SIEMENS

Binding Corporate Rules ("BCR") – Summary of Third Party Rights

This document contains in its Sections 3 – 9 all provision of the "Binding Corporate Rules (BCR) for Siemens Group Companies and Other Adopting Companies for the Protection of Personal Data" which are binding vis-à-vis data subjects, by virtue of third-party beneficiary rights.

1. Purpose of the BCR

Protecting the security and privacy of personal data is important to Siemens. Therefore, Siemens conducts its business in compliance with applicable laws on data privacy protection and data security. The BCR are internal rules adopted by Siemens, i.e. Siemens AG and its participating group companies, to adduce "adequate safeguards for the protection of the privacy and fundamental rights and freedoms of individuals" within the meaning of applicable data protection law, especially the data protection laws of member states of European Economic Area ("**EEA**").

2. Scope of the BCR

The BCR apply to the processing of all personal data relating to data subjects by participating companies established

- outside an EEA country to the extent that this personal data has been transferred from a participating company established in an EEA country or established in a country with an adequate level of data protection as acknowledged by a decision of the EU Commission to a participating company established outside the EEA; and
- in an EEA country or in a country with an adequate level of data protection as acknowledged by a decision of the EU Commission.

3. Substantive principles for the processing of personal data

The following principles which derive specifically from the EU Data Protection Directive 95/46/EC and the Madrid Resolution of November 5, 2009 apply to the processing of personal data by participating companies within the scope of these BCR:

3.1 Legitimacy & legality of data processing

The processing of personal data shall be done lawfully in compliance with the relevant statutory provisions and with due regard for the principles laid down in these BCR.

Processing is only permissible if at least one of the following prerequisites is fulfilled:

- The data subject has freely given his/her unambiguous, effective consent; or
- Data processing is for the purpose of establishing a contractual relationship or similar relationship of trust with the data subject; or
- Processing is necessary to safeguard justified interests of the controller (for the purpose of these BCR "**controller**" shall mean the company which determines the purposes and means of data processing; dependent branches, places of business and permanent establishments are part of the controller) and there are no grounds for assuming that the data subject has an overriding legitimate interest in precluding data processing; or
- Processing is stipulated or permitted by national law and regulations that apply for the controller; or
- Processing is necessary for compliance with legal obligations to which the controller is subject; or
- Processing is required, exceptionally, to protect the life, health or safety of the data subject.

The controller shall provide simple, fast and efficient procedures that allow the data subject to withdraw his/her consent at any time.

3.2 Purpose

Personal data shall be processed exclusively for specified, explicit and legitimate purposes. Under no circumstances, shall personal data be processed in a way incompatible with the legitimate purposes for which the personal data was collected. Participating companies are obligated to adhere to these original purposes when storing and further processing or using data transferred to them by another participating company; the purpose of data processing may only be changed with the consent of the data subject or to the extent permitted by the national law to which the participating company transferring the data is subject.

3.3 Transparency

All participating companies shall process personal data in a transparent manner. Data subjects whose personal data is processed by a participating company shall be provided with the following information by the participating company (in consultation with the transferring company, if applicable):

- Identity of the controller and of the transferring company;
- Categories of recipients or identity of the receiving entity;
- Purpose of processing;
- Origin of the data (unless this is personal data collected directly from the data subject);
- Right of objection to the processing of personal data of the data subject for advertising purposes;
- Other information to the extent required for reasons of equity, e.g. rights of information, rectification and erasure.

To the extent that the personal data was not collected directly from the data subject, such information - as an exception - need not be provided, if this non-provision of information is necessary in order to protect the data subject or the rights of other persons, if the data subject has already been informed or if this would involve disproportionate effort.

3.4 Data quality and data economy

Personal data must be factually correct and – if necessary – kept up to date. Appropriate measures are to be taken to ensure that inaccurate or incomplete data is corrected or erased.

Data processing shall be guided by the principle of data economy. The objective is to collect, process and 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 anonymized or pseudonymized data are not relevant for data privacy protection purposes, provided that such data cannot be used to identify the data subject.

