DATA PROTECTION POLICY.

of **ADMEDES GmbH** I Rastatter Str. 15 I 75179 Pforzheim, Germany

CONTENT

INTRODUCTION

Ladies and Gentlemen,

data is constantly collected and processed in the digital era. Where data is saved and sent, there must be guaranteed a high level of data privacy and data security. This applies to our customer's data, potential customers and business partners, as well as our employee's data, for the protection of the person's privacy and security.

It is our claim that ADMEDES GmbH not only stands for ideas, expertise and passion, but also sets standards in data privacy. For us, safeguarding the personal rights and privacy of each individual is the basis for trustful business relationships.

In our company policy for data privacy, we have defined strict requirements for the processing of personal data of customers, potential customers, business partners and employees. This complies with the requirements of the European General Data Protection Regulation (GDPR) and the Federal Data Protection Act (BDSG). In this way, we set a data protection and data security standard in our company.

All employees of ADMEDES GmbH are required to comply with this company guideline for data privacy and to comply with the respective data protection laws.

1. PURVIEW AND ADJUSTMENT OFT HE DATA PROTECTION POLICY

This Data Protection Policy applies to the ADMEDES GmbH as also for all sub companies. The field of application of the Data Protection Policy applies to all processing of personal data.
Data, which was anonymised, e.g. for statistical evaluation, is not subject of this Data Protection Policy. Any adjustment of this Data Protection Policy can only be made in consultation with the data protection officer (DPO). The latest version of the Data Protection Policy can be found on the website of ADMEDES GmbH, www.admedes.com.

2. PRINCIPLES

The safety of personal data is an important matter of ADMEDES GmbH. Therefore, we are processing the personal data of our employees, customers and business partners in accordance with the legal regulations for data processing and data privacy.
This Data Protection Policy describes which kind of personal data we are collecting, how we use it, to whom it is sent and which rights the affected persons have in context of the processing of data. Also, we describe in which way the safety of data is guaranteed and how affected persons can contact us, if they have questions to our Data Protection Policy.
This policy regulates data protection-compliant information, processing and responsibilities existing at ADMEDES GmbH. All employees are compelled to comply with the policy.
The following principles apply:
Hardware and software processing personal data, must only be used for operational tasks, for intended purposes in each case and must be secured against loss and manipulation.
Each employee is responsible for the implementation of the guideline in his or her area of responsibility. The compliance must be checked regularly.
Responsible for the systems processing must ensure that their employees (users) are informed of this policy. This also applies to temporary employees.
The DPO gives advice in the implementation of the policy and checks their compliance. Insofar all addressees of the policy are constrained to provide information to the DPO.

3. THE OPERATIONAL DATA PROTECTION OFFICER/DATA PROTECTION COORDINATOR

3.1. The ADMEDES GmbH has appointed a data protection officer (DPO) in accordance with Article 37 GDPR. The DPO executes tasks assigned to him by law and this policy, by applying his professional knowledge and qualifications.

3.2. Tasks of the DPO:

- Informing and advising management and employees on their data protection obligations
- Monitoring compliance with data protection rules
- Develop personal data protection strategies with those responsible
- Allocation of responsibilities
- Sensitization and training of employees

3.3. In case of high-risk data processing, the DPO assist the responsible person with risk assessment.

3.4. The DPO shall be involved in all data protection issues at an early stage and shall be supported by both management and employees in the performance of his duties.

3.5. As far as it proves to be organizational, the management appoints a data protection coordinator.

3.6. The coordinator ensures, with the DPO, compliance with the data protection rules applicable to the company. He informs the DPO of any data protection issues that have arisen on site.

3.7. The company must keep a register of all processing activities (VVT). In each department, at least one person is responsible for gathering the necessary information on the procedures of the respective department and documenting it in accordance with the requirements of Art. 30 GDPR.
The DPO may be consulted in the event of any ambiguities regarding the information required by law. A copy of the VVT must be passed to the DPO. The VVT must always be kept up to date with support of the DPO.
On request, the company provides the VVT to the supervisory authority. In agreement with the management, the DPO is responsible for this and cooperates with the supervisory authority.

3.8. Every employee can contact the DPO directly with hints, suggestions and complaints, where absolute confidentiality is maintained if requested.

3.9. The DPO reports annually in an activity report the management and the data protection coordinator about audits that have taken place, complaints and any organisational deficiencies that need to be remedied. If the report concerns the processing of personnel data or questions of operational organization, it will also be made accessible to the works council.

4. PROCUREMENT OF HARDWARE AND SOFTWARE

4.1. The procurement of hardware and software is basicallytasks of the IT department. Already during the selection of hardware and software, data protection is considered as a basic criterion by means of data protection-friendly presetting.

