SIEMENS

Legal and Compliance

Siemens Circular Circular No. 216, Version 1.0

Specialist responsible
Dr. Axel Kessler, LC C DP
Tel.: +49 (89) 636 32323
mailto:axel.kessler@siemens.com

Scope
Siemens AG, Affiliated Companies

SIPEX
- - -

Distribution
Members of the Managing Board; CEOs, CFOs of the Divisions / Healthcare / BUs, Countries, Affiliated Companies (acc. to CISS); Heads of Corporate Core / Corporate Services; GCs; Global Position Levels 1 – 4; Central Works Council; GSpA

Munich, October 1, 2014

Binding Corporate Rules for the Protection of Personal Data

The intragroup exchange of data across international borders forms an essential part of the business activities of an internationally operating company such as Siemens. Under the data protection laws in the European Union (EU), the transfer of personal data to a country outside the European Economic Area (EEA), for which the European Commission did not acknowledge an adequate level data protection (third country), is only permissible if the recipient in such third country ensures adequate safeguards for the protection of personal data.

The “Binding Corporate Rules (BCR) for Siemens Group Companies and Other Adopting Companies for the Protection of Personal Data” ensure such safeguards on group level. The BCR apply in particular to the processing of personal data by

(i) units of Siemens AG and Affiliated Companies located within the EEA, and

(ii) Affiliated Companies located outside the EEA if the personal data originate from Siemens AG / Affiliated Companies located within the EEA.

The BCR must be implemented by 30 September 2015 at the latest and their implementation must be documented by signing and returning the Declaration of Commitment contained in the Annex to this Circular.

The BCR are annexed to this Circular. Further information on the scope of the BCR and implementation steps are available on the following Intranet site: http://intranet.siemens.com/data-privacy/BCR.

This Circular is binding for all units of Siemens AG and applies to Siemens’ Affiliated Companies in accordance with Siemens Circular No. 105 (previous Z Circular No. 3/2008) “Implementation of Siemens-internal regulations in Affiliated Companies”. It supersedes Z Circular No. 10/2004. Until the implementation of the BCR the CDP Memo dated 1 December 2003 remains in full force.

sgd. Hoffmann

Annex

The Control Requirement resulting from this Circular is

PCMB Ref	4.3.3.2	that the Binding Corporate Rules (BCR) for the Protection of Personal Data are adhered to and the signed Declaration of Commitment is returned as defined in the respective Circular.

Annex: Binding Corporate Rules

BCR for Siemens Group Companies and Other Adopting Companies for the Protection of Personal Data

Contents

1 Introduction 2
2 Scope of application of the BCR 2
3 Definitions 3
4 Substantive principles for the processing of personal data 4
4.1 Legitimacy & legality of data processing 4
4.2 Purpose 5
4.3 Transparency 5
4.4 Data quality and data economy 5
4.5 Onward transfer of data 6
4.6 Special categories of personal data 6
4.7 Automated individual decisions 7
4.8 Data security 7
4.9 Confidentiality of data processing 7
4.10 Commissioned data processing 8
5 Substantive rights of the data subject 8
6 Description of the data transfer 9
7 Procedural issues 10
7.1 Binding nature of the BCR 10
7.1.1 Binding nature for Siemens group companies and other adopting companies 10
7.1.2 Binding nature vis-à-vis employees of participating companies 11
7.1.3 Binding nature vis-à-vis data subjects 12
7.2 Publicity of BCR 12
7.3 Implementation of BCR in the participating companies 13
7.4 Monitoring of compliance with BCR 13
7.5 Training 14
7.6 Complaint process 14
7.7 BCR audit 14
7.8 BCR updating & change management 15
7.9 Mutual assistance and cooperation with the data protection authorities 16
7.10 Relationship between BCR and local statutory regulations 16
8 Liability 16
9 Contact 17
Change History 17
Appendices 17

1 Introduction

The primary aim of these Binding Corporate Rules (BCR) is to ensure, in all Siemens group companies and other adopting companies, adequate protection of personal data transferred in the course of business from a participating company established in a country in the European Economic Area (EEA country) or established in a country with an adequate level of data protection as acknowledged by a decision of the EU Commission to other Siemens group companies and/or other adopting companies.

For this purpose, it is essential to establish harmonized data privacy protection and data security standards for the processing of such personal data within the meaning of the EU Data Protection Directive and thus to assure that an adequate level of data protection and sufficient guarantees are provided within the meaning of the EU Directive regarding the protection of the right to privacy and the exercise of related rights.

These BCR provide the general and universally valid regulatory framework for the processing of all personal data relating to employees, customers, suppliers, business partners or future business partners and other data subjects by Siemens group companies or other adopting companies

- 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
- for the processing of personal data by participating companies established in an EEA country or in a country with an adequate level of data protection as acknowledged by a decision of the EU Commission.

The present BCR reflect the status and the current international data protection requirements prevailing at the time of entry into force of the BCR, specifically the requirements of the EU Data Protection Directive 95/46/EC, the relevant working documents of the EU Article 29 Data Protection Group and the principles of the International Conference of Data Protection and Privacy Commissioners on International Standards on the Protection of Privacy (referred to below as the "Madrid Resolution") of November 5, 2009.

