

Data Protection Policy

AW (TC) Europe

V 1.3 (07/2018)

1. Introduction

In the performance of its activities, AW (TC) Europe processes various data, both commercial and personal.

This policy, which aims at teaching employees how to treat personal data, deals with the processing of personal data carried out by AW (TC) Europe.

The personal data that is subjected to processing by AW (Technical Center) Europe SA is the personal data relating to employees, clients, and potential clients, visitors of our website, suppliers or any other person contacting us.

AW (TC) Europe understands the importance of data protection and the concerns of its employees, clients and clients' contact persons, suppliers and suppliers' contact persons and other people with whom it has contacts regarding the processing of their personal data. AW (TC) Europe always carefully considers data protection during the different personal data processing operations.

Different people within the company may have access to the personal data of its employees (the term employees shall include: everyone who works for AW(TC) Europe, including managers, independent service providers and consultants, temporary workers such as agency workers, trainees, student workers, volunteers, former workers) and other individuals (clients and suppliers) in the performance of their duties. Each of these people within AW (TC) Europe is bound by this policy.

The legislation regarding data protection imposes obligations on AW (Technical Center) Europe SA regarding the way it needs to process personal data. Moreover, the legislation regarding data protection provides rights for the workers whose data is processed, in order for them to have more control over their personal data.

This policy gives an overview of the general obligations that AW (Technical center) Europe SA and its workers must respect in the frame of the legislation regarding data protection. The respect of this policy is important for the following reasons:

- The respect of the legislation regarding personal data is a legal obligation. The failure to respect these duties may generate responsibility, sanctions and fines.
- The respect of the legislation regarding personal data leads to a more correct and efficient processing of personal data.
- The respect of the legislation regarding personal data holds the base for a mutual trust between AW (technical center) Europe SA and its business relationships, its clients, the individuals whose data is processed as well as its workers.

2. Field of application

This policy applies to AW (Technical Center) Europe SA as data collector, which processes personal data and understands the guidelines to which all data processing must conform, be it by a totally or partially automatized process, and that will be part of a structured file.

The data controller for the purposes of this policy is AW (TC) Europe S.A., with registered office address at Avenue de l'Industrie 19, Parc Industriel, 1420 Braine-l'Alleud, Belgium and registered

at the Crossroads Bank for Enterprises under the numbers: 0441.938.532 for AW Europe SA-0474.474.114 for AW Technical Center Europe SA.

3. Contact point for personal data protection

AW (Technical Center) Europe SA has set up a team responsible for ensuring the execution and respect of the legislation regarding data protection and this policy (hereafter, the data controller).

This team is reachable via email: GDPR@aweurope.be. To exercise any of your rights, see article 8 of this policy.

4. Definitions

The applicable data protection legislation uses specific language and refers to an abstract matter. Hereafter, you will find several definitions in order to allow you to better understand the terminology, and by extension, this policy.

a. Data protection legislation

Various pieces of legislation can apply, depending on the concrete application in which personal data are processed.

The basic principles and obligations are indicated in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. This regulation is also known as the *General Data Protection Regulation (GDPR)*. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and privacy protection in the electronic communications sector is applicable in specific cases (e.g. processing of location data; use of cookies).

As well as the European regulations, specific national data protection legislation also applies, such as the Belgian Law of 8 December 1992 on the protection of privacy with regard to the processing of personal data and the Law of 13 June 2005 on electronic communications.

b. Personal data

Personal data concerns all information about an identified or identifiable natural person, also known as the **data subject**. A person is considered identifiable when a natural person can be directly or indirectly identified, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more elements that are characteristic of the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.

c. Data controller

The **controller** is a natural person or legal person (for example a company), a public authority, agency or other body which, alone or jointly with others, **determines the purposes and means** for the processing of personal data.

d. Processor

The **processor** is a natural person or legal person, a public authority, agency or other body that processes personal data on behalf of and only on instructions from the controller.

e. Processing personal data

Processing personal data means any operation or set of operations performed upon personal data or a set of personal data, whether or not by automatic means (e.g. software), such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

An example of the processing of personal data is collection and storage, in the software for the client management relationship (CRM) of the organization, or in a client file in paper format, of the details of contacts for clients.

f. Filing system

A filing system means any structured set of personal data which is accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

This implies both electronic structured filing systems by means of the use of software or cloud applications, and paper files and filing systems, provided that these filing systems are organized and structured in a logical way by connecting them to individuals or which are connected to individuals on the basis of criteria.

