

## **Company directive for the protection of personal data for affiliates in "third countries"**

In the sense of this directive, the notion of third countries shall refer to all states, which are not those states, providing an appropriate data protection level in the sense of Article 25 of the EU-directive N° 95/46/EC from October 24, 1995 (Official Journal N° L281/31). States, providing an appropriate data protection level are the member states of the European Union (EU), the other contractual states of the Agreement on the European Economic Area (EEA) and those states approved through the EU-Commission.

### **Content**

1. Target and Scope
  - 1.1 Commitment
  - 1.2 Relation to legal provisions
2. Definitions
3. Principles for processing personal data
  - 3.1 Data processing Reliability
  - 3.2 Purpose
  - 3.3 Transparency
  - 3.4 Data quality
  - 3.5 Data transfer within a third country or to another third country
  - 3.6 Special types of personal data
  - 3.7 Direct marketing/Market or opinion research
  - 3.8 Automatized individual decisions
  - 3.9 Data safety
  - 3.10 Confidentiality of data processing
  - 3.11 Data processing by order
4. Rights of the parties involved
5. Process-related questions
  - 5.1 Implementation within the company
  - 5.2 Questions and concerns
6. Publicity
7. Adherence control



## 1. Target and Scope

The target of the company directive is to globally secure the transfer of personal data, necessary for the daily business within the group. To do so, it is necessary also for affiliates, having their seat in third countries, to guarantee uniform data protection and data security standards in the sense of the EU-directive on data protection for the processing of personal data and to ensure, that there are also an appropriate data protection level and sufficient guarantees in the sense of the EU-directive on the protection of the personal rights and the exercise of the related rights.

The directive shall apply as frame directive to the processing of personal data from employees, customers, suppliers, other business partners, persons interested and other parties involved through affiliates in third countries and this irrespective of the origin of those data.

### 1.1 Commitment

The provisions of this directive are binding for all affiliates, which are based in third countries. All employees of the affiliates concerned must know this directive and comply with it. Other companies, in which the is AG is directly or indirectly participating, can commit themselves to adhere to the provisions of this directive on a voluntary basis.

If an affiliate has not yet committed to comply with this directive, the legitimacy of the data transfer to this affiliate shall be controlled in each individual case and secured by appropriate special measures.

### 1.2 Relation to legal provisions

Existing legal provisions are not affected by this directive. Each affiliate shall control (e.g. through its data protection officer or through its legal department), whether there are similar relevant legal provisions in place (e.g. data protection laws) and shall ensure that they are complied with. In the event that such legal provisions contradict the obligations from this directive in third countries, the affiliate concerned shall notify this immediately to the is AG and also to the affiliates in the EU/EEA-states, which have transmitted data to them, even if these legal obligations come into effect later. In such case, the is AG together with the affiliate concerned will try to elaborate a practicable solution in the sense of the EU-directive on data protection and according to section 1.1, par. 2 record it to the register.

The responsibility for the general implementation of this directive is assumed by the management of the individual affiliates in the third country; the execution in individual cases respectively by the instance within the same affiliate, which processes personal data in the context of its specific tasks.

## 2. Definitions

In this directive the following expressions shall have meanings, defined hereinafter:

- Contractor the natural or legal person, processing personal data by order of a responsible entity;
- Party involved any specific or specifiable natural person, whose data are being processed. A person is then specifiable if he/she/it can be directly or indirectly identified, e.g. through assignment of an index number;
- Third person any natural or legal person, that can not be assigned to a competent entity;
- Third country any state in the sense of the footnote on page 1;
- Consent a volition, expressed without force and in knowledge of the facts, by which the party involved accepts that its personal data are processed;
- Affiliate the is AG and each company, in which the is AG directly or indirectly has the majority of voting rights (affiliated companies); these companies are respectively identified in the updated list of the affiliates;



- Customers and suppliers natural or legal persons, with who there is or will be a business relationship;
- Personal data any information on a party involved;
- Transfer of personal data or data transfer the transmission of personal data, their distribution or any form of disclosure to third parties;
- Competent entity in relation to third parties the legally autonomous is-affiliate, where the management initiates the data processing. Dependent branches, representations and operating units are part of the competent entity;
- Processing of personal data or data processing any process, executed with or without automated processes or each sequence of processes in connection with personal data - such as the collection, saving, storing, adjustment, changing, readout, request, use, transfer through transmission as well as blocking, deleting or destroying of data.

### 3. Principles for processing personal data

For the processing of personal data through the affiliates in a third country the following principles apply, which the affiliates must comply to.

