



Corporate Guidelines
for Subsidiaries (in “Third Countries”)^{*)}
for the Protection of Personal Data

^{*)} For the purposes of these Corporate Guidelines, “Third Countries“ are all those countries, which do not provide an adequate level of data privacy protection within the meaning of Article 25 of EU Directive 95/46/EC of October 24, 1995 (Official Journal No. L281/31).
Countries which ensure an adequate level of data privacy protection include the member states of the European Union (EU), the other states that are party to the European Economic Area (EEA) Agreement and those states recognized by the Commission of the European Union as providing an adequate level of data protection;

Table of Contents

	Page
1. Objective and scope of application	3
1.1 Binding character of the Guidelines	3
1.2 Relationship to statutory regulations	3
2. Definitions	4
3. Principles for Processing Personal Data	5
3.1 Legitimacy of Data Processing	5
3.2 Purpose	5
3.3 Transparency	5
3.4 Data quality	6
3.5 Transfer of Personal Data within a Third Country or to another Third Country	6
3.6 Special categories of Personal Data	6
3.7 Direct marketing/market research or opinion polling	7
3.8 Automated individual person-related decisions	7
3.9 Data security	7
3.10 Confidentiality of Data Processing	7
3.11 Data Processing Contracts	8
4. Rights of the Data Subject	8
5. Procedural issues	9
5.1 Implementation in the Siemens Subsidiary	9
5.2 Questions and complaints	9
6. Publicity	9
7. Monitoring compliance	9

1. Objective and scope of application

The objective of these binding corporate guidelines (“Guidelines”) is to safeguard Personal Data which needs to be transferred within the Siemens Group of companies worldwide in the course of business processes. For this purpose, it is essential also for Siemens Subsidiaries with their seat in Third Countries to establish harmonized data privacy protection and data security standards for the processing of Personal Data within the meaning of the EU Data Protection Directive and thus to assure that these companies also provide an adequate level of data privacy protection and sufficient guarantees within the meaning of the EU Directive regarding the protection of the right to privacy and the exercise of related rights.

These Guidelines provide a framework for the Processing of Personal Data relating to Siemens employees, Customers and Suppliers, other business partners, prospective partners and other Data Subjects by Siemens Subsidiaries based in Third Countries, regardless of the origin of this Personal Data.

1.1 Binding character of the Guidelines

The provisions of these Guidelines become binding on all Siemens Subsidiaries (see Section 2 “Definitions”) with a seat in Third Countries as soon as such Siemens Subsidiaries commit to Siemens Aktiengesellschaft (“Siemens AG”) in a binding manner to comply with these Guidelines. The Guidelines are to be brought to the attention of employees of the affected Siemens Subsidiaries and are to be observed by all such employees. Companies other than Siemens Subsidiaries, in which Siemens AG maintains a direct or indirect holding, may voluntarily make a legally binding commitment to comply with these Guidelines.

Siemens AG maintains an electronic register of all Siemens Subsidiaries based in Third Countries which have made a written commitment to comply with these Guidelines. If such a commitment ends (e.g. through withdrawal, revocation, termination, expiration, or divestiture from the Siemens Group), this should also be entered in the register; in this case the commitments arising from these Guidelines shall continue to apply to the Processing of Personal Data that is performed up to the expiry of the commitment.

If a Siemens Subsidiary has not yet made a commitment to comply with these Guidelines, the permissibility of the Data Transfer to this Subsidiary is to be reviewed in each individual case and is to be assured through appropriate special measures (see Clause 3.5).

1.2 Relationship to statutory regulations

Existing statutory obligations are not affected by these Guidelines.

Each Siemens Subsidiary must itself review (e.g. through its data privacy protection officer or legal department) whether such statutory regulations exist (e.g. data privacy protection laws) and, where they exist, must assure their adherence and compliance. If statutory regulations, which apply in Third Countries, conflict with the obligations imposed by these Guidelines, the affected Siemens Subsidiary must inform immediately so that the conflict can be entered into the register according to Section 1.1 and must also inform the Siemens Subsidiaries in EU/EEA states (see footnote on page 1), which had already transferred Personal Data to the relevant

- **Transfer of Personal Data or Data Transfer:** the disclosure of Personal Data to Third Parties, the transmission of such data to Third Parties, or the process of making such data available to Third Parties in any form for inspection or retrieval.

3. Principles for Processing Personal Data

The following principles apply to Processing Personal Data by Siemens Subsidiaries in Third Countries and are to be adhered to.

3.1 Legitimacy of Data Processing

The Personal Data referred to in Section 1, Paragraph 2 may be Processed only if at least one of the following prerequisites is fulfilled:

- The Data Subject has given its effective consent.
- Processing serves the purpose of a contractual relationship or contract-similar trust relationship with the Data Subject.
- Data Processing is required to maintain the Responsible Principal's justified interests and there are no grounds for assuming that the Data Subject has an overriding legitimate interest in precluding Data Processing.
- Processing is stipulated or permitted in accordance with national law or regulations.

These Guidelines shall be complied with in any case.

3.2 Purpose

Personal Data may only be collected and processed for specified, unambiguous and lawful purposes. Siemens Subsidiaries based in Third Countries, which have committed to comply with these Guidelines, are obligated to adhere to the purpose of Data Transfer when storing or otherwise using Personal Data transferred to them by a Siemens Subsidiary from an EU/EEA state (see footnote on Page 1). The purpose of Data Processing may only be changed with the Consent of the Data Subject or if permitted by the national law to which the data exporter from the EU/EEA state is subject.