Personal data which is no longer required for the business purposes for which it was originally collected and stored, is to be erased. In the event that statutory retention periods apply, the data shall be blocked rather than erased.

3.5 Onward transfer of data

The transfer of personal data from a participating company to a non participating company (i.e. a company that is not bound to the BCR) outside the EEA is only permissible under the following conditions:

- The receiving entity is endowed with an adequate level of protection for personal data within the meaning of Article 25 of the EU Data Protection Directive 95/46/EC, e.g. by concluding an EU standard contract (Standard Contractual Clauses for Data Processors 2010/87/EU or Standard Contractual Clauses between Data Controllers 2001/497/EC or 2004/915/EC) or by concluding other appropriate contractual agreements between the transferring and the receiving entity;
- The transfer is permissible under the exceptions defined in Article 26 of the EU Data Protection Directive 95/46/EC;
- If the receiving entity is a processor, the conditions set out in Article 16 and 17 of the EU Data Protection Directive 95/46/EC must additionally be satisfied.

3.6 Special categories of personal data

Special categories of personal data, in other words information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, may not be processed as a general principle.

Should the processing of special categories of personal data be necessary, the explicit consent 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) and processing is necessary to protect the vital interests of the data subject or of another person; or
- processing is required in connection with medical diagnosis, preventive medicine, the provision of care or treatment or the management of healthcare services where data processing is carried out by medical staff who are subject to the obligation of professional secrecy or by other staff subject to an equivalent obligation of secrecy, or
- the data subject has already made public the data in question; or
- processing is necessary for the establishment, exercise or defense of legal claims in court proceedings, 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
- processing is expressly permitted by law under the applicable national legislation (e.g. for the purpose of registering/protecting minorities), and additional guarantees within the meaning of the EU Data Protection Directive 95/46/EC are provided for the processing of the data, including specifically adequate security measures for this data.

The competent Data Privacy Officer (DPO) of the participating company shall be consulted prior to the processing of special categories of personal data.

3.7 Automated individual decisions

If personal data is processed for the purpose of making automated individual decisions, the legitimate interests of the data subject must be ensured through appropriate measures. Decisions which have negative legal consequences for the data subject or substantially prejudice the data subject, may not be reached exclusively on the basis of an automated individual procedure designed to evaluate an individual's personal characteristics, i.e. decisions may not be exclusively based on the use of information technology. An exception applies only if the decision

- is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as giving him/her the opportunity to put his point of view; or
- is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

3.8 Data security

Controllers are to take appropriate technical and organizational measures to ensure the requisite data security, which protects personal data against accidental or unlawful erasure, unauthorized use, alteration, against loss, destruction as well as against unauthorized disclosure or unauthorized access. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. Special categories of personal data are to be given special protection.

The security measures to be provided relate in particular to computers (servers and workplace computers), networks, communication links and applications.

To ensure an adequate level of technical and organizational measures for data protection, Siemens introduced the Corporate Information Security Guide with binding effect for the entire Siemens group.

Specific measures used to ensure adequate protection of personal data include admission controls, system access controls, data access controls, transmission controls, input controls, job controls, availability controls and segregation controls.

All workplace computers – including mobile devices (e.g. laptops) – are password-protected. The Siemens intranet has a firewall system to protect internal company content from unauthorized external access. Transmission of personal data within the company's own network is typically encrypted – to the extent that the nature and intended purpose of the personal data requires this.

3.9 Confidentiality of data processing

Only personnel who are authorized and have been specifically instructed in compliance with data privacy protection requirements, may collect, process or use personal data. Access authorization of the individual employee will be restricted according to the nature and scope of his/her particular field of activity. The employee is prohibited from using personal data for private purposes, from transferring or from otherwise making available personal data to unauthorized persons. Unauthorized persons in this context include, for example, other employees, to the extent that they do not require the personal data to complete their specialist tasks. The confidentiality obligation continues beyond the end of the employment relationship of the employee in question.

