HAKRO GmbH

Data privacy policy

Stand: 01.05.18

DATA PRIVACY POLICY

Foreword

Dear Sir or Madam,

In the digital age, we, HAKRO GmbH, like every organisation and every company, depend on the collection and processing of relevant data for our business processes.

This also applies to your data if you are a customer, prospective customer, business partner or employee of our company.

The protection of your personal data has the highest priority for us. We therefore consider it our duty to ensure that the collection and processing is in accordance with the various legal requirements.

The personal rights and privacy of each individual are among the most important achievements of our society.

We have laid down strict conditions for the processing of personal data in our data privacy policy. This complies with the requirements of the General Data Protection Regulation and other laws within the Federal Republic of Germany and the European Union.

Our employees are obliged to comply with our data privacy policy and to preserve the respective data protection laws.

Carmen Kroll

Thomas Müller

HAKRO
HÄLT. SEIT 1969

Table of contents

1. Objective

HAKRO GmbH commits itself within the scope of its social responsibility to comply with data protection rights. This data privacy policy applies to HAKRO GmbH and bases on the basic principles of data protection accepted in the European Union.

The data privacy policy creates one of the necessary framework conditions for the collection, processing and, where applicable, transmission of personal data. It ensures the adequate level of data protection required by the European Data Protection Directive and local laws.

2. Scope of application

This data privacy policy applies to HAKRO GmbH and our employees. The data privacy policy covers all processing of personal data.

Anonymised data, e.g. for statistical evaluations or investigations, are not subject to this data privacy policy.

The employees are not entitled to make any regulations differing from this data privacy policy. An amendment to this data privacy policy will only be made in agreement with the data protection officer. The changes will be announced within HAKRO GmbH immediately.

3. Principles of processing of personal data

3.1 Right to informational self-determination

The basis of the data protection law is the informational self-determination of the individual.

3.2 Lawfulness

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

3.3 Transparency

The data should be collected from the data subject himself. In doing so, the data subject should be informed about the purpose of the data processing, the responsible authority and, where applicable, about any necessary transfer to third parties.

3.4 Earmarking

Personal data must only be processed in accordance with the purpose that was specified at the time of collection. Any subsequent change of purpose requires the consent of the data subject or relevant justification.

3.5 Data avoidance

In any processing of personal data, only the data necessary for the purpose of the processing must be used. Personal data must not be saved for any subsequent possible purpose.

3.6 Deletion

After the expiry of the legal or business process related retention periods, the personal data must be deleted. If, in the individual case, there are indications for the protection of legitimate interests, the data will be saved until the legitimate interest no longer exists.

3.7 Correctness of the data

The personal data must be saved correctly and completely. Appropriate measures must be taken to ensure that incomplete or outdated data are deleted or corrected.

3.8 Confidentiality

Personal data must be handled confidentially. This must be ensured by appropriate organisational and technical measures against unauthorised access, unlawful processing and disclosure, alteration or destruction.

4. Admissibility of data processing

4.1 Customer, prospective customer and partner data

4.1.1 Data processing for the fulfilment of the contractual relationship

Personal data of the prospective customer, customer or partner are allowed to be processed for establishment, executing and ending the contractual relationship. This also includes the support of the contractual partner, insofar as this is connected with the purpose of the contract. In the run-up to a contract, the processing of personal data is permitted for the preparation of offers, for the preparation of purchase requests or for the fulfilment of other wishes of the prospective customer, which are aimed at the conclusion of a contract. Prospective customers are allowed to be contacted during the preparation of a contract by using the data they have provided. Any restrictions expressed by the prospective customer must be respected.

If the data subject contacts HAKRO GmbH with a request for information, the data processing for the fulfilment of this request is permitted. If the data subject objects to the use of his data for advertising purposes, any further use of his data for these purposes is not permitted and they must be blocked or deleted for these purposes.

