches may be reported to ASEAP as a complaint in accordance with Section 10 of this Policy.

11. AMMENDMENT

ASEAP reserve the right to amend this notice from time to time consistent with the applicable standard, regulatory, statutory and legal requirements.

12. ENQUIRIES AND COMPLAINTS

General enquiries relating to data handling should be addressed to dataprotection@autosprings.net
Complaints may be referred to the CEO using the email address: info@autosprings.net

APPROVED BY:

C.E.O: NEPHAT NJENG'WA

DATE: 31/01/2024

SIGN: