Group Privacy Policy

Table of Contents

Content

1. Introduction

Information is a valuable resource and the basis for conducting our global business activities that enable us to achieve our business goals. Information technologies offer different possibilities of availability and use of information by means of different communication systems and channels. These possibilities require HTI AG and its subsidiaries to process information legally, including personal data, in order to minimize risks for the companies of the HTI AG Group and the persons concerned.

2. Purpose

HTI AG's Group Privacy Policy sets standards regarding data protection and data security for the processing of personal data by HTI AG and its subsidiaries in order to ensure adequate protection of the fundamental rights and freedoms of the persons concerned.

With this Group Privacy Policy, HTI AG assumes its corporate responsibility to process the personal data of its employees, customers, suppliers, business partners and other persons concerned with the necessary care and to ensure sufficient data protection within the scope of all relevant business activities and business processes.

Compliance with this Group Privacy Policy is an essential prerequisite for the creation of a standard for the legal exchange of personal data between HTI AG and its subsidiaries. Compliance with this Directive contributes to an adequate level of data protection in the cross-border exchange of personal data, in accordance with the relevant data protection laws.

3. Scope of application

This guideline applies to all subsidiaries and locations under the responsibility of the HTI AG Group.

As a European company with worldwide operations and subsidiaries, HTI AG processes data about our employees, customers, suppliers and others in accordance with EU laws, the laws of the United States and the relevant regulations of other countries.

Relevant national and international legal obligations take precedence over this directive. If the personal data of persons domiciled outside the EU are processed by a subsidiary or by a location of a subsidiary of HTI AG, the relevant applicable national or international law of the place where the data subject is resident shall take precedence over this Directive. This may include, inter alia,

prior consultation with the competent supervisory authorities where the processing of data would pose a high risk to the fundamental rights and freedoms of data subjects.

In case there are no relevant legal provisions or these are less strict, this group data protection guideline shall be applied as a common obligatory data protection standard of the HTI AG group. This Directive should not be interpreted as conferring more rights on individuals than provided for by applicable law or other legally binding agreements.

4. Definitions

"**Applicable law**" means the legal provisions of the territory, including any regulations, regulatory requirements or guidelines to which the data controller is subject.

"**Anonymization**" is a change of data that can no longer be attributed to a person and can only be restored with disproportionate use of time, costs and effort.

"**data subject's consent**" means any voluntary statement of intent, made in an informative and unequivocal manner for the particular case, in the form of a statement or other clear affirmative act by which the data subject indicates his or her consent to the processing of personal data concerning him or her. Consent must be documented in an appropriate manner to serve as evidence.

"**Responsible**" means any natural or legal person within the HTI AG Group who decides on the purpose and means of processing personal data based on the business activities of HTI AG and its subsidiaries.

"**Data Protection Impact Assessment (DSFA)**" is a process that is documented by or on behalf of the controller and, where specified and necessary by applicable law, involving the GDPC. A DSFA is carried out prior to the actual processing of data in those cases where it is likely that the processing will entail a high risk to the rights and freedoms of natural persons, since the processing of personal data involves the use of new technologies, taking into account the nature, scope, context and purpose of the processing. Within the scope of a DSFA, the effects of planned processing procedures for the protection of personal data are assessed.

"**Data subjects**" are all natural or (depending on the applicable law) legal persons whose data are processed.

"**Corporate Privacy Coordinator (GDPC)**" is a person formally appointed by the Executive Committee to inform, advise and monitor HTI AG on applicable data protection laws and guidelines.

"**Local Data Protection Coordinators (LDPC)**" are appointed individually by the management of the respective subsidiaries in consultation with the GDPC for each HTI AG Group company.

"**Personal Information**" means any information relating to an identified or identifiable natural person or (subject to applicable law) legal person ("Data Subject"). Identifiable is a natural person who can be identified directly or indirectly by association with an identifier such as name,

identification number, location data, online identifier or one or more special characteristics that express the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.