4.2. Private hardware and software may not be used to process personal data.

4.3. The IT department keeps a list of the hardware used and the application programs used. The DPO receives a copy.

4.4. The IT department and the DPO must be informed immediately about any suspicion of the hardware and software, unauthorized access to personal data, sabotage, etc.

5. OBLIGATION/TRAINING OF EMPLOYEES

5.1. Every employee who handles personal data must be obligated to handle personal data confidentially and to comply with this policy. The obligation is carried out using the information sheet „Mitarbeiterinformation Datenschutz“ provided for this purpose and in the form attached to it in „Anlage 1“, which contains the obligation to data secrecy in accordance with § 53 BDSG.

5.2. Employees who are subject to special confidentiality obligations (e.g. telecommunications secrecy pursuant to § 88 TKG) will be additionally obligated in writing by their superiors. The respective declaration of commitment has to be attached to the personal files.

5.3. The DPO is responsible for the obligation of employees and their workplace for the purpose of further training to be provided by the DPO and for determining any need for monitoring. He must be informed about new employees, who need to be trained.

5.4. The employees concerned will be released from their duties for the training dates scheduled in consultation with the respective department heads.

6. PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA

6.1. Fairness and legality
The processing of personal data must respect the personal rights of the data subject. Personal data must be collected and processed lawfully and fairly.

6.2. Earmarking
The processing of personal data can only be carried out for the purposes previously defined. Subsequent changes to the purposes are only possible to a limited extent and require justification.

6.3. Transparency
The data subject must be informed about the handling of his/her data. In principle, personal data must be collected from the person concerned. When collecting the data, the data subject must at least be able to identify or be informed of the following:

- The body responsible for processing
- The purpose oft he data processing
- Third parties or categories of third parties to whom the data may be disclosed

6.4. Data reduction and data economy
Before personal data is processed, it must be checked whether and to what extent it is necessary in order to achieve the intended purpose. If it is possible to achieve the purpose and the effort is proportionate to the intended purpose, anonymous or statistical data shall be used. Personal data may not be stored in advance for potential future purposes unless required or permitted by state law.

6.5. Deletion
Personal data that is no longer required after the expiry of legal or business process related retention periods must be deleted. If, in individual cases, there are indications of interests worthy of protection or of a historical significance of these data, the data must remain stored. This is the case until the interests worthy of protection have been legally clarified or the company‘s archives have been able to examine the data stock for its historical purpose and thus for the archival recording.

6.6. Factual accuracy and timeliness of data
Personal data must be stored correctly, completely and if necessary up to date. Appropriate measures have to be taken to ensure that inaccurate, incomplete or outdated data is erased, corrected, supplemented or updated.

6.7. Confidentiality and data security
Data secrecy applies to personal data. It must be treated confidentially in personal dealings and protected by appropriate technical and organizational measures (TOM) against unauthorized access, unlawful processing and disclosure, as well as accidental loss, alteration or destruction.

7. PERMISSIBILITY OF DATA PROCESSING

The collection, processing and use of personal data are only permitted if one of the following authorizations exists. Such permission is also required when it is a matter of simply changing the purpose of the collection, processing and use.

7.1. CUSTOMER AND PARTNER DATA

7.1.1. Data processing for a contractual relationship

Personal data of the interested party, customer or partner concerned may be processed for the justification, execution and termination of a contract. This also includes the support of the contractual partner; insofar it is in connection with the purpose of the contract. In the run-up to a contract - i.e. in the contract initiation phase - the processing of personal data is permitted for the preparation of offers, purchase applications or for the fulfilment of other wishes of the interested party relating to the conclusion of a contract. Interested parties may be contacted during the preparation of the contract using the data provided by them. Any restrictions expressed by the interested party must be observed. The following prerequisites under 7.1.2 must be observed for further advertising measures. Customer names are pseudonymized at ADMEDES GmbH, which means that the customer name is replaced by a pseudonym.

7.1.2. Data processing for advertising purposes

If the data subject contacts ADMEDES GmbH with a request for information (e.g. request for information material), data processing is permitted for the fulfilment of this request. Further measures beyond this require further legal prerequisites. The processing of personal data for purposes of advertising or market and opinion research is permitted if this is compatible with the purpose for which the data were originally collected. The person concerned must be informed about the use of his/her data for advertising purposes. If data is collected exclusively for advertising purposes, its disclosure by the person concerned is voluntary. The data subject shall be informed of the voluntary nature of the data provided for these purposes. Within the communication with the data subject, its consent to the processing of its data for advertising purposes shall be obtained. If the data subject disagrees with the use of his/her data for advertising purposes, further use of his/her data for these purposes is not permitted and must be blocked for these purposes.

7.1.3. Consent to data processing

Data processing can take place with the consent of the data subject. Before consent is given, the data subject must be informed in accordance with 6.3. of the Data guidline for reasons of proof, the declaration of consent must always be obtained in electronically or in written form. Under certain circumstances, e.g. in the case of telephone consultation, consent may also be given orally. The granting of verbal consent must be documented.

7.1.4. Data processing based on legal permission

The processing of personal data is also permitted when national legislation requires, presupposes or permits the processing of such data. The type and extent of data processing must be necessary for the data processing permitted by law and comply with these legal provisions.

7.1.5. Data processing based on legitimate interest

Personal data may also be processed if this is necessary to realize a legitimate interest of ADMEDES GmbH. As a rule, legitimate interests are legal (e.g. enforcement of outstanding claims) or economic (e.g. avoidance of breaches of contract). Personal data may not be processed based on a legitimate interest if in an individual case, there is an indication that the interests of the data subject worthy of protection outweigh the interest of processing. The interests worthy of protection must be examined for each processing operation.

7.1.6. Processing of particularly sensitive data

The processing of particularly sensitive personal data may only take place if this is required by law or if the data subject has expressly consented. Such data can also be processed if it is necessary in order to assert, exercise or defend legal claims against the data subject. If the processing of particularly sensitive data is planned, the DPO or data protection coordinator must be informed in advance.

7.1.7. Automated individual decisions

Automated processing of personal data, which evaluates individual personality traits (e.g. creditworthiness), is not used by ADMEDES GmbH.

7.1.8. User data and Internet

When visiting the Admedes Website, the information from which personal data is collected, processed and used, can be found in the data protection and cookie information on the website. The data protection and cookie notices are integrated in such a way that they are easily recognizable, immediately accessible and permanently available to those concerned. There are no areas requiring registration. The data entered via the contact form or the applicant portal will only be stored and processed for the purposes they have been collected. Data will not be passed to third parties without subject´s consent and will be deleted after the normal periods for deleting the data.

7.2. EMPLOYEE DATA

7.2.1. Data processing for the employment relationship

Personal data necessary for the establishment, execution and termination of the employment contract may be processed for the employment relationship. When initiating an employment relationship, personal data of applicants may be processed. The „Privacy policy by ADMEDES GmbH for applications" applies to applicant data. In the existing employment relationship, data processing must always be related to the purpose of the employment contract, unless one of the subsequent authorizations for data processing intervenes. If it is necessary to collect further information about the applicant from a third party during the initiation of the employment relationship or in the existing employment relationship, the respective national legal requirements must be considered. In case of doubt, the consent of the person concerned must be obtained. For the processing of personal data related to the employment relationship which do not serve the fulfilment of the employment contract, a legal legitimation must exist in each case. These can be legal requirements, collective agreements with employee representatives, employee consent or the legitimate interests of the company.

7.2.2. Data processing due to legal permission

Requirement for the processing of personal employee data is anchored additionally in the law. Nature and extent of the data processing operation must fit on the government regulations and therefore fulfil the requirements for data processing permitted by law. The interests of the employee´s protection worth must be considered, if there subsist any room for manoeuvre at the interpretation of legal requirements.

7.2.3. Collective regulations for data processing

If a processing goes beyond the purpose of the contract it is also valid, when its permitted by a collective regulation. Collective regulations are wage agreements or arrangements between employer and employee union representation within options of the respective employment law. The regulations must extend on the specific purpose of desired processing and must be shaped within the framework of national data protection law.

7.2.4. Consent to data processing

Employee data may be processed with the consent of the data subject. Declarations of consent must be given voluntarily. Involuntary consents are ineffective. The declaration of consent must be obtained in electronically or in written form for reasons of proof. Exceptionally if circumstances do not permit this, consent may be given orally. In any case, the provision of data must be properly documented. In the case of an informed voluntary declaration of data by the data subject, consent can be assumed if national law does not prescribe explicit consent. Prior to consent, the data subject must be informed in accordance with 6.3. of this Data Protection Policy.

7.2.5. Data processing based on legitimate interest

The processing of personal employee data may also take place if this is necessary to realize a legitimate interest of ADMEDES GmbH.
Justifications of a legitimate interest are usually:

- legal (e.g. the assertion, exercise or defence of legal claims)
- economic (e.g. valuation of companies)

Personal data may not be processed on the basis of a legitimate interest if in an individual case; there is an indication that the interests of the employee worthy of protection outweigh the interest of processing. The existence of interests worthy of protection must be checked for each processing operation. Control measures that process employee data may only be carried out if there is a legal obligation to do so or if there is a justified reason to do so. The proportionality of control measures must also be examined whether there are justified grounds for doing so. The legitimate interest of the company in the implementation of the control measure (e.g. compliance with legal provisions and internal company rules) must be weighed against any interests worthy of protection of the employee affected by the measure and may only be implemented if they are appropriate. The legitimate interest of the company and the possible interests of the employees worthy of protection must be determined and documented before any action is taken. In addition, other requirements existing under state law (e.g. employee representation rights of co-determination and information rights of the persons concerned) may have to be considered.

7.2.6. Processing of particularly worth being protected data

Particularly worth being protected personal data may only be processed under certain requirements. Particularly worth being protected data is data about racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or the health or sexual life of the person concerned. Other categories of data can be classified as particularly worthy of protection because of state law. Equally, data relating to criminal offences may often only be processed under specific national conditions. Processing must be expressly authorized or required by national law. In addition, processing may be permitted, if it is necessary to enable the controller to comply with its rights and obligations in the field of labour law. The employee may also voluntarily give his or her consent the processing. If the processing of worth being protected data is planned, the DPO for the data protection must be informed beforehand.

7.2.7. Automated decisions

No automated processing of personal data takes place at ADMEDES GmbH during employment.

7.2.8. Telecommunications and Internet

Telephone systems, e-mail addresses, intranet and the Internet are primarily made available by the company within the scope of fulfilling operational tasks. Private use is not permitted. They are work equipment and a company resource. They may be used as part of the applicable legal regulations and the „Binding instructions for the use and application of equipment" contained in the employee manual. It is prohibited to have confidential texts translated using translation platforms (such as „Google Translator"), as such translation platforms process the entire text and could be revealed personal and confidential data. There is no general monitoring of telephone and e-mail communication or of intranet and Internet use. To defend against attacks against the IT infrastructure or individual users, regular, multi-level evaluations of protocols, virus protection, firewall and email filter system are carried out and the redundant backup system is checked for its proper functioning. For security reasons, the use of telephone systems, e-mail addresses, intranets and the Internet can be logged for a limited period. Personal evaluations of this data may only be carried out if there is a concrete and justified suspicion of a violation of the laws or policies of ADMEDES GmbH. These controls must be proportionate and may only be carried out by investigating areas. The respective national laws are to be observed as well as the existing company regulations.

8. TRANSMISSION OF PERSONAL DATA

The transmission of personal data to recipients inside and outside ADMEDES GmbH is subject to the permissibility requirements for the processing of personal data in Section 7. In the case of data transmission within ADMEDES GmbH and a subsidiary or parent company, these may only be disclosed without the consent of the data subject if there is a legal obligation or a legitimate interest in disclosure and the identity of the applicant has been ascertained beyond doubt. In case of doubt, please contact the DPO.
In the case of data transfer to a recipient outside ADMEDES GmbH, the recipient of the data must be required to use it only for the specified purposes.
If data is transferred to a recipient outside ADMEDES GmbH in a third country, the recipient must guarantee a data protection level equivalent to this data protection policy. This does not apply, if the transmission is based on a legal obligation. Such a legal obligation may arise from the law of the location of ADMEDES GmbH or from the law of the location of the data recipient. The recipient of the data is obliged to cooperate with the supervisory authority and to observe the findings of the supervisory authority regarding the transmitted data.

In the event that a data subject alleges a breach of this data protection policy by the recipient of the data, who is based in a third country, ADMEDES GmbH undertakes to support the data subject whose data has been collected by ADMEDES GmbH both in clarifying the facts of the case and in asserting his rights under this data protection policy against the recipient of the data. Furthermore, the person concerned is entitled to assert his rights also against ADMEDES GmbH. In the event of an alleged violation, ADMEDES GmbH must provide the data subject with proof that the recipient of the data in a third country is not responsible for a violation of this data protection policy in the event of further processing of the data received.
In the case of data transfer from third parties to ADMEDES GmbH, it must be ensured that the data may be used for the intended purposes.
In the event of a transfer of personal data from ADMEDES GmbH to a subsidiary or parent company domiciled in a third country, ADMEDES GmbH shall place the person whose personal data has been collected in the European Economic Area in a position of liability against this Data Protection Policy in the event of attributable violations by the subsidiary or parent company domiciled in a third country as if ADMEDES GmbH had committed the violation. The place of jurisdiction shall be the competent court at the registered office of ADMEDES GmbH

9. EXTERNAL SERVICE PROVIDERS/ORDER PROCESSING/MAINTENANCE

9.1. If external service providers are commissioned for the first time with the processing of personal data or individual processing steps (e.g. collection, deletion = disposal) or with activities (e.g. maintenance, repair) in which they have the opportunity to gain knowledge of personal data, a contract for the processing of order data must be concluded.

9.2. The same shall apply if ADMEDES-GmbH intends to perform corresponding activities on behalf of third parties.

10. ACCOUNTABILITY AND DOCUMENTATION OBLIGATIONS

Compliance with the requirements resulting from this policy must be always accountable. Verifiability must be demonstrated by conclusive and comprehensible written documentation regarding the measures taken and the associated considerations.

Pforzheim, 10th October 2019

ADMEDES GmbH

Dr. Axel Pfrommer
CEO & President