3.3 Transparency

Data Subjects whose Personal Data is transferred by a Siemens Subsidiary from an EU/EEA state (see footnote on page 1) must be provided with the following information by the receiving Siemens Subsidiary in the Third Country (in consultation with the data exporter, where applicable):

- identity of the Responsible Principal in the Third Country and of the data exporter in the EU/EEA state.
- purpose of Data Transfer
- other information to the extent required for reasons of equity, e.g.
 - rights of information, rectification and erasure
 - right of objection if Personal Data is used for advertising.

Such information does not need to be furnished if

- this is required for the protection of either the Data Subject or for the rights and obligations of other persons, or
- the Data Subject has already been informed, or
- the cost and effort associated with it is unreasonable, or
- the data is publicly accessible and the provision of information is unreasonable due to the multitude of cases concerned.

3.4 Data quality

Personal Data must be factually correct and – if necessary – kept up to date. Appropriate measures are to be taken to assure that inaccurate or incomplete data is corrected or erased. Data Processing has to be arranged with the objective to collect, process or use only such Personal Data as is required – i.e., as little Personal Data as possible. In particular, use is to be made of the possibility of anonymous or pseudonymous data, provided that the cost and effort involved is commensurate with the desired purpose. Statistical evaluations or studies based on anonymous data or data used with pseudonyms are not relevant for data privacy protection purposes, provided that such data cannot be used to identify the Data Subject. Personal Data, which are no longer required for the business purposes for which they were originally collected and stored, are to be erased, subject to adherence to the statutory retention provisions.

3.5 Transfer of Personal Data within a Third Country or to another Third Country

Transfer of Personal Data received from a Siemens Subsidiary of an EU/EEA state (see footnote on page 1) to another location in the same Third Country or to another Third Country is only permissible, if at least one of the following prerequisites are fulfilled:

- The Data Subject has given its effective consent.
- Transfer is used to determine the intended purpose of a contractual relationship or contract-similar trust relationship with the Data Subject.
- The recipient shows an adequate level of data privacy protection within the context of these Guidelines; should the recipient be a Siemens Subsidiary, which has undertaken to comply with these Guidelines, it is not necessary to verify whether adequate data privacy protection is shown.

3.6 Special categories of Personal Data

Special categories of Personal Data, e.g., information about a person's racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, health, or sex life, may not be processed as a general principle. Should such information be required, the explicit Consent ("opt-in") of the Data Subject must be obtained, unless

- the Data Subject is not in a position to give his/her Consent (e.g. medical emergency), or
- the Data Subject has already placed the affected data in the public domain, or
- the Processing is essential for the purpose of establishing, exercising or defending legal claims, provided that there are no grounds for assuming that the Data Subject has an overriding legitimate interest in ensuring that such data is not processed, or
- the Processing is permitted by national law (e.g., registration/protection of minorities).

This also applies if Personal Data is collected in a Third Country.

- An Agent is to be selected, who ensures the required technical and organizational data security measures required to perform Data Processing that is compliant with data privacy protection.
- The performance of Data Processing must be governed by a written or otherwise documented contract, which specifies the rights and obligations of the Agent.
- The Agent is to be contractually obligated to process the data obtained from the Responsible Principal only as provided in the contract and in accordance with the instructions issued by the Responsible Principal. Data Processing for the Agent's own purposes or for the purposes of a Third Party must be contractually excluded.
- The Responsible Principal retains responsibility for the legitimacy of the Data Processing and is the contact person for the Data Subject (Customers and Suppliers, employees, etc).


4. Rights of the Data Subject

The Data Subject has specific mandatory rights as regards his/her Personal Data:

- The Data Subject can demand **information** (including, in writing) about any Personal Data stored about him/her and about its origin and the purposes for which it is being stored. For Data Transfers, the Data Subject also has the right to information about the recipient (or categories of recipients) of such Personal Data. The Data Subject has no right to information if the disclosure is in connection with business or trade secrets.
- The Data Subject has the right of **rectification** if his/her Personal Data is shown to be inaccurate or incomplete.
- The Data Subject has the right of **blocking** his/her Personal Data, if neither their accuracy or inaccuracy can be determined.
- The Data Subject has the right of **erasure** of his/her Personal Data if the Data Processing was impermissible or the Personal Data for the purpose of the Data Processing are no longer required. If there are statutory retention obligations, then the blocking of the Personal Data takes precedence over the erasure.
- The Data Subject has the right of **objection** if his/her Personal Data is used for
 - advertising purposes, or
 - market research or opinion polling purposes.
- The Data Subject also has a **general right of objection** which is to be taken into account if a review reveals that, due to the Data Subject's special personal situation, his/her legitimate interests override those of the Responsible Principal.

The Data Subject can exercise these rights out of court at no cost and against the transferring Siemens Subsidiary in an EU/EEA state.



Commitment 
to comply with
Corporate Guidelines
for Subsidiaries (in “Third Countries”)
for the Protection of Personal Data

To
Siemens AG
ZV CPO
D-80312 Munich
E-Mail: datenschutz@siemens.com

The Siemens Subsidiary designated below hereby confirms that it has implemented the Guidelines referred to above in a binding manner effective as of _____ (date: DD.MM.YY):

(Name and registered office/principal place of business of the Siemens Subsidiary, include City and Country)

(ARE)

In accordance with Sections 5.2 and 7 of the Guidelines, the following person is the data privacy protection coordinator and is responsible, in particular, for monitoring compliance with the Guidelines:

Name, first name:

Business address:

Tel.:

Fax:

e-mail:

This coordinator is InfoSec Officer too: Yes No

The Siemens Subsidiary shall ensure that the Guidelines are implemented and shall, in particular, instruct its employees in accordance with Section 5.1.

_____ (Place)

_____ (Date)

(Signature(s) of the Siemens Subsidiary executive management)

(Names, typed)