"**processor**" means a natural or legal person, authority, institution or other body processing personal data on behalf of the data controller.

"**processing**" means any operation carried out with or without the aid of automated procedures or any such series of operations relating to personal data, such as the collection, collection, organization, sorting, storage, adaptation or alteration, reading, consultation, use, disclosure by transmission, dissemination or any other form of provision, comparison or linking, restriction, erasure or destruction. In the context of this Directive, this definition also applies to the terms "processed" and "processed".

"**Pseudonymisation**" means the processing of personal data in such a way (e.g. by exchanging names or numbers) that the personal data can no longer be assigned to a specifically affected person without the use of additional information (e.g. a reference list of names and numbers), provided that this additional information is kept separately and is subject to technical and organisational measures which ensure that the personal data is not assigned to an identified or identifiable natural person.

"**Special categories of personal data**" are data relating to ethnic origin, political views, religious or philosophical beliefs or trade union membership and include genetic information, biometric data for the sole purpose of identifying a natural person, health, sexual behavior or sexual orientation data.

"**third party**" means any natural or legal person, public authority, institution or other body other than the controller, the data subject or a processor. This means that every company of the HTI AG Group, as well as every external business partner are considered as third parties, unless they process personal data on behalf of a company of the HTI AG Group (e.g. in the provision of IT or HR services).

"**Transmission**" means any transmission, transfer or distribution of personal data and any form of transmission to third parties by the controller.

5. Responsibilities relating to this policy

5.1 The GDPC is responsible for creating, revising, monitoring and implementing the Group Privacy Policy.

5.2 Management is responsible for approving the Group Privacy Policy.

6. Principles for the processing of personal data

The processing of personal data requires compliance with international and national data protection laws and regulations as well as internal guidelines and specifications.

The principles set out the obligations to be respected by the controller and all other parties concerned to ensure the lawful and fair processing of personal data and provide guidance for the correct processing of personal data.

6.1 Legality, good faith processing and transparency

Personal data will be processed in a lawful manner, in good faith and in a manner that is comprehensible to the data subject.

6.2 Intended use

Within the HTI AG Group, personal data is collected exclusively for legitimate, clear and defined purposes and is not further processed for purposes that run counter to the purpose of destination, unless there is a corresponding legal basis.

6.3 Data minimization

The processing of personal data must be appropriate, significant and limited to what is necessary for the purpose of the processing.

6.4 Correctness

The processing of personal data must be factually correct and, if necessary, up-to-date. Since the processing of incorrect personal data involves risks which may have different consequences for the data subject and/or for the companies of HTI AG, appropriate and appropriate measures must be taken by the controller in order to ensure that personal data which are incorrect with regard to the purposes of their processing are immediately deleted or corrected.

6.5 Limitation of data storage

Personal data must be stored in a form that allows the identification of the data subject only for as long as is necessary for the purposes for which they are processed.

6.6 Security: Confidentiality, Integrity, Availability

The protection of personal data requires that the controller ensures an adequate level of security to protect the personal data, including protection against unauthorized or unlawful processing and protection against accidental loss, accidental destruction or damage by appropriate technical and organizational measures.

The choice of appropriate technical and organizational security measures shall be made taking into account the seriousness and likelihood of existing risks to the rights and freedoms of the natural person, taking into account the state of the art, the costs of implementation, the nature, the scope, the context and the purpose of processing.

These measures may include the following:

the anonymisation, pseudonymisation and/or encryption of personal data;

the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services in the long term;

the ability to rapidly restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

a process for regularly checking, evaluating and evaluating the effectiveness of technical and organizational measures to ensure the security of data processing.

In addition to these requirements, any processing of personal data within or for the purposes of the HTI AG Group is subject to additional restrictions and rules described in the relevant IT processes.

6.7 Responsibility

The controller is responsible for compliance with the principles set out in Articles 6.1 to 6.5 and for demonstrating compliance. For this reason, he must always be able to prove compliance with the principles for the processing of personal data by means of appropriate documents.

7. Exceptional measures to safeguard the confidentiality of business data within the HTI AG Group

The employees of HTI AG and its subsidiaries are prohibited from using business data and personal data contained therein for their own private purposes or from making such data accessible to unauthorized persons or companies.

For purposes of this policy, the term "unauthorized" refers to the use of personal data by employees who do not require access to such data in the course of their employment. d Description and definition of duties and responsibilities by the person responsible for the processing of personal data ensures that employees have access to personal data only when it is necessary and appropriate to perform their tasks.

Only authorized employees who have committed themselves to data secrecy may process personal data for the intended purpose and within the existing, data protection-relevant IT systems. In accordance with applicable local law, this includes a separate agreement on data secrecy or an obligation to secrecy in the employment contract, which stipulates that such an obligation exists beyond the end of the employment relationship.

8. The processing of special categories of personal data

Unless it is absolutely necessary to fulfil certain rights and obligations and/or the controller has a legal justification under applicable law, special categories of personal data will only be processed with the express consent of the data subject.

9. Legality of processing

9.1 General conditions for the processing of personal data

The processing of personal data is only legal if at least one of the following conditions is fulfilled:

- the data subject has given his/her consent to the processing of his/her personal data for one or more purposes as determined by m controllers;
- the processing of data is necessary in connection with the conclusion of a contract between the data subject and the controller;
- where the data subject has already concluded a contract with the controller, processing is lawful where processing is necessary for the performance of the contract;
- the processing is necessary to fulfil a legal obligation to which the controller is subject;
- processing is necessary for the protection of the vital interests of the data subject or another natural person;
- processing is necessary to safeguard the legitimate interests of the data controller or a third party, unless the interests or fundamental rights and freedoms of the data subject which require the protection of personal data prevail
- any other lawful reason provided for by applicable law.

9.2 Special provisions for video surveillance systems

The processing of personal data by video surveillance systems is subject to the following restrictions:

The use of video surveillance systems in publicly accessible locations and within the work area is only permitted if:

- such use is justified for legitimate reasons and by the overriding interest of the controller, i.e. for the safety of employees or visitors, the protection of property, access control, etc..;
- the use is limited to what is necessary to achieve the purpose (e.g. with regard to the number of cameras, screen recording etc.),;
- the conditions of the applicable law are fulfilled.

If required by applicable law, authorization must be obtained from the competent authorities (data protection authority, labor inspectorate, etc.).

If the above conditions are met and a video surveillance system is to be installed, a separate policy must be established for each video surveillance system, which must include at least the following points: technology used, surveillance area, access rights to the cameras and recordings, deadlines for the storage and deletion of personal data, procedures for the protection and transfer of recordings to third parties, in particular to authorities.

10. Order data processing

If the controller instructs a data processor to carry out the processing of personal data on his behalf, the controller shall be responsible for compliance with the applicable law and regulations governing the processing of personal data.

For this reason, the controller shall appoint only such data processors as are sufficiently guaranteed to take appropriate technical and organizational measures to ensure the protection of the data subject's rights.

The order data processor shall be commissioned exclusively on the basis of a written contract which defines the subject matter of the contract, the duration, type and purpose of the processing and the categories of personal data to be processed, the categories of data subjects, the rights and obligations of the controller and the order data processor, as well as the technical and organizational measures (see Article 6.6) which must be implemented by the order data processor.

In the event that the data processor is required to appoint another data processor, this shall be done only with the prior express written consent of the controller.

The LDPCs must be contacted as early as possible in order to ensure the placement of the order data and the drafting of a contract between the controller and the order data processor.

11. Transmission of personal data to third parties

A controller shall not disclose personal data to third parties unless appropriate measures have been taken to ensure that such a transfer is carried out on an adequate legal basis and that all personal data are adequately protected during the transfer.

As soon as the controller transfers personal data to a third party to process data on behalf of the controller, Section 10 shall apply.

In certain circumstances, personal data must be disclosed on the basis of applicable law, in particular to public authorities. In the event of a request for such disclosure, the controller will ensure that the GDPC is promptly informed and, to the extent permitted by law, will do its utmost to refuse or limit disclosure and in particular to ensure that only personal data relevant and necessary to the request is disclosed.

In the case of the transmission of personal data abroad, the legislation in many countries provides for special requirements. This applies in particular, but not only, to the transfer of personal data from the countries of the European Economic Area (EEA) to countries outside the EEA. LDPCs must be contacted as early as possible to ensure compliance with applicable law.

12. Rights of the persons concerned

Every data subject has inalienable and extensive rights against the controller, depending on the applicable law. These rights can neither be excluded nor limited by a contract or legal transaction.

12.1 Information on personal data

The principle of transparency stipulates that the processing of personal data must be as transparent as possible for the data subject. The controller shall provide the data subject with transparent information to the extent required by the applicable law.

For further information please contact the GDPC/LDPC.

12.2 Right of the data subject to information

Each data subject is entitled to request information regarding his/her personal data which is processed by HTI AG and its subsidiaries. This information must contain at least the content required by the applicable law.

The person concerned may submit a request for information to the responsible department of the respective company of the HTI AG Group. It is obliged to provide the necessary support.

12.3 Right to correction

If the personal data processed is inaccurate or incomplete, the data subject may request the rectification of inaccurate personal data concerning him/her. Taking into account the purpose of the processing, the data subject may also request the completion of incomplete personal data.

12.4 Right to cancellation ("Right to oblivion")

The data subject may request the deletion of personal data concerning him/her and the controller is then obliged to delete the data subject's personal data if he/she is no longer authorised to process them or if this is required by the applicable law.

Reasons for deletion can be:

- the personal data are no longer required for the purposes for which they were collected or otherwise processed;
- the data subject withdraws his/her consent on the basis of which the processing was carried out and there are no other grounds for lawful processing;
- the data subject has lodged an objection to the processing referred to in Article 12.7 and there are no overriding grounds for lawful processing;
- the personal data have been processed illegally;
- the personal data must be deleted by legal means.

12.5 Right to limitation of processing

The data subject may request that processing be restricted. In this case, the controller is obliged to restrict the processing of the data subject's personal data in accordance with the relevant laws.

12.6 Right to Data Transferability

Upon request, the controller must be able to provide the data subject with personal data in a structured, commonly used and machine-readable format. In addition, where such a right exists under the applicable law, the data subject must be able to transfer such data without hindrance by the controller to another controller.

In exercising their data transfer rights, the data subject shall have the right, where technically possible, to have the personal data transferred directly from one controller to another.

12.7 Right of objection

In the event that the processing is carried out on the basis of a legitimate interest of the controller or of a third party or for the performance of a public task, the data subject may, depending on the relevant law, object to the processing of personal data relating to him/her on the basis of his/her particular situation.

12.8 Right to compensation

Depending on the applicable law, any data subject may claim damages for any damage caused by the processing of incorrect, incomplete, outdated, incorrect, unlawfully obtained personal data or by unauthorized processing of personal data.

12.9 Questions, complaints and remedies

Questions and requests, complaints and remedies, including claims for data protection damages, will be dealt with and processed exclusively as described in Section 14 and with the cooperation of the GDPC/LDPC.

13. Integrated data protection management

13.1 GDPC (Global Data Protection Coordinator)

HTI AG names a GDPC and a representative.

The GDPC is responsible for monitoring compliance with the applicable laws for the protection of individuals with HTI AG Group-wide processing of personal data within the framework of this guideline. As part of this responsibility, the GDPC creates and implements the necessary corporate documents and processes and monitors compliance with them.

The GDPC will be determined on the basis of professional qualifications and in particular expertise in the field of data protection rights and data protection practices and its suitability to perform the tasks listed below. The GDPC is bound to secrecy and discretion in the performance of its duties. The GDPC should be easily accessible from every Group company.

The GDPC has the following tasks:

- inform and advise those responsible for the processing of personal data and employees about the obligations arising from the applicable data protection laws and from this directive;
- Monitoring compliance with the principles set out in the Data Protection Act within the framework of this directive, including the assignment of responsibilities; coordination of awareness raising and training of employees involved in the processing processes and the initiation of appropriate audits;
- Initiation and support of data protection impact assessments upon request and when required;
- Support of LDPCs in their cooperation with supervisory authorities upon request of the LDPC;

Coordination and support of LDPCs in questions concerning the processing of personal data in the HTI AG Group including the submission of comments, participation in consultations, consultation and the implementation of other activities in connection with data protection.

The GDPC is assisted by a deputy.

13.2 LDPC (Local Data Protection Coordinator)

Each group company of the HTI AG Group which processes personal data appoints an LDPC.

The LDCP is responsible for monitoring compliance with applicable laws on the protection of individuals with regard to the processing of personal data in the respective Group company within the framework of this Directive and in consultation with the GDPC. As part of this responsibility, LCPC creates and implements the necessary corporate documents and processes and monitors compliance with them in the respective Group company.

The LDPCs support the GDPC in fulfilling its tasks. They support him by collecting the necessary information and making this information available to the GDPC. In addition, they communicate Group requirements and Group data protection standards to the respective Group companies.

In coordination with the GDPC, the tasks of the LDPC include in particular:

- to inform and advise those responsible for the processing of personal data of the respective group company and the respective employees about the obligations arising from the applicable data protection laws and from this directive;
- Monitoring compliance with the principles set out in the Data Protection Act within the framework of this policy, including the assignment of responsibilities; coordination of awareness raising and training of employees involved in the processing processes and the initiation of appropriate audits;
- the initiation and support of data protection impact assessments upon request and if necessary in the respective Group company in coordination with the GDPC;
- participation in consultations and cooperation with supervisors in consultation with the GDPC
- advising and carrying out other activities related to data protection in the respective Group company.

If necessary, the respective company will appoint a deputy to support the LDPC in fulfilling its tasks.

He may appoint a deputy to assist him in the performance of his duties.

If required, the GDPC can describe and/or supplement the tasks of the LDPCs in a separate guideline.

13.3 Cooperation

Data protection management requires joint efforts and close cooperation between the GDPC, the LDPC and all other parties involved to set the standard for an adequate level of data protection and to comply with applicable international and national data protection laws and regulations in the processing of personal data.

The companies of the HTI AG Group and their employees support the GDPC and the LDPCs in fulfilling their legal tasks. Questions to the GDPC or LDPCs are answered truthfully and without unnecessary delay. The GDPC and the LDPCs are informed by the departments and/or management in the following cases:

- Development and introduction of new systems/processes that are important for data protection;
- significant changes to existing systems/processes that are important for data protection;
- Purchase of new external service providers who have potential access to personal data;
- significant changes to contracts with external service providers who have potential access to personal data;
- any request from a customer, employee, works council, cooperation partner or other relevant person for data protection;
- Consulting requests from the operative business or projects about data protection standards.

If there are indications of a violation of the data protection laws or this guideline, the GDPC, the management and the LDPC of the affected HTI AG Group company will be informed. The GDPC classifies the incident and coordinates the approach. The GDPC ensures that the supervisory authorities and data subjects are notified when required by law.

14. Inquiries, complaints and remedies

Data subjects may contact the LDPC and/or the GDPC at any time with questions and complaints regarding the processing of their personal data. In any case, the LDPCs will inform the GDPC of requests from affected persons. All inquiries and complaints received will be treated as strictly confidential.

Questions and/or complaints of a data subject who allegedly violates this policy or the applicable data protection law by a group company of the HTI AG Group, which has its registered office in a country other than the location of the data subject, may be addressed to the LDPC of the country of residence, the LDPC of the allegedly infringing company or the GDPC, at the discretion of the data subject.