3.10 Commissioned data processing

If a participating company commission another company ("**processor**") to process personal data under the terms of these BCR, the following requirements must be observed:

- The processor is to be carefully selected by the controller; a processor shall be selected who is able to ensure the necessary technical and organizational security measures required to perform data processing in compliance with data privacy protection regulations;
- The controller shall ensure and regularly verify that the processor remains fully compliant with the agreed technical and organizational security measures;
- The performance of commissioned data processing must be regulated in a written or otherwise documented contract, in which the rights and obligations of the processor are unambiguously defined;
- The processor must be bound by contract to process the data received from the controller only within the contractual framework and in accordance with the instructions issued by the controller. The processing of data for the processor's own purposes or for the purposes of a third party must be prohibited by contract;
- The controller retains responsibility for the legitimacy of processing and continues to be the point of contact for the data subject.

4. Substantive rights of the data subject

Data subjects have the inalienable rights listed below in respect of their personal data processed by a participating company within the scope of these BCR.

- The data subject can demand communication to him in an intelligible form of the personal data processed in relation to him/her, of any available information as to its source, and the purpose of the processing. The data subject also has the right to information about the identity of the controller and, in the event of the transfer of personal data, the data subject also has the right to information about the recipients or categories of recipients. The right to information also covers the logical structure of automated processing operations, to the extent that automated decisions are affected. When provided for by applicable local law, the data subject does not have a right to information if it would involve considerable impairment of business purposes, including specifically if the disclosure of business secrets and the interest in safeguarding the business secrets outweighs the data subject's interest in disclosure. Local legal regulations may restrict the data subject's right to information if this right is exercised repeatedly within a short period of time, unless the data subject can show a legitimate reason for the repeated assertion of claims for information. The participating company may charge the data subject a reasonable fee for providing the information, to the extent that the applicable national law permits this.
- The data subject can demand **rectification** if his/her personal data is found to be incorrect or incomplete.
- The data subject has the right to demand that his/her personal data be **blocked** off if it is not possible to establish whether the data is correct or incorrect.
- The data subject has the right to demand that his/her personal data be **erased** if the data processing was unlawful or has become unlawful in the interim or as soon as the data is no longer required for the purpose of

the processing. Justified claims by the data subject for erasure are to be acted on within a reasonable period, to the extent that statutory retention periods or contractual obligations do not prevent erasure. In the event of statutory retention periods, the data subject may demand that his/her data be blocked rather than erased. The same applies if it would be impossible to erase the data.

- The data subject has the right to **object** to the processing of his/her personal data for advertising purposes or for purposes of market research and/or opinion polling purposes. The data subject shall be informed of his/her right to object free of charge.
- The data subject also has a **general right of objection** to the processing of his/her personal data, if because of the data subject's special personal situation, the legitimate interest of the data subject outweighs the legitimate interest of the controller in processing the personal data.

The data subject can assert the above rights in writing vis-à-vis the respective participating company, the competent Data Privacy Officer (DPO) of such participating company or the Global Data Privacy function (LC CO DP) of Siemens AG. The justified request of the data subject shall receive a response from the contacted entity within a reasonable period. The response shall be in written form (e-mail is sufficient).

5. Binding nature vis-à-vis data subjects

The regulations in the BCR contained in Sections 3 - 9 of this document are also binding vis-à-vis data subjects, by virtue of third-party beneficiary rights.

Data subjects can choose to lodge a complaint for non-compliance with the regulations of the BCR contained herein by a participating company either against the participating company or against Siemens AG (LC CO DP).

In addition, data subjects are entitled to enforce compliance with one of the above-mentioned third party beneficiary rights by a participating company, by lodging a complaint before the competent data protection authority or by seeking other legal remedies in the competent courts. Data subjects may claim compensation for damages.

Data subjects can choose to lodge such a complaint

- before the jurisdiction of the participating company that transferred the data; or
- before the jurisdiction of the headquarters of Siemens AG; or
- before the competent data protection authority.

This means that in the event of a breach of the BCR regulations by a participating company established outside the EEA, courts and authorities within the EEA are also competent. The data subject holds the same rights vis-à-vis the participating company that has accepted liability, as if the breach had been committed by a participating company established in an EEA country.