#### 3.1 Data processing Reliability

The processing of the personal data, defined in section 1, par. 2 shall only be admitted, if at least one of the following conditions is fulfilled:

- The party involved has issued an effective consent.
- The processing serves the purpose definition of a contractual relationship or of a quasi-contractual relationship with the party involved.
- The processing is necessary for the protection of justified interests of the competent entity and there is no reason to assume that the legitimate interests in an exclusion of the processing of the party involved prevail.
- The processing is required or permitted by national legal provisions. This directive must be complied with in either case.

#### 3.2 Purpose

Personal data shall only be collected and processed for defined, explicit and legal purposes. Affiliates in third countries, which committed to adhere to this directive, shall be obliged to comply with the purpose of the data transferred to it by an affiliate of an EU/ EEA-state (see footnote on page 1) in saving, processing and using those data; changes of the purpose require the consent of the party involved or are admitted when the respective national law of the data exporter from the EU/ EEA-state allows them.

#### 3.3 Transparency

Parties involved, whose personal data are transmitted by an affiliate from an EU/ EEA-state (see footnote on page 1), shall receive the following information from the receiving affiliate in a third country (if necessary, upon agreement with the data exporter):

- Identity of the competent entity in the third country and of the data exporter in the EU/EEA-state
- Purpose of the transmission
- Other information provided that this is necessary for reasons of equity, e.g.
  - Information, correction and deletion rights



- Right of objection to advertisements.

This information is not required, if

- this is necessary for the protection of the party involved or for the protection of the rights and obligations of other persons or
- if the party involved has already been informed or
- if this is connected to an disproportionate expenditure or
- if the data are publicly accessible and if a notification would be disproportionate because of the multitude of the relevant cases.

### 3.4 Data quality

Personal data shall be factually correct and - if necessary - updated. Those steps must be taken, which are necessary to correct or delete incorrect or incomplete data. The data processing must be aligned with the purpose that only required personal data, i.e. as few personal data as possible, are collected, processed or used. This means, that in particular the possibilities of anonymization and pseudonymization shall be used, inasmuch as the expenditure is in an appropriate relation to the intended purpose. Statistical evaluations or examinations, which are done on the basis of anonymized or pseudonymized data are not relevant for data protection inasmuch as the data do not provide any conclusion on the party involved. Personal data, which were saved for those business purposes for which they had originally been collected and saved and which are no longer necessary, shall be deleted by complying with those saving obligations provided by law.

### 3.5 Data transfer within the third country or to another third country

The transfer of the personal data, received by one company from an EU/ EEA-state (see footnote on page 1) to another entity within the third country or to a different third country shall only be admitted, if at least one of the following conditions is fulfilled:

- The party involved has issued an effective consent.
- The transfer serves the purpose definition of a contractual relationship or of a quasi-contractual relationship with the party involved.
- The receiving entity exhibits an appropriate data protection level in the sense of this directive; if this is an affiliate, which has committed to adhere to this directive, the presence of an appropriate data protection level must not be controlled.

### 3.6 Special types of personal data

The processing of special types of personal data, e.g. information on racial or ethnic origins, political opinions, religious or philosophical convictions, memberships in trade unions, health or sexual life, is categorically forbidden. If this should become necessary, the party involved must expressly agree, unless,

- the party involved is not in the capacity to agree (e.g. medical emergency) or
- the party involved has already published these data or
- the processing is necessary to assert, exercise or defense legal claims, and if there is no reason to believe that legal interests of the party involved in the processing prevail or
- the processing is forbidden by national law (e.g. collection/protection of minorities). This applies analogously if the personal data are collected in a third country.



### 3.7 Direct marketing/Market or opinion research

The processing of personal data for direct marketing / market or opinion research purposes is generally admitted, provided that this can be reconciled with the originally defined purpose of the data processing and that no more severe provisions result from the national law (e.g. requires a consent). The party involved, however, has the right to object to a use of his/her data at any time. In this case, the data shall be blocked for this purpose.

### 3.8 Automated individual decisions

If personal data are processed with the target to take individual decisions, the justified interests of the party involved shall be guaranteed through appropriate measures. Decisions, which will have negative consequences for the parties involved or which will considerably affect the latter shall not exclusively be based on an automated individual decision, which serves the purpose of an evaluation of individual personal characteristics (e.g. credit worthiness), i.e. shall not exclusively be taken on the basis of the use of the information technology. Automated processes shall in general only be used as support for such decisions. The only exception to this is when the interests of the party involved are guaranteed through information on the logics of the decisions and if there is the possibility to issue a statement. In the event of a statement of the party involved, sole the competent entity shall be obliged to control the relevant decision.

### 3.9 Data safety

The competent entities shall take the appropriate technical and organizational measures, required to guarantee the necessary data security, which protects the personal data from unintended or unlawful deletion, modification or loss and from unjustified transmission or access. Those measures refer in particular to computers (server and desktop PCs), networks, communication lines and/or applications and result from the implementation of the binding applicable set of rules on information safety, which applies also to affiliates in third countries and which does not only cover the processing of data on natural persons, but also the complete information processing.

### 3.10 Confidentiality of data processing

Only those employees, who are authorized and informed on the adherence to the data protection, are allowed to collect, process or use personal data. It is forbidden to use personal data for private interests, to transfer them to unauthorized third persons or to otherwise disclose them. Unauthorized in this sense are also employees, inasmuch as they do not need these data for the execution of their individual tasks.

### 3.11 Data processing by order

If an affiliate in a third country demands from a third party to process personal data, the following applies additionally:

- It shall select such a contractor, who guarantees the technical and organizational security measures for the data protection compliant processing.
- The execution of the data processing by order shall be fixed in a written or otherwise documented agreement, in which the rights and obligations of the contractor are defined.
- The contractor must be contractually obligated to process the data he receives from the contracting entity only in the context of the order and by adhering to the instructions of the latter. Processing for own purposes or for the purposes of third parties shall be contractually excluded.
- The contracting entity assumes the responsibility for the legitimacy of the processing and shall be the interlocutor for the party involved (customer, employee etc).

## 4. Rights of the parties involved

With respect to their personal data, the parties involved shall have the following precedent rights:



- They can (also in writing) request information on the data, saved on their person, on their origin and purpose.

In the event of a transmission they shall be entitled to be notified about the receiver and/or categories of receivers.

There is no right in notification in the event that such a notification is connected with a disclosure of business secrets.

- They shall have a right in correction, if it turns out that their personal data are false or incomplete.
- They have a right in blocking these data; if neither their correctness nor their incorrectness can be determined.
- They have the right that his data be deleted, if the data processing was illicit or the data are no longer required for the purpose of data processing. If there are legal obligations to save the data, data shall be blocked instead of deleted.
- They shall have the right to object, if their data are used for

- advertisement

- or market and opinion research purposes.

- Moreover, they have a general objection right, which shall be accounted for in the event that a control shows that a legal interest of the parties involved prevails the interest of the competent entity because of their particular personal situation.

A party involved may exercise its rights extrajudicially and free of charge and also against the transferring affiliate in an EU/EEA-state.

## 5. Process-related questions

### 5.1 Implementation within the company

The respective management of an affiliate in a third country shall ensure the implementation of this directive, which in particular means that it shall inform its employees correspondingly.

Part of this information is also the note that violations of this directive can result in criminal and other consequences, arising from liability or employment law.

### 5.2 Questions and concerns

The parties concerned can at any time contact the locally responsible person and/or, where applicable, the competent authority with questions and concerns. The affiliate in the third country commits to cooperate with and to respect the position and requests of the data protection authorities of the state, in which the transferring affiliate has its seat. Also a transferring affiliate, in an EU/EEA-state (see footnote on page 1) has the right to verify in individual cases the data processing, executed by the receiving affiliate in a third country. It shall impose identified rights of parties involved and assist parties involved, who suffered damages on the grounds of a violation of the obligations, resulting from this directive in the exercise of their rights against the responsible affiliate in the third country.

## 6. Publicity

This directive is made accessible to the parties involved in appropriate form, e.g. via the Internet.

## 7. Adherence control

Next to the revision bodies of the is AG and the affiliate in the third country, the person, who is in charge of the data protection in the affiliate in the third country controls the adherence to this directive as data protection coordinator.





*Reisen erster Klasse*

These persons shall be assisted by the management and the respective executives and shall be informed correspondingly in the event of complaints or violations of the obligations, arising from this directive. In these events, the data protection coordinators contact the data protection officer of the is AG, whose decisions to remedy data protection violations shall be respected by the management of the affiliate in the third country. All employees and other parties involved can at any time contact the data protection coordinators or the data protection officer is AG with questions, remarks and complaints.

**Contact address:**

Oliver Schell  
Sandweg 1  
96132 Schlüsselfeld-Aschbach  
Germany  
Tel.: +49 - 9555 - 92 29-0  
Fax: +49 - 9555 - 92 29-29  
E-Mail: [Oliver.Schell@phoenix-reisemobile.de](mailto:Oliver.Schell@phoenix-reisemobile.de)