4.1.2 Consent to data processing

Insofar as the data subject consents to data processing, this can take place. Before giving the consent, the data subject must be informed about the nature and scope of the processing and of his/her rights.

The declaration of consent must always be obtained in writing or electronically. In case of telephone consultation, consent can also be given verbally. This must be documented.

4.1.3 Data processing due to a legal base

The processing of personal data is permitted if it is required, assumed or permitted by state legislation. The type and scope of permissible data processing is based on these legal provisions.

4.1.4 Data processing due to legitimate interest

The processing of personal data can happen if this is necessary for the realisation of a legitimate interest of HAKRO GmbH.

As a rule, legal (e.g. enforcement of open claims) or economic (e.g. avoidance of contractual disturbances) interests are entitled. The interest worthy of protection of the date subject must not prevail. This must be checked before each processing.

4.1.5 Processing of data particularly worthy of protection

The processing of personal data particularly worthy of protection must only be carried out if law requires this or if the data subject has explicitly consented.

The processing of this data is also permitted if it is mandatory to assert, exercise or defend legal claims against the data subject.

Before processing the data worthy of protection, the data protection officer must be informed.

4.1.6 User data on the internet

If personal data is collected, processed and used on websites or in programmes, the data subject must be informed in data protection notices. These notices must be easily recognisable and understandable for the data subject.

If user profiles are created to analyse the usage behaviour of websites and programmes, the data subject must be informed comprehensibly in the data protection notices.

If websites or programmes in a personal area allow access to personal data, the identification and authentication of the data subject must be designed so that adequate protection is achieved for the respective access.

4.2 Employee and applicant data

4.2.1 Data processing for the employment relationship

For the employment relationship, only the personal data, which are necessary for the establishment, execution and ending of the employment contract, must be processed. Personal data of applicants are allowed to be processed when an employment relationship is initiated. After rejection, the applicant's data must be deleted considering evidentiary time limits, unless the applicant has consented to a further storage for a subsequent selection process.

In an existing employment relationship, data processing must always be related to the purpose of the employment contract.

4.2.2 Data processing due to legal permission

The processing of personal data is permitted if it is required, assumed or permitted by state legislation. The type and scope of permissible data processing is based on these legal provisions.

4.2.3 Consent to data processing

The processing of employee data can happen due to the consent of the data subject. Declarations of consent must be given voluntarily.

The declaration of consent must always be obtained in writing or electronically. If circumstances do not allow this in exceptional cases, consent can be given orally. The issuance must be documented in any case.

4.2.4 Data processing due to legitimate interest

The processing of employee data can happen if this is necessary for the realisation of a legitimate interest of HAKRO GmbH.

As a rule, legal (e.g. enforcement of open claims) or economic (e.g. avoidance of contractual disturbances) interests are entitled. The interest worthy of protection of the date subject must not prevail. This must be checked before each processing.

Control measures which require the processing of employee data are only allowed to be carried out if there is a legal obligation or a justified reason for doing so. The interest worthy of protection of the date subject must not prevail. This must be checked before each processing.

4.2.5 Telecommunications and internet

Telephone systems, e-mail addresses, intranet and internet are primarily provided by the company within the framework of the operational scope of tasks. They are tools and company resource. They are allowed to be used within the framework of the valid legal provisions and the company's internal guidelines.

There is no general monitoring of telephone or e-mail communication or internet use. For the defence against attacks on the IT infrastructure or on individual users, protective measures can be implemented at the transitions of the company network, which block technically damaging content or analyse the patterns of attacks.

For security reasons, the use of telephone, e-mail communication or the internet usage can be recorded for a limited period of time.

Person-related evaluations of this data are only allowed to be carried out if there is a concrete, justified suspicion of a violation of laws or guidelines of HAKRO GmbH. The data protection officer must be consulted in this case.

5. Transmission of personal data

If personal data are transmitted to third parties, the admissibility of the data processing must exist. The recipient of the data must be obliged to use them only for the specified purposes.