5. Principles applicable when collecting and processing personal data

In addition to having its specific language, personal data legislation has several basic principles which every controller must comply with in order to be in accordance with this legislation.

Legislation imposes the implementation and update of a record which would include all instances of personal data processing. This record is accompanied by an obligation to proceed to a risk analysis in certain cases.

In the event of doubt regarding the application of these principles in a concrete case, do not hesitate to contact the GDPR contact point for further explanations, as described in article 8.

Personal data legislation states that personal data must be processed in compliance with several basic principles and resulting conditions.

a. Lawfulness

GDPR provides that personal data must be processed lawfully and fairly with respect to the data subject.

In order to process personal data lawfully, a legal basis must exist. In principle, personal data can only be processed when:

- **The data subject has given his or her consent.** The company shall inform the person concerned at the latest before the data is collected about the purpose for which consent is required, which personal data will be collected for the processing, the right to revoke consent, the possible consequences for the data subject in the context of automated individual decision-making and profiling, and transfer to third countries.
- The 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.
- The processing is necessary for complying with **a legal obligation** which is imposed upon the organization.
- The processing is necessary for **the protection of the vital interests** of the data subject or another natural person.
- The 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 organization, which acts as the controller.
- The processing is necessary for the purposes of the **legitimate interests** pursued by the company as a controller or the interests of a third party, except where the fundamental rights and freedoms of the data subject regarding the protection of his or her personal data override these interests.

The person involved can revoke the consent they have given to the data controller for the processing of their personal data for a determined purpose at any time. The data controller will then stop any further processing of your data for which you have consented and will inform you of the possible consequences of the withdrawal of your consent. If the data controller processes your personal data for other purposes and in doing so, it refers to other legal bases; it will still be able to process your personal data.

The data controller ensures that it always refers to at least one of the above-mentioned legal bases when it processes personal data... If you have questions about the applicable legal basis that the organization is referring to, you can always contact the data controller by following the procedure mentioned in article 8.

Some categories of personal data are of a sensitive nature and data protection legislation also has a stricter regime for these special categories of personal data (also known as 'sensitive personal

data'). This is data concerning race or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and processing of genetic data, biometric data for the unique identification of a person, or data about health, sexual behavior or sexual orientation. Data relating to criminal offences or convictions also form a special category.

In principle, the processing of these sensitive personal data is forbidden unless the data processing can refer to one of the exceptions. In a limited number of cases, should the data controller process sensitive personal data, the data subject will be informed in advance. In the case of the processing of this data, the data controller must inform the person involved beforehand and in depth of the purposes and the foundations of the processing. For more information about the data controller's handling of sensitive personal data, please contact the data controller by following the procedure mentioned in article 8.

b. Fairness

The data controller ensures that personal data shall be processed:

- For specific, explicit and legitimate purposes and may not be processed further in a way incompatible with the initial purposes for which the data was collected. The data controller shall always clearly communicate the purposes before starting the processing.
- This processing shall be limited to what is necessary for the purposes for which the data was collected. If possible, the data controller will anonymize the data or use pseudonyms in order to limit the impact for the data subject as much as possible. This means that the name or identifier will be replaced so that it is difficult or even impossible to identify an individual.
- Limited in time and only as necessary for the specific purpose.
- Accurately, and the data shall be updated where necessary. The data controller shall take all reasonable measures to erase or update the personal data, taking into account the purposes for which it is processed.

c. Transparency (personal data collected and purposes for processing)

In principle, the data controller processes personal data it has received directly from the data subject and shall inform him/her about the following matters:

- the identity and contact details of the controller;
- the purpose of the processing and its legal basis;
- if the personal data processing is supported by a legitimate interest, an explanation of this interest;
- the (categories of) recipients of the personal data;
- the transfer of personal data to third countries (outside the EU) or international organizations (+ on what basis);
- the time limit for the storage of personal data or the criteria used to determine the time limit;
- the rights of the data subject (including the right to revoke consent);
- the right to lodge a complaint with the related supervisory authority;
- explanation when the transmission of personal data is a contractual or legal obligation;

- the logic behind automated decision-making processes and the possible legal consequences for the data subject;
- if the company receives personal data from a third party, it shall clearly inform the data subject about the categories of personal data which it received from this third party and will also make this third party known to the data subject.

When the data subject already has all the information, the data controller will not inform the data subject unnecessarily about the processing of his/her personal data.

If the data controller processes personal data for other purposes that are incompatible with the purposes for which they were initially collected (the new purpose is not described in the initial information note and the data subject cannot guess that their personal data will also be processed for this new purpose), the data controller will take all the necessary measures to process such data lawfully and will inform the person concerned.

The data controller can provide information on both a collective and individual basis and will always ensure that it is written in understandable and simple language.

Specific legislation may contain exceptions or set additional requirements which the company must comply with, with respect to the provision of information to data subjects. These mandatory legal provisions take precedence over this policy.

d. Confidentiality and integrity

The data controller takes the required technical and organizational measures to ensure that the processing of personal data is always carried out with the appropriate safeguards to protect the data against unauthorized access or unlawful processing and against loss, destruction or damage of accidental origin. When selecting appropriate safety measures, the data collector took into account the nature, the context, the purpose and the scope of the processing, the possible risks when processing personal data, the costs of the measures' execution and the state of the art. Additional measures must be taken in the case of processing sensitive data. In this case, the GDPR team should be contacted via the following email address: GDPR@aweurope.be.

These measures apply to the physical aspect of personal data, to the access of this data via computers, servers, networks or other computer equipment, software applications and data base. In addition to technical and organisational measures, workers who, in the course of their work, have access to personal data, must respect several obligations aiming at ensuring the confidentiality and integrity of personal data as referred in article 9 of this policy.

The data controller will make sure that anyone who receives personal data from the organization applies the legislation on personal data and this policy.

6. Transfer of personal data

In some cases, the data controller may have to transmit personal data to third-party recipients, both inside and outside the data controller's business group. In any case, this personal data is only transferred on a need-to-know basis to these recipients who carry out the processing for specific purposes. The data controller shall always observe the necessary security measures when transferring the data and with respect to the recipients, in order to guarantee the confidentiality and integrity of personal data.

The transfer to third parties can take several forms, as described in more details below.

a. Transfer within the business group of the data controller

Personal data transfers within the business group of the data controller are considered third-party transfers. Thus, it can only occur if the data controller has respected the various principles and obligations imposed by GDPR. This means, among other things, that the data subject must be informed about the transfer and the reason for this transfer and that the data controller must rely on a legal basis for this transfer. In this ulterior processing, the data controller must also comply with the other principles listed in article 5 of this policy.

For transfers of the personal data of the person involved to companies within the group, but which are located outside the European Economic Area (i.e. The European Union, Norway, Iceland and Liechtenstein), AW (TC) Europe set up Standard Contractual Clauses (SCCs) between the company located within the EEA and the company located outside the EEA importing data. You can get a copy of these Standard Contractual Clauses (SCCs) by contacting the data collector whose details are provided hereafter (see article 8)

b. Transfer to processors

The data collector may ask a third party, a processor, to process personal data, on behalf of and only on instructions from the data collector. The processor may not process these personal data for its own purposes which are independent of the purposes for which the data collector uses the processor

The data collector will only collaborate with processors and will provide them with personal data if a processor contract was concluded in compliance with legal requirements. GDPR namely specifies that the contract must contain a clause stating that the processor can only process personal data under instructions of the data collector; that the processor must assist the data collector on their demand; that data must remain confidential; etc.

A section of this processor contract also concerns safety measures that the processor must implement before processing personal data and maintain them for the whole duration of processing to ensure the confidentiality and integrity of data.

The data collector will adopt the necessary measures if they notice the non-compliance with the execution of these processor contracts of their workers.

A standard processor contract is accessible at the purchasing service or on demand via the following address: GDPR@aweurope.be.

c. Transfer to third countries - outside the European Economic Area

It is also possible that the data collector may transfer personal data to parties that are based in third countries, namely countries outside the European Economic Area (the European Union, Norway, Iceland and Liechtenstein) outside the 2 situations stated earlier.

Such a transfer is possible if the country where the recipient is based offers sufficient legal guarantees to protect your personal data and which the European Commission has assessed as being adequate. In other cases, the data collector shall conclude a contract including CCS with the recipient so that equivalent or similar protection to that offered in Europe is offered.

Where this has not occurred or is not possible, the data collector may still transfer the personal data of the data subject, following the consent of the data subject, within the limits of the relationship with AW (TC) Europe. In order to allow the transfer, and therefore the processing, also in these cases, AW (TC) Europe will ask the person concerned if they agree to this occasional transfer to third countries. If more information or a copy of the guarantees for these international transfers is desired, the procedure as described under article 8 can always be followed.

7. Time limit for the storage of personal data

The data collector will not hold personal data for longer than needed for the specific purpose for which it was collected. At the end of the ultimate conservation period, the data collector will delete or anonymize the personal data.

The data collector will anonymize the personal data if they wish to use it for statistical purposes. The data collector may hold the personal data for a longer duration if required by the law (until the statutes of limitations expire), for litigation management, study or archiving purposes.

8. Rights of individual data subjects

Data protection legislation provides for different rights for data subjects with respect to the processing of personal data so that the data subject can still exercise sufficient control over the processing of their personal data.

Through this policy, the data collector is already trying to provide as much information as possible to the data subjects in order to be as transparent as possible with respect to the processing of personal data. This general policy must be read together with more specific information notes which give more explanations about the company's specific processing purposes.

The data collector understands that the data subject may still have questions or desire additional clarifications with respect to the processing of his or her personal data. The data collector thus understands the importance of the rights and shall therefore comply with these rights, considering the legal limitations in the exercise of these rights. The different rights are described in detail below.

a. The right of access

The data subject has the right to obtain confirmation from the data collector of whether or not their personal data is being processed. If their data is being processed, the data subject may request the right to consult their personal data.

The data collector shall inform the data subject of the following:

- the processing purposes;
- the categories of personal data concerned;
- the recipients or categories of recipients to which the personal data are supplied;
- the transfer to recipients established in third countries or international organizations
- if possible, the period during which it is expected that the personal data will be saved, or if this is not possible, the criteria used to determine this period;
- that the data subject has the right to ask the company to correct or erase personal data, or to limit the processing of his or her personal data, as well as the right to object to this processing;
- that the data subject has the right to lodge a complaint with a supervisory authority;
- if the personal data are not collected from the data subject, all available information about the source of the data;
- 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 data subject.

The data collector shall also supply a copy of the personal data that are being processed. For any further copies requested by the data subject, the data collector may charge a reasonable fee.

b. The right to rectification

When the data subject establishes that data collector has incorrect or incomplete data about them, the data subject always has the right to inform the data collector of this fact so that they can take appropriate action to rectify or supplement this data. It is the data subject's responsibility to provide correct personal data to the company.

c. The right to oblivion

The data subject can ask to have their personal data erased if the processing is not in accordance with data protection legislation and within the limits of the law (Article 17 GDPR).

d. The right to restriction of processing

The data subject may request the processing's restriction if:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to check their accuracy;
- the processing is unlawful and the data subject opposes the erasure of the data;
- the data collector no longer needs the data, but the data subject requests that they not be removed, given that they need them for the exercise or defense of legal claims;
- a complaint was filed against the processing, pending the verification whether the legitimate grounds of the controller override those of the data subject.

e. The right to data portability

The data subject has the right to obtain their personal data which they provided to the data collector in a structured, commonly-used and machine-readable format. The data subject has the right to have those personal data transmitted to another controller (directly by the organization). This is possible if the data subject has consented to the processing and if the processing is carried out via an automated process.

f. The right to object

When personal data is processed for direct marketing purposes (including profiling), the data subject can always object to the processing.