2 Scope of application of the BCR

All Siemens group companies and all other adopting companies worldwide come within the scope of the BCR.

The BCR apply, on the one hand, to the processing of all personal data transferred from a Siemens group company or other adopting 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 Siemens group company or other adopting company established outside the EEA. They also apply, on the other hand, to the processing of personal data by participating companies established in an EEA country or in a country with an adequate level of data protection as acknowledged by a decision of the EU Commission.

The BCR thus protect all personal data of employees, customers, suppliers, shareholders and all other – present or future – contracting parties and business partners of a Siemens group company or other adopting 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, including to the extent that such data is transferred to a participating company established outside the EEA and is processed further there by the latter.

3 Definitions

The terms used in these BCR are defined as follows

- **BCR** the present Binding Corporate Rules and the regulations contained in them;
- **CDPO** Chief Data Privacy Officer of Siemens AG;
- **Consent** a freely given and informed expression of will whereby the data subject agrees to the processing of his/her personal data [*)];
- **Controller** the legally independent company which determines the purposes and means of data processing. Dependent branches, places of business and permanent establishments are part of the controller;
- **Customers and suppliers** natural and legal persons with whom a business relationship exists or is planned;
- **Data subject** any identified or identifiable natural person whose data is processed. An identifiable person is one who can be identified, directly or indirectly, e.g. by reference to an identification number; legal persons may be included within the scope of the BCR by an agreement to that effect between the company transferring the data and the data recipient;
- **DPO** Data Privacy Officer, i.e. the person with responsibility for implementation of and compliance with the BCR, appointed by the participating company;
- **DPE** Data Privacy Executive of a Siemens group company; this role is performed by the CEO of the Siemens group company in question ;
- **EEA country / EEA countries** the member states of the European Union (EU) and the other signatories to the Treaty on the European Economic Area (EEA);
- **Group company or Siemens group company** Siemens Aktiengesellschaft and any company, in Germany or overseas, in which Siemens Aktiengesellschaft, directly or indirectly, has a majority holding or owns or controls the majority of the voting rights ("Affiliated Companies");
- **LC CO DP / LC C DP** the global Data Privacy function of Siemens AG;
- **Participating company** a Siemens group company for which implementation of these BCR is mandatory, or another Siemens associated company in Germany or overseas in which Siemens AG or an affiliated company has a minority stake and which, with the approval of Siemens AG, has given a voluntary undertaking to comply with the regulations of the BCR by entering into an Adoption Agreement ("other adopting companies");

[*)] *Certain national legislations may set down special requirements for consent, which may affect the validity of the consent.*

- **Personal data** all information relating to a data subject;
- **Processing of personal data** or **data processing** any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as the collection, storage, retention, adaptation, alteration, reading, retrieval, use, disclosure by transmission, blocking, erasure or destruction.
- **Processor** natural or legal person which processes personal data on behalf of a controller
- **Third party** any natural or legal person or other entity other than the data subject, processor or controller;
- **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;

4 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:

4.1 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 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.

4.2 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.

4.3 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.

4.4 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.

4.5 Onward transfer of data

The transfer of personal data from a participating company (i.e. a Siemens group company or other adopting company) to a non participating company (i.e. a company that is not bound to the BCR, including minority owned companies that have not entered into an Adoption Agreement and external companies) 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.

4.6 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 DPO of the participating company shall be consulted prior to the processing of special categories of personal data.

4.7 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**.**

4.8 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, the **Corporate Information Security Guide** was introduced with binding effect for the entire Siemens group by CIT Circular No. 4/2009. The current version of the Corporate Information Security Guide is available on the intranet.

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.

4.9 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.

4.10 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 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.

5 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 participating company, the competent DPO of the participating company or LC CO DP. 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).

6 Description of the data transfer

Siemens has a complex group structure with a large number of group companies and participating companies, between which personal data is exchanged for many purposes. Data exchange takes place between participating companies established in an EEA country and also with participating companies established outside the EEA.

The need for such intra-group exchange of data throughout the Siemens group affects personal data of employees, customers, suppliers, shareholders and other business partners and contracting parties. This includes – depending on the intended purpose – for example, name, Global Identifier, date of birth, nationality, marital status, gender, contact details, address details, account details, bank details, religious affiliation, information about education, knowledge and skills, career, entry date, position level, etc.

This data is processed and transferred within the Siemens group exclusively within the scope of normal business purposes and for purposes of internal administration. Data transfer is thus done for purposes of recruitment, HR administration and staff development, for compliance purposes, for the execution and implementation of assignments and projects for external and internal customers, for the processing of purchase orders and work orders with suppliers and service providers, for the fulfillment of reporting

duties, for the fulfillment of accounts payable or collection of accounts receivable, for accounting, for purposes of internal communication, for purposes of consolidation and pooling of IT processes in certain regions in order to reduce costs, and also in connection with the cooperation and coordination of group companies at Division and regional level or at a global level in the course of global business transactions and projects.

7 Procedural issues

7.1 Binding nature of the BCR

The BCR are comprehensively binding.

7.1.1 Binding nature for Siemