DATA PROTECTION POLICY

This "Data Protection Policy" indicates how TEAM INDUSTRIES deals with the processing of personal data: which personal data are processed, for what purpose, to whom they are transferred, rights of the data subjects, ... It shows the policy of the company (and Group) on data protection.

Data Protection Policy

1. Introduction

In the exercise of the activities of TEAM INDUSTRIES, it processes various data, both commercial data and personal data. This policy concerns the processing of personal data by TEAM INDUSTRIES. The personal data of different categories of identifiable persons are processed, such as employees, customers and suppliers, users of the website, subscribers and other stakeholders.

TEAM INDUSTRIES understands the importance of the protection of personal data and the deliveries of its employees, (contact persons of) customers, (contact persons of) suppliers and other persons with whom they have contact with regard to the processing of their personal data. TEAM INDUSTRIES always takes careful consideration of the protection of personal data in the various processing of personal data.

Several people within the organization can have access to the personal details of their employees (the term employees include managers and everyone who works for TEAM INDUSTRIES, including independent service providers and consultants, temporary employees such as interims, trainees, job students, volunteers ex-employees) and other individuals (customers and suppliers) in the performance of their duties. Each of these persons within TEAM INDUSTRIES is bound by this policy on the protection of personal data.

The applicable data protection regulations impose obligations on TEAM INDUSTRIES as to how they should process data. Moreover, the regulation provides for rights for the persons whose data are processed so that they have more control over their own personal data.
This policy provides an overview of the general obligations under the data protection regulations that the company and its employees must comply with. Compliance with this policy is important for the following reasons:

- Compliance with data protection regulations is a legal obligation and non-compliance with these obligations can result in liability, sanctions and fines;
- Compliance with data protection regulations leads to a more proper and more efficient processing of personal data;
- Compliance with data protection regulations is the basis for a relationship of trust between TEAM INDUSTRIES and its business relations, consumers and employees

2. Application area

This policy applies to TEAM INDUSTRIES that processes personal data and includes the guidelines that must be met by any processing of personal data that may or may not be carried out through fully or partially automated processes and which are part of a structured procedure INDUSTRIES GROUP.

This policy will be applied within the enterprise group except where other mandatory data protection legislation is applicable which implies stricter obligations and conditions.

3. Contact point for the protection of personal data

The company has appointed a responsible, assisted by a team, to ensure implementation and compliance with data protection legislation and this policy.

The person responsible for data protection can be contacted by e-mail lieven.coelus@teamindustries.be or by telephone +32 (0) 9 2544943. For the exercise of your rights, you can go to article 8 of this policy.

4. Definitions

The applicable data protection legislation has its own use of language and it is an abstract matter. Some definitions are included below to allow you to better understand the terminology and, by extension, this policy.

a. Data protection legislation

Different legislations may apply depending on the specific application case where personal data are processed.

The basic principles and obligations are contained in Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95 / 46 / EC. These regulations are also referred to as the General Data Protection Regulation (AVG) or 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 the protection of privacy in the electronic communications sector applies in special cases (like processing of location data; cookies).

In addition to European regulations, the specific national data protection laws apply, such as the Act of 8 December 1992 on the protection of privacy with regard to the processing of personal data and the Act of 13 June 2005 on electronic communications.

b. Personal data

Personal data concern all information about an identified or identifiable natural person, also referred to as the person concerned. A person shall be regarded as identifiable when a natural person can be identified directly or indirectly, in particular by means of an identifier such as a name, identification number, location data, an online identifier or one or more elements characteristic of the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.

c. Processing manager

The controller is a natural or legal person (for example, a company), a government agency, a service or any other body that, individually or jointly with others, determines the purpose and means for the processing of personal data.
For example, TEAM INDUSTRIES is a legal entity that is the controller of the processing of personal data of its employees in the context of its personnel management.

d. Processor

The processor is a natural or legal person, a government body, a service or another body that processes personal data for the benefit of and solely on behalf of the controller.

e. Processing personal data

A processing of personal data is an operation or a set of operations relating to personal data or a set of personal data, whether or not carried out via automated processes (like software), such as collecting, recording, organizing, structuring, storing, updating or changing retrieve, consult, use, provide by means of forwarding, disseminating or otherwise making available, aligning or combining, blocking, erasing or destroying data.

An example of the processing of personal data is when the organization collects the contact details of the contact persons from its clients and stores them in the client relationship management software system of the organization or in a paper customer database.

f. File

A file is any structured set of personal data that is accessible according to certain criteria, irrespective of whether it is entirely centralized or decentralized or has been disseminated on functional or geographical grounds.

This implies both electronic structured files through the use of software or cloud applications, as paper files and files insofar as these files are organized and structured in a logical way by linking them to individuals or that are linked to individuals on the basis of criteria.

5. Applicable principles when collecting and processing personal data

In addition to their own use of language, the data protection legislation has a number of basic principles that every controller must comply with in order to comply with these regulations. In case of doubt about the application of these principles in a specific case, you can always contact the lieven.coelus@teamindustries.be for further explanation and according to the procedure described in Article 8.

The data protection law prescribes that personal data must be processed in accordance with the various basic principles and the resulting conditions.

a. Legality

The data protection law prescribes that personal data must be processed in a manner that is lawful and proper with respect to the data subject.

To process personal data lawfully there will always have to be a legal basis. Personal data can in principle only be processed when:

- The person concerned has given permission. The organization will inform the person concerned at least in advance about the purpose for which permission is sought, which personal data will be collected for processing, the right to withdraw the consent, the possible consequences for the data subject in the context of automated individual decision making and profiling. , and the transfer to third countries
- The processing is necessary for the performance of an agreement in which the party concerned is a party or at the request of the person concerned to take measures before the conclusion of an agreement
- The processing is necessary to comply with a legal obligation imposed on the organization
- The processing is necessary to protect the vital interests of the data subject or of another natural person
- The processing is necessary for the fulfillment of a task of general interest or of a task in the exercise of the public authority which is entrusted to the organization acting as controller
- The processing is necessary for the representation of the legitimate interests of the organization as controller or of a third party, except when the fundamental rights and freedoms of the data subject regarding the protection of his personal data outweigh those interests.

If you have given your permission to the organization for a certain processing purpose to process your data for that purpose, you can withdraw this consent at any time. The organization will then stop to process your data for which you have given your consent and will inform you about the possible

consequences of the withdrawal of your consent. If the organization processes your personal data for other purposes and relies on other legal grounds for this, it will still be able to process your personal data.

The organization ensures that it always relies on at least one of the aforementioned legal bases when processing personal data. If you have questions about the applicable legal basis on which the organization relies, you can always contact us in accordance with the procedure as prescribed in Article 8.

Some categories of personal data are of a sensitive nature and the data protection law also has a stricter regime for these special categories of personal data (also known as 'sensitive personal data'). This concerns data concerning race or ethnic origin, political opinions, religious or philosophical convictions, whether membership of a trade union appears, and processing of genetic data, biometric data with a view to the unique identification of a person, or data on health, or data related to a person's sexual behavior or sexual orientation. Data relating to criminal offenses or convictions also form a special category.

In principle, it is prohibited to process this sensitive personal data, unless the organization can rely on one of the exceptions. In certain limited cases, the organization must process sensitive personal data. In these cases, the person concerned will be informed in advance. For these specific purposes, the organization will provide the person concerned in advance with detailed information about the specific purposes and the basis of the processing. For more information about the processing of sensitive personal data by the organization, you can always contact us in accordance with the procedure described in article 8 of this policy.

b. Prosperity

The organization ensures that personal data will be processed:

- For specified, explicit and legitimate purposes and will not be further processed for purposes incompatible with the initial purpose for which the data were collected. The organization will always communicate the goals clearly before starting the processing.
- Limited to what is necessary for the purposes for which the data were collected. If possible, the organization will anonymize or pseudonymize the data 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 becomes difficult or even impossible to identify an individual.
- Limited in time and as far as necessary for the particular purpose.
- Accurately and the data will be updated as necessary. The organization will take all reasonable measures to delete or improve the personal data, taking into account the purposes for which they are processed.

c. Transparency

The organization processes personal data that it has in principle received directly from the person concerned. The organization that processes the personal data of the data subject will always inform the data subjects about the following:

- identity controller and contact details
- if a data protection officer has been appointed, his contact details
- processing purposes and legal basis
- if there is a legitimate interest in the processing of personal data, an explanation of this interest
- (categories of) recipients of personal data
- Transfer of personal data to third countries (outside the EU) or international organizations (+ on what basis)
- Retention period of the personal data or the criteria on the basis of which the retention period is determined
- Rights of the person concerned (including the right to withdraw permission)
- Right to lodge a complaint with the supervisory authority
- Explanation when the provision of personal data is a contractual or legal obligation
- The logic behind automated decision-making procedures and the possible legal consequences for the data subject
- If the organization receives personal data from a third party, it will clearly inform the data subjects about the categories of personal data it has received from this third party and will also make this third party known to the data subject.

If the person concerned already has all the information, the organization will not inform the person concerned unnecessarily about the processing of his personal data.

If the organization processes personal data for other purposes that are not compatible with the purposes for which the personal data were initially collected (the new purpose does not appear to be described in the initial information note and the data subject can not assume that his personal data will also be used for this new purpose. will be processed), the organization will take all necessary measures to lawfully process these personal data and will inform the data subjects accordingly.

The organization can provide the information both on a collective and on an individual basis and will always ensure that it is drafted in an understandable and simple language.

Special legislation may contain exceptions or impose additional requirements with regard to the provision of information to data subjects that the organization must comply with. These mandatory legal provisions take precedence over this policy.

d. Confidentiality and integrity

The company takes the necessary technical and organizational measures to ensure that the processing of personal data is always carried out with the appropriate safeguards so that the data are protected against unauthorized access or unlawful processing and against unintentional loss, destruction or

damage. In choosing the appropriate safety measures, the organization has taken into account the nature, context, purpose and scope of the processing, the possible risks in the processing of the personal data, the implementation costs of the measures and the state of the art.

These measures apply to physical access to personal data, access to personal data via computers, servers, networks or other IT hardware and software applications and databases. In addition to the technical and organizational measures, the employees of the company, who have access to personal data in the performance of their duties, are subject to various obligations to ensure the confidentiality and integrity of personal data and as listed in article 9 of this policy.

The organization will organize training courses for employees who will process personal data on behalf of the organization in the performance of their duties. Employees may only process the personal data on instructions from the organization or if the law imposes them on doing so. The organization will also implement access rights so that employees only have access to the data they need in the performance of their duties. Employees who have access to personal data will sign a confidentiality agreement.

The organization will ensure that third parties receiving personal information from the organization will comply with the applicable data protection law and this policy.
A general summary of the technical and organizational security measures that the group of companies has introduced can be found in the Safety Policy.

6. Transfer of personal data

In some cases, the organization may be forced to pass on your personal data to third-party receivers, both within the organization's group and outside it . In any case, the personal data will only be transferred on a need-to-know basis to these recipients who carry out the processing for specific purposes. The organization always observes the necessary security measures for the transfer and with regard to the recipients in order to guarantee the confidentiality and integrity of the personal data.

The transfer to third parties can take various forms as described below.

a. Transfer within the organization group of the organization

The transfer of personal data within the enterprise group of the organization is considered as a transfer to a third party. Consequently, this transfer can only take place when the organization has complied with the various principles and obligations of the data protection legislation. This means, among other things, that the data subject must be informed about the transfer and the reason for this transfer and that the transmitting organization can base itself on a legal basis (consent of the data subject, execution of an agreement, legitimate interest, ...) for this transfer. The organization must also comply with the other principles as enumerated in article 5 of this policy during this further processing.

When your personal data are transferred to companies within the group, but which are located outside the European Economic Area (ie the European Union, Norway, Iceland and Liechtenstein), the group of companies provides the appropriate guarantees as described under point c.

b. Transfer to processors

The organization may request a third party, a processor, to process personal data for the benefit of and only on behalf of the organization. The processor may not process this personal data for his own purposes that are separate from the purposes for which the organization uses the processor.

The organization may opt to work with these processors, who provide services at the request of the organization, for travel agencies, rental services, medical and other professional consultants, etc.

The organization will only appeal to processors and provide personal data when processing agreements have been concluded with the processors that meet the legal requirements. The AVG prescribes, among other things, that the agreement must contain a clause stating that the processor can only process the personal data on instructions from the organization; that the processor must provide assistance to the organization at its request; that data must remain confidential; etc.

Part of this agreement processors as well as the security measures that must implement the processor before processing the personal data and should have throughout the duration of the process to ensure the confidentiality and integrity of data.

The organization will take the necessary measures if it determines that its processors do not comply with the obligations under the agreement.

A standard processor agreement is available at lieven.coelus@teamindustries.be .

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

It is also possible that the organization passes on your personal data to parties established in third countries, ie countries outside the European Economic Area (ie the European Union, Norway, Iceland and Liechtenstein).

Such a transfer is possible if the country where the recipient is established offers sufficient legal guarantees to protect your personal data and which the European Commission has assessed as adequate. In the other cases, the organization has concluded a model contract with the recipient so that a similar (w) kind of protection is offered as in Europe.

For cases in which this has not been done or can not be done, the organization can always pass on the personal data of the data subject, subject to the consent of the data subject, within the limits of the relationship the data subject has with the organization. In order to enable transfer and thus processing in those cases, the organization will also ask the person concerned, if applicable, whether this occasional transfer to third countries can be accepted.

If more information or a copy of the guarantees for these international transfers of personal data is desired, the procedure described in Article 8 can always be followed.

7. Storage period of personal data

The organization will not retain personal data for longer than necessary for the specific purpose for which the data was collected. After the expiry of the last storage period, the organization will delete or anonymize the personal data. The organization will anonymize the data if it still wishes to use it for statistics. The organization may retain the personal data longer for its dispute management, investigations or archiving purposes.

8. Rights of the individuals involved

The data protection law provides for different rights for data subjects with regard to the processing of personal data so that the data subject can continue to exercise sufficient control over the processing of their personal data.

By means of current policy, the organization already tries to provide as much information as possible to the data subjects in order to be as transparent as possible with regard to the processing of personal data. This general policy must be combined read with more specific information notes that provide more information about the specific processing objectives of the organization.

The organization understands that the person can still have questions or additional clarifications regarding the processing of his personal data. The organization therefore understands the importance of the rights and will therefore comply with these rights taking into account the legal restrictions in the exercise of these rights. The various rights are described in more detail below.

a. Right of access / access

The data subject has the right to obtain confirmation from the organization about whether or not to process his personal data. In the positive case, the data subject can request access to his personal data.

The organization will inform the person concerned about the following matters:

- the processing purposes;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data have been provided;
- the transfer to recipients in third countries or international organizations;
- if possible, the period during which the personal data are expected to be stored, or if this is not possible, the criteria for determining this period;

- that the data subject has the right to request the organization that personal data be corrected or deleted, or that the processing of personal data relating to him is limited, as well as the right to object to such processing;
- that the person concerned has the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, all available information on the source of that data;
- the existence of automated decision-making, including profiling, and useful information about the underlying logic of this decision-making and the importance and expected consequences of that processing for the data subject.

The organization also provides a copy of the personal data that is being processed. If the person requests additional copies, the organization can charge a reasonable fee.

b. Right to improvement

If the person concerned determines that the organization has incorrect or incomplete personal data, the data subject always has the right to report this to the organization so that the necessary measures can be taken to improve or supplement this data. It is the responsibility of the data subject to provide correct personal data to the organization.

c. Right to forgetfulness

The data subject may request the erasure of his personal data if the processing is not in accordance with the data protection legislation and within the limits of the law (article 17 AVG).

d. Right to limit processing

The person concerned may request that the processing be restricted if

- the correctness of the personal data has been questioned and for the period to check the accuracy;
- the processing is unlawful, and the data subject does not wish to erase the data;
- the organization no longer needs the data, but asks the person concerned not to remove them as he needs them in the exercise or substantiation of a legal claim;
- objection to the processing is made pending the explanation of the legitimate interests that outweigh the interests of the person concerned.

e. Right of transferability

The data subject has the right to obtain his personal data that he has provided to the organization in a structured, current and machine readable form. The data subject has the right to transfer this

personal data (directly by the organization) to another controller. This can be done if the processing is based on the permission of the person concerned and on the basis of a processing by means of an automated process.

f. Right of objection

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

The person concerned may also object to the processing due to a specific situation related to the person concerned. The organization will cease processing unless the organization invokes compelling legitimate reasons for the processing that outweigh the interests of the data subject or that are related to the exercise or substantiation of a legal claim.

g. Automated individual decision making

The data subject has the right not to be subject to a decision based exclusively on automated processing, including profiling, which has legal consequences for him or which otherwise affects him in a significant way such as evaluating personal aspects relating to the execution of work, reliability, creditworthiness, etc.

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

The person concerned can not invoke this right if the decision is necessary for the conclusion or the execution of the agreement between the person concerned and the organization or based on the express permission of the person concerned. In the latter two cases, the person concerned is entitled to human intervention by someone from the organization and he has the right to make his point of view known and to challenge the automated decision.

h. Right to withdrawal of consent

If you have given your organization permission to process your data for a certain processing purpose, you can withdraw this consent at any time by sending an e-mail.

i. Procedure for exercising the rights and other provisions

The person can exercise his rights by sending an e-mail to Lieven Coelus o p lieven.coelus@teamindustries.be or by contacting the latter by telephone on +32 (0) 9 2544943 . The

organization may request the data subject to identify himself to ensure that the exercise of the rights has been effectively requested by the person concerned.

If you have questions about the application of the principles or the (legal) obligations resting on the organization, you can always contact Lieven Coelus via lieven.coelus@teamindustries.be or +32 (0) 9 2544943 .

In principle, the organization will comply with the request of the person concerned within a month. So not, the organization will inform the person concerned why the request has remained without result or can not be followed in time. The organization makes the necessary efforts to inform the recipients of the data subject of the data subject about the exercise of the right of correction, the right to erasure or the restriction of processing by the data subject.

9. Responsibilities of employees

The organization expects its employees to respect this policy and to ensure that this policy is complied with by those for whom they are responsible.

It is crucial that employees understand the goals of this policy and become familiar with them so that they can comply with the provisions contained in this policy. The employees must therefore:

- to process the personal details of fellow employees, customers, etc. in a regular and proper manner in accordance with the applicable legislation, the instructions of the employer and the privacy policy of the company and where personal data are processed in a confidential manner and with due regard for its integrity;
- Board to ask their supervisor, Lieven Coelus, in case of doubt about the application of this policy or about compliance with the data protection legislation in the performance of the function;
- Process personal data only when required for the performance of the function / on behalf of the organization;
- Follow training about the confidentiality of personal data and the general principles and obligations stemming from data protection legislation;
- Provide assistance to the Lieven Coelus.
- No copies of personal data to be stored on the desktop or personal media when there is centralized and secure storage of the organization since the storage of own files or copies may lead to incorrect personal data and higher risks of infringements;
- Inform Lieven Coelus immediately when they identify a possible or actual breach of personal data or data protection legislation.

10. Compliance

All entities that are part of the organization's group ensure that this policy is complied with. Any person who has access to personal data processed by the organization must comply with this policy. Failure to comply with this policy may result in disciplinary action / sanctions such as a warning, resignation or any other sanction that the law allows, without prejudice to the right to bring civil or criminal claims.

11. Audit and review

The organization reserves the right to amend and review this policy whenever it deems it necessary and to remain in compliance with the legal obligations and / or recommendations of the competent data protection supervisory authority.

The organization informs Lieven Coelus if it is impossible for her to comply with this policy as a result of mandatory legal provisions imposed on the organization.

12. Entry into force

This policy applies from May 25, 2018.

13. Technical and organizational security measures

Here after a concise, non-exhaustive overview of a number of technical and organizational safety measures that the organization has introduced.

Organizational measures
- Safety consultant
- Safety and risk plan
- Safety directive
- Raising awareness among staff through information provision and training
- Procedure for reporting physical / technical incidents
- Information classification
- Disciplinary consequences in case of non-compliance with one of the measures
- Recovery plan, contingency plan or emergency plan in case of physical / technical incidents
- Continuity plan
- Plan that ensures that the effectiveness of the organizational / technical measures is regularly checked / evaluated and assessed
- Monthly check of the suitability of the processing systems and services
Technical measures
- Backup system
- Measures in case of fire, burglary or water damage or physical / technical incidents
- Access control (physical and logical)
- Authentication system
- Password policy
- User ID policy
- Logging system , access detection and analysis
- Patching
- Antivirus
- Firewall
- Network security
- Monitoring, research and maintenance of the systems
- Encryption of Personal Data
- Pseudonomization of Personal Data

* note L; The grey marked passages regards legislation that will soon change with the result that the changes will have to be implemented in this policy.