The data subject can also object to processing due to a specific situation regarding the data subject. The data collector shall stop processing the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests of the data subject or for the exercise or defense of legal claims.

g. Automated individual decision-making

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 them or similarly significantly affects them such as evaluating personal aspects with respect to the performance of work, reliability, creditworthiness, etc.

This right not to be subjected to such automated decision-making does not exist when the decision is permitted by a mandatory legal provision.

Nor may the data subject invoke this right when the decision is necessary for entering into, or the performance of, a contract between the data subject and the organization or is based on the data subject's explicit consent. In these last two cases, the data subject does have the right to obtain human intervention from a member of the organization and they the right to make their point of view known and to challenge the automated decision process.

h. Right to withdraw consent

If the person involved has given their consent for a specific processing purpose to the data collector in order to process your data, they can withdraw this consent at any time by sending an email to the following address: GDPR@aweurope.be.

i. Procedure for exercising rights and other provisions

The data subject can exercise their rights by sending an e-mail to the GDPR team via the following address: GDPR@aweurope.be;

The data collector may ask the person involved to identify themselves (copy of both sides of the ID card) in order to ensure that the effective exercise of the rights is requested by the data subject.

If you have any question regarding the application of principles or (legal) obligations that the data collector is in charge of, do not hesitate to contact the team in charge of data protection via email.

In principle, the data collector shall respond to the request of the person involved within one month. Otherwise, the data collector informs them of the reasons for their delay in the follow-up of the request. The data controller makes the efforts needed to inform the recipient of the personal data of the person involved that they exercise their right to rectification, to be forgotten and to restriction of processing.

9. Responsibility of the data controller and its workers

The data collector expects of its workers that they comply with this policy and that they demand its compliance from their workers.

It is essential that the workers understand the purposes of this policy and familiarize themselves with it so that they can comply with the dispositions that they contain. Therefore, workers must:

- Process regularly and appropriately the personal data of colleagues, clients, etc. in compliance with the applicable legislation, with the employer's instructions and with the company's confidentiality policy, all the while ensuring integrity and confidentiality;
- In case of doubt over the application of this policy or the compliance of the legislation regarding data protection in the execution of their duties, ask their superior or the data controller for advice;
- Process personal data only if necessary in the execution of their duties/ on instruction from the data controller;
- Receive trainings on confidential data processing and general principles and obligations resulting from the legislation regarding data protection;
- Assist the data controller
- Not keep copies of personal data on the office computer or on a personal medium if the data collector possesses a central storage and safety location, because saving personal files or copies can lead to errors in personal data and increased risks of intrusion;
- Inform immediately the data collector if they notice a potential or actual violation of personal data legislation

10. Compliance

All entities of the data controller's group ensure the compliance with this policy. Each person with access to personal data processed by the data controller must abide by this policy. The non-compliance with this policy can lead to measures, verbal remarks, cautions and/or disciplinary sanctions in the event of repeated offences, for instance a warning, a dismissal or any sanction authorized by the law, without prejudice to its right to file a civil or criminal suit.

11. Revision of this policy

The data controller reserves the right to adjust and review this policy when it deems necessary and to remain coherent with the legal obligations and/or recommendations of the competent supervisory authority for data protection.

If the data controller is unable to comply with this policy as a result of imperative legal dispositions that are imposed to them, they must inform the team in charge of data protection.

12. Links with other internal policies

This policy is completed by:

- P-0174 : Confidentiality information rules
- P-0523 : Information Security Policy
- P-0562 : Industrial Surety & Security Plan