6. Order processing

An order data processing exists if a contractor is commissioned with processing personal data without being given responsibility for the associated business process.

In such cases, a contract for data processing must be concluded. In doing so, the commissioning company retains full responsibility for the correct execution of the data processing. The contractor is only allowed to process personal data within the scope of the instructions of the customer. When the order is placed, the following instructions must be observed:

a) The contractor has to be selected according to his suitability to guarantee the necessary technical and organisational protective measures.

b) The order has to be placed in text form. In doing so, the instructions for data processing and the responsibilities of the customer and the contractor must be documented.

c) The customer must make sure that the contractor complies with his obligations before the data processing begins. A contractor can prove compliance with the requirements for data security in particular by presenting suitable certification. The control must be repeated regularly during the term of the contract, if necessary.

7. Rights of the data subject

If the following rights are asserted, they must be processed immediately and must not lead to any disadvantages for the data subject.

a) The data subject can request information about which personal data of him/her from which source and for what purpose are stored.

b) If personal data are transmitted to third parties, information about the identity of the recipient or on the categories of recipients must also be provided.

c) If personal data is incorrect or incomplete, the data subject can demand your correction or supplement.

d) The data subject can object to the processing of his personal data for the purposes of advertising or market and opinion research. For these purposes, the data must be blocked or deleted.

e) The data subject is entitled to demand the deletion of his/her data if the legal basis for processing the data is missing or does no longer exist. The same applies for the case that the purpose of the data processing does no longer exist due to the passage of time or for other reasons. Existing storage obligations and interests worthy of protection that conflict with deletion must be observed.

f) The data subject has a fundamental right to object to the processing of his/her data, which must be taken into account if his/her interest worthy of protection outweighs the interest in processing due to a special personal situation.

This does not apply if a legal provision requires the processing to be carried out.

8. Confidentiality of processing

Personal data are subject to data secrecy. Unauthorised collection, processing or usage is prohibited for employees.

Unauthorised is any processing that an employee undertakes without being entrusted with it within the framework of fulfilling his/her duties and without being authorised accordingly.

This requires the careful division and separation of roles and responsibilities as well as their implementation and maintenance within the framework of authorisation concepts.

Employees are not allowed to use personal data for their own private or economic purposes, transfer them to unauthorised persons or make them accessible to them in any other way.

This obligation continues to exist even after ending the employment relationship.

9. Security of processing

Personal data must be protected against unauthorised access, unlawful processing or disclosure and against loss, falsification or destruction at all times. This applies regardless of whether the data processing is carried out electronically or in paper form. Before new data processing methods, in particular, new IT systems, are introduced, technical and organisational measures to protect personal data must be defined and implemented. These measures must be orientated to the state of the art, the risks arising from the processing and the need to protect the data.

10. Data protection control

The compliance with the data privacy policy and the applicable data protection laws is regularly checked by appropriate controls.

11. Data protection incidents

Employees must report data protection incidents to the management or the data protection officer immediately.

In particular in cases of

- unlawful transmission of personal data to third parties

- unlawful access by third parties to personal data

- in case of loss of personal data

the notification must be made without delay so that the existing notification obligations to the supervisory authorities can be fulfilled without delay.

12. Responsibilities and sanctions

The management is responsible for proper data processing.

Therefore, the management is obliged to ensure that the legal requirements and the requirements contained in the data privacy policy are taken into account.

The implementation of these requirements is the responsibility of the responsible employees.

In case of controls by the supervisory authorities, the data protection officer must be informed immediately.

13. Data protection officer

Every data subject can contact the data protection officer with suggestions, enquiries, requests for information or complaints in connection with data protection or data security issues.

Enquiries and complaints will be treated confidentially, if requested.

You can contact your data protection officer as follows:

Guido Petermann
Hildebrandtstr. 24C
40215 Düsseldorf

Telephone: +49 211 72139550
E-mail: datenschutz@planitas.de
Website: www.planitas.de