The competence of courts and authorities in the EEA as described above does not apply however if the data recipient is established in a country outside the EAA but that country does have an adequate level of data protection as acknowledged by a decision of the EU Commission.

In order to ensure that data subjects enjoy legally enforceable third party beneficiary rights also in those countries where the granting of third party beneficiary rights in the BCR document might not be sufficient, Siemens AG will – to the extent necessary – draw up additional contractual agreements with the relevant participating companies allowing for this. A third party beneficiary clause granting the necessary rights to data subjects is included in the Declaration of Commitment which group companies sign to signify their acceptance and implementation of the BCR. The same applies for the Adoption Agreement which the other adopting companies conclude with Siemens AG.

6. Complaint process

Data subjects can contact the competent complaint handling department in Siemens AG (LC CO DP; for contact details, see Section 10) or the participating company's competent local point of contact for data protection (generally the Data Privacy Officer (DPO)), at any time, with complaints about a breach of the BCR by a participating company or with any questions. The data subject shall be given prompt confirmation of receipt of the complaint at the entity contacted and the complaint shall be processed within three (3) months of receipt of the complaint. This timeframe can be reasonably exceeded in case of delays not attributable to the participating company, e.g. in case of a failure of the data subject to timely provide information that is reasonably necessary.

The employees involved with complaint processing in the competent complaint handling department benefit from an appropriate level of independence in the exercise of this function.

In any inquiry, the participating company and LC CO DP are obligated to cooperate with the data protection authorities of the country and to respect their opinions.

7. Mutual assistance and cooperation with the data protection authorities

Siemens AG and the participating companies will trustfully cooperate and support one another in the event of inquiries and complaints from data subjects with regard to non compliance with the BCR.

Siemens AG and the participating companies further undertake to trustfully cooperate with the competent data protection authorities in the context of implementation of the BCR. They will answer BCR-related requests from the data protection authority within an appropriate timeframe and in an appropriate fashion and will follow the advice and decisions of the competent data protection authority with regard to implementation of the BCR.

8. Relationship between BCR and local statutory regulations

The legitimacy of processing of personal data is judged on the basis of the applicable local law. To the extent that the applicable local law stipulates a higher level of protection of personal data than these BCR, data processing shall be in accordance with the applicable law. Each participating company shall check for itself (e.g. through its Data Privacy Officer (DPO) or by the Legal department), whether such local statutory regulations (e.g. data privacy laws) exist and shall ensure compliance with these. If the applicable local law provides a lower level of protection for personal data than these BCR, the present BCR shall be applied.

In the event that obligations arising from the applicable local law are in conflict with the BCR, the participating company shall inform the LC C DP without undue delay. LC C DP will record the reported conflict.

LC C DP will inform all participating companies which previously transferred data to the participating company in question, of the reported conflict between the BCR and the local law. LC C DP will also inform the competent data protection authority of the regulatory conflict and, together with the data protection authority and the participating company, will seek a practical solution that comes as close as possible to the principles in the EU Data Protection Directive 95/46/EC.

9. Liability

Siemens AG assumes liability for non-compliance with the BCR by participating companies established outside the EEA. Siemens AG undertakes to monitor BCR compliance by participating companies established outside the EEA and to ensure that participating companies established outside the EEA take the necessary corrective actions to remedy breaches of the BCR.

Siemens AG further undertakes to pay compensation for damages in the event of a proven breach of the BCR and a resulting violation of a data subject's rights.

The burden of proof lies with Siemens AG. Siemens AG shall demonstrate that no breach of the BCR has taken place or that the participating company established outside the EEA is not responsible for the breach of the BCR on which the data subject's claim for damages is based.

SIEMENS

10. Contact

Data subjects can raise any concerns with the Data Privacy Officer (DPO) of the relevant participating company or with the global Data Privacy function of Siemens AG:

Siemens AG

LC CO DP

St.-Martin-Str. 76

D-81541 Munich

Email: datenschutz@siemens.com

Internet: http://www.siemens.com