Binding Corporate Rules for the Protection of Personal Data ("BCR")

Summary of Third Party Rights

 siemens.com

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 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 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 GDPR 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 given consent to the processing of his or her personal data for one or more specific purposes;
- Data processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which 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) is subject;
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person; or
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
- 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 limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3.3 Transparency, fairness and lawfulness

All participating companies shall process personal data lawfully, fairly and in a transparent manner in relation to the data subject. Data subjects whose personal data is processed by a participating company shall be provided with the information required by Article 13 and 14 GDPR by the participating company (in consultation with the transferring company, if applicable), in particular:

- Identity and contact details 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; and
- Other information, e.g. rights of access, rectification and erasure.

3.4 Data quality and data minimization

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate in regard to the purposes for which it is processed, is erased or rectified without delay.

Data processing shall be guided by the principle of data minimization. The objective is to process only such personal data as is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. 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.

3.5 Limited storage periods

Personal data which is no longer required for the business purposes (taking retention rights and duties into account), for which it was originally collected and stored, is to be erased.

3.6 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 framework of Chapter V of the GDPR (Art. 45 – 49 GDPR). That means that the conditions laid down in Chapter V of the GDPR are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organization to another third country or to another international organization.

3.7 Special categories of personal data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited 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,

- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The competent Data Privacy Manager (DPM) of the participating company, i.e. the person with responsibility for implementation of and compliance with the BCR, determined by the participating company, shall be consulted prior to the processing of special categories of personal data.

3.8 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.

3.9 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, the Siemens Information Security Policy was introduced with binding effect for the entire Siemens group by a Circular.

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 complex password-protected and - as a general rule – have a hard drive encryption. 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.

3.10 Confidentiality of data processing

Only personnel who are authorized and have been specifically instructed in compliance with data privacy protection requirements, may process 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.

3.11 Commissioned data processing

If participating companies commission another company 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 contract, in which the rights and obligations of the processor are unambiguously defined, including the duty to notify without undue delay any personal data breaches to the controller, whereby such personal data breaches should be documented (comprising the facts relating to the personal data breach, its effects and the remedial action taken) and the documentation should be made available to the supervisory authority on request;
- 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; and
- 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 has the **right of access** and can demand communication to him/her 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 is restricted if it is not possible to establish the accuracy of the personal data.
- 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 restricted 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 participating company, the competent DPM of such participating company or the Global Data Privacy Function 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 provisions in the BCR contained in 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.

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 and the competent court of the EU member state.

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 EEA 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.

6 Complaint process

Data subjects can contact the competent complaint handling department in Siemens AG (for contact details see Section 10) or the participating company's competent DPM, 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 without undue delay and within one (1) month of receipt of the complaint; in complex or in exceptional cases within three (3) months of receipt of the complaint, with the duty to inform the data subject accordingly. This timeframe can be reasonably exceeded in case of delays not attributable to 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 Siemens AG 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.

Where a data protection impact assessment under Art. 35 GDPR indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the competent supervisory authority should be consulted prior to the processing (Art. 36 GDPR).

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 DPM 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 Global Data Privacy Function of Siemens AG without undue delay. The Global Data Privacy Function of Siemens AG will record the reported conflict in the status overview.

The Global Data Privacy Function 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 and 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 GDPR.

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.

10 Contact

Data subjects can raise any concerns with the DPM 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 München

E-Mail: datenschutz@siemens.com
Internet: http://www.siemens.com/datenschutz