HAKRO GmbH

Data Protection Guideline

Issued: 01.05.2018

DATA PROTECTION GUIDELINE

Foreword

Dear Sir or Madam,

In this digital age, we – the HAKRO company – like every other organisation and enterprise, depend upon the collection and processing of data relevant to our businesses processes.

This applies to your data as well, insofar as you are a customer, an interested party, a business partner or a staff member of ours.

Protection of your personal data has top priority for us. We therefore view it as our duty to ensure that the collection and processing of data is in accordance with the provisions of the various statutory regulations.

Personal rights and the right to privacy for everyone are among the most important accomplishments of our society.

In our Data Protection Guideline, we have set out stringent conditions for the processing of personal data. It corresponds to the requirements of the General Data Protection Regulation and other legislation within Germany and the European Union.

Our staff are obligated to adhere to our Data Protection Guideline and to respect the relevant data protection regulations.

Carmen Kroll

Thomas Müller

HAKRO
HÄLT. SEIT 1969

Table of Contents

1. Objective

In the context of its social responsibility, the HAKRO company commits itself to observance of data protection rights. This Data Protection Guideline applies within the HAKRO company and is based on the accepted fundamental principles of data protection in the European Union.

The Data Protection Guideline provides one of the frameworks necessary for the collection, the processing and, if required, the transmittal of personal data. It guarantees the appropriate level of data protection demanded by the European Data Protection Guideline and national legislation.

2. Applicability

This Data Protection Guideline is applicable for the HAKRO company and our staff. The Data Protection Guideline applies in respect of all processing of personal data.

Anonymised data, e.g. for statistical evaluations or studies, are not subject to this Data Protection Guideline.

Staff are not authorised to adopt measures in derogation from this Data Protection Guideline. Any change to this Data Protection Guideline shall require authorisation by the Data Protection Officer. Changes made shall be disseminated throughout the HAKRO company forthwith.

3. Principles for processing personal data

3.1. Right to informational self-determination

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

3.2. Legality

Personal data must be collected and processed in a legal manner. During processing of personal data, the right to privacy of the person concerned must be upheld.

3.3. Transparency

The data should be collected directly from the person concerned. He/she should be informed thereby as to the purpose of the processing, the person responsible and, if appropriate, any necessary transmittal to a third party.

3.4. Purpose

Personal data may only be processed for the purpose specified during its collection. An alteration to the purpose shall require the permission of the person concerned or a convincing justification.

3.5. Data avoidance

Every processing of personal data shall make use of only that data essential for the processing concerned. Personal data may not be retained for possible use later for another purpose.

3.6. Erasure

After expiry of the statutory or business process-related retention period, personal data shall be erased. Should grounds exist in individual cases to protect our legitimate interests, the data will be retained until the legitimate interests cease to exist.

3.7. Accuracy of data

Personal data stored shall be accurate and complete. Appropriate measures shall be taken to erase or correct incomplete or obsolete data.

3.8. Confidentiality

When handling personal data, it must be treated in confidence. This shall be guaranteed through the use of appropriate organisational and technical measures against unauthorised access, illegal processing and transmittal, alteration or destruction.

4. Legitimacy of processing

4.1. Customer, interested party and partner data

4.1.1. Data processing in fulfilment of the contractual relationship

The processing of personal data of an interested party, customer or partner is permissible in the course of the establishment, execution and termination of the contractual relationship. This may also include supporting the contractual partner, inasfar as this is associated with the purpose of the contract. In advance of the signing of the contract, the processing of personal data is permitted in respect of the drafting of quotations, the preparation of purchase orders or for the fulfilment of other wishes of the interested party directed towards the conclusion of the contract. Interested parties may be contacted during contract initiation making use of the data they have made available. Any restrictions the interested party may have expressed shall be respected.

If the data subject addresses the HAKRO company with a request for information, processing of the data is permissible in meeting this request. If the data subject has entered an objection to the use of his data for advertising purposes, a further use of the data for such purpose is not permissible and it must be either blocked against such use or erased.

