AESC Privacy Policy

1. Objective

This policy regulates the Company Policy concerning the protection of Personal Data of data subjects as meant in the General Data Protection Regulation (GDPR), with enforcement date May 25th 2018. It concerns the way we have to handle with Personal Data and it describes Data security measures that have to be taken.

2. Applicability

This policy is applicable to all AESC employees and all those processing personal data of data subjects who are in the EU.

3. Policy

Policy Statement

Every day our business will receive, use and store personal information about our (potential) clients, suppliers, business relationships and colleagues. It is important that this information is handled lawfully and appropriately in line with the requirements of the General Data Protection Regulation (here after referred to as the 'GDPR').

We take our data protection duties seriously, because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

About This Policy

This policy, and any other documents referred to in it, sets out the basis on which we will process any personal data we collect or process.

All employees are expected to adhere to this Policy.

What is Personal Data?

Personal data means data (whether stored electronically or paper based) relating to an individual who can be identified directly or indirectly from that data (or from that data and or in combination with other information in our possession).

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, organizing, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes personal data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offenses or convictions. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.

Data Protection Principles

Anyone processing personal data, must ensure that data is:

a. Processed fairly, lawfully and in a transparent manner.
b. Collected for specified, explicit and legitimate purposes and any further processing is completed for a compatible purpose.
c. Adequate, relevant and limited to what is necessary for the intended purposes.
d. Accurate, and where necessary, kept up to date.
e. Kept in a form which permits identification for no longer than necessary for the intended purposes.
f. Processed in line with the individual's rights and 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.
g. Not transferred to people or organizations situated in countries without adequate protection and without firstly having advised the individual.

Fair and Lawful Processing

The GDPR are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual.

In accordance with the GDPR, we will only process personal data where it is required for a lawful purpose. The lawful purposes include (amongst others): whether the individual has given their consent, the processing is necessary for performing a contract with the individual, for compliance with a legal obligation, or for the legitimate interest of the business. When sensitive personal data is being processed, additional conditions must be met.

Processing for Limited Purposes

In the course of our business, we may collect and process the personal data set out in the Schedule 1 (internal document). This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, location data, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

We will only process personal data for the specific purposes set out in the Schedule 1 or for any other purposes specifically permitted by the GDPR. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

Notifying Individuals

If we collect personal data directly from an individual, we will inform them about:

a. The purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing.
b. Where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued.
c. The types of third parties, if any, with which we will share or disclose that personal data.
d. The fact that the business intends to transfer personal data to a non-EEA country or international organization and the appropriate and suitable safeguards in place.
e. How individuals can limit our use and disclosure of their personal data.
f. Information about the period that their information will be stored or the criteria used to determine that period.
g. Their right to request from us as the controller access to and rectification or erasure of personal data or restriction of processing.
h. Their right to object to processing and their right to data portability.

i. Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn.
j. The right to lodge a complaint with the a supervisory authority.
k. Other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources.
l. Whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data.
m. The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

If we receive personal data about an individual from other sources, we will provide them with this information as soon as possible (in addition to telling them about the categories of personal data concerned) but at the latest within 1 month.

Adequate, Relevant and Non-excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

Accurate Data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

Processing in line with Data Subject's Rights

We will process all personal data in line with data subjects' rights, in particular their right to:

a. Confirmation as to whether or not personal data concerning the individual is being processed.
b. Request access to any data held about them by a data controller (see also Clause 15 Subject Access Requests).
c. Request rectification, erasure or restriction on processing of their personal data.
d. Lodge a complaint with a supervisory authority.
e. Data portability.
f. Object to processing including for direct marketing.
g. Not be subject to automated decision making including profiling in certain circumstances.

Data Security

We will take appropriate security measures against unlawful or unauthorized processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a. **Confidentiality** means that only people who are authorized to use the data can access it.
b. **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
c. **Availability** means that authorized users should be able to access the data if they need it for authorized purposes. Personal data should therefore be stored on the ATS Global B.V. central computer system instead of individual PCs.

Security procedures include:

a. **Entry controls**. Any stranger seen in entry-controlled areas should be reported.
b. **Secure lockable desks and cupboards**. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
c. **Data minimization**. Data being not necessary or irrelevant for the intended purposes should not be collected and will therefore be out of reach.
d. **Pseudonymization and encryption of data**. The personification will be kept away.
e. **Methods of disposal**. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
f. **Equipment**. Staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

Subject Access Requests

In the case that an individual wants to have access to his personal data, he must make a formal request for information we hold about him. An employee who receives a request should forward it to the process owner immediately.

When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

a. We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
b. We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

Where a request is made electronically, data will be provided electronically where possible.

Our employees will refer a request to their line manager (Process owner) or the Data Protection Officer for assistance in difficult situations.

Changes to this Policy

We reserve the right to change this policy at any time. Where appropriate, we will notify changes by mail or email.