4.1.2. Consent to data processing

If the data subject has consented to data processing, such processing is permissible. Prior to giving consent, the data subject must be informed of the nature and extent of processing as well as his rights. As a matter of principle, consent shall be made in writing or electronically. In the case of consultation by telephone, the consent can be

granted verbally. This must be documented.

4.1.3. Data processing on the grounds of statutory obligations

The processing of personal data is permissible, if required, assumed or permitted under applicable national law. The nature and extent of the processing permissible derives from such law.

4.1.4. Data processing on the grounds of legitimate interest

Personal data can be processed, if this is necessary to give effect to a legitimate interest of the HAKRO company. As a rule, legitimate interests include for legal (e.g. collection of outstanding receivables) and economic (e.g. prevention of breaches of contract) reasons. The data subject's right to data privacy is not paramount in such cases. This shall be established prior to any processing.

4.1.5. Processing of particularly sensitive data

The processing of particularly sensitive personal data is permissible only when required by law or when the data subject has expressly consented. The processing of these data is also permissible when it is mandatory in order to assert, enforce or to defend legal claims against the data subject. Prior to the processing of the sensitive data, the Data Protection Officer shall be informed.

4.1.6. User data on the Internet

If personal data collected on websites or in programs is processed or otherwise used, the data subjects shall be informed accordingly by way of a data protection notice. The notification must be readily recognisable and understood by the recipient. If usage profiles are generated for analysis of user behaviour on websites and in programs, the users shall be informed by way of an easily understood data protection notice.

If access to personal data is enabled for websites or programs in a private environment, the identification and authentication of the data subject shall be so designed that protection appropriate to the individual access is afforded.

4.2. Employee and job applicant data

4.2.1. Data processing for employment-related purposes

Only those personal data necessary for the establishment, execution and termination of the employment contract shall be processed for employment-related purposes. During the establishment of an employment relationship, the processing of the personal data of an applicant is permissible. After rejection, the applicant's data shall be erased, having due regard to statutory requirements for retention of evidence, unless the applicant has consented to continued storage for a later selection process. In existing employment relationships, the data processing shall always correlate with the purpose of the employment contract.

4.2.2. Data processing on the grounds of statutory obligations

The processing of personal data is permissible if requested, required, or permitted under applicable national law. The nature and extent of the processing permissible derives from such law.

4.2.3. Consent to data processing

If the data subject has consented, the processing of employee data is permissible. Declarations of consent must be given of free will. As a matter of principle, consent shall be made in writing or electronically. If circumstances do not permit this, then – exceptionally – consent may be granted verbally. In any event, consent must be documented.

4.2.4. Data processing on the grounds of legitimate interest

The personal data of employees can be processed, if this is necessary to give effect to a legitimate interest of the HAKRO company. As a rule, legitimate interests include for legal (e.g. collection of outstanding receivables) and economic (e.g. prevention of breaches of contract) reasons. The data subject's right to data privacy is not paramount in such cases. This shall be established prior to each and every processing. Control measures requiring the processing of employee data are only permissible when a statutory obligation to do so exists or there are reasonable grounds for doing so. The data subject's right to data privacy is not paramount in such cases. This shall be established prior to each and every processing.

4.2.5. Telecommunications and Internet

The telephone system, email addresses, the Intranet and the Internet are made available by the company primarily in the context of business operations. They are working tools and company resources. They may be used within the scope of applicable legal provisions and company-internal guidelines. General monitoring of telephone or email communications and use of the Internet shall not occur. Defence against attacks on the IT infrastructure or on individual users may require the implementation of protective mechanisms at the interfaces to the company's network to block technically damaging content or to enable the analysis of patterns of attack. For security reasons, the use of telephone and email communications and the Internet may be protocolled for limited periods. Evaluation of this data with respect to a particular individual is permissible only in the case of specific, justifiable suspicion of a violation of statutory requirements or the guidelines of the HAKRO company. In such case, the Data Protection Officer shall be consulted.

5. Transfer of personal data

In the case of transfer of personal data to a third party, the permissibility of the data processing must have been established. The recipient of the data shall commit himself to using the data only for the purposes established beforehand.

6. Commissioned data processing

Commissioned data processing is when a service provider is charged with the processing of personal data but does not bear responsibility for the associated business process. In such cases a contract for commissioned data processing shall be concluded. In this, the commissioning entity retains full responsibility for the correct execution of the data processing. The service provider must process the personal data strictly within the scope of the directives issued by the commissioning entity. When issuing the mandate, the following stipulations shall be observed:

a) The service provider shall be selected on the basis of his ability to guarantee the necessary technical and organisational measures for data protection.

b) The processing shall be commissioned in written form. The instructions regarding data processing and the responsibilities of principal and contractor shall be documented.

c) Prior to commencement of processing, the principal shall satisfy himself that the contractor is fulfilling all his obligations. In particular, the contractor can demonstrate adherence to the requirements for data security by presenting appropriate certification. As necessary, the check shall be repeated at regular intervals during the term of the contract.

7. Rights of the data subject

If a data subject asserts any of the rights listed below, the issue shall be addressed without delay and may not result in any disadvantage to the data subject.

a) The data subject has the right to obtain confirmation of what personal data of his from what source is stored and for what purpose.

b) If personal data is transferred to third parties, the identity of the recipient or the categories of recipients must be declared.

c) If personal data is inaccurate or incomplete, the data subject is entitled to demand its rectification or completion.

d) The data subject is entitled to object to the processing of his personal data for purposes of advertising or market research or polling. The data shall either be blocked for such processing or erased.

e) The data subject is entitled to demand the erasure of his personal data, if the legal basis for processing does not exist (any more). The same shall apply in cases where the purpose of processing no longer exists, either through the passage of time or for other reasons. Existing statutory periods of retention and legitimate interests requiring continued retention shall be respected.

f) The data subject has a fundamental right of objection to the processing of his data. This shall be taken into consideration when, in a particular personal situation, his interest in the protection of

his data outweighs the interest in the processing of the data.

This shall not apply where the data processing is occasioned by statutory requirements.

8. Confidentiality during processing

Personal data is confidential. Unauthorised collection, processing or usage of such data by members of staff is prohibited. Any type of processing undertaken by an employee is unauthorised unless performed within the scope of tasks with which he has been entrusted so that he is then duly authorised.

This necessitates the careful allocation and separation of roles and responsibilities together with their implementation and maintenance in the context of authorisation concepts.

Employees are forbidden to make use of personal data for their own private or economic purposes or to transfer it or otherwise make it available to unauthorised persons. This commitment also remains in effect after the employment contract has ended.

9. Security of processing

Personal data shall at all times be secured against unauthorised access, illegal processing or transferral as well as loss, falsification or destruction. This applies irrespective of whether the processing is electronic or on paper. Prior to the introduction of new data processing procedures and, in particular, new IT systems, technical and organisational measures for the protection of personal data shall be established and implemented. These measures shall be oriented to the state of the art, the risks arising from the processing and the sensitivity of the data.

10. Monitoring of data protection

Adherence to this Data Protection Guideline and to applicable data protection law shall be monitored regularly through appropriate checks.

11. Breaches of data confidentiality

Employees shall report breaches of data confidentiality to company management or the Data Protection Oficer without delay. Particularly in cases of:
- unauthorised transferral of personal data to third parties,
- unauthorised access to personal data by third parties and
- loss of personal data

the notification shall be made immediately so that the mandatory reporting to supervisory authorities can be made in the timely manner prescribed.

12. Responsibilities

Company management is responsible for proper data processing. In this, it is required to ensure that statutory requirements and the specifications contained in this Data Protection Guideline are adhered to.

The implementation of these requirements is incumbent upon the responsible employee.

Inspections by the supervisory authorities shall be reported to the Data Protection Officer immediately.

13. The Data Protection Officer

Every data subject is entitled to approach the Data Protection Officer with suggestions, queries, requests for information or complaints in connection with questions of data protection or data security. Queries and complaints shall be treated in confidence, if requested.

You can reach your Data Protection Officer at:

Guido Petermann
Oberbilker Allee 203
40215 Düsseldorf

Telephone: +49 211 72139550
Email: datenschutz@planitas.de
Website: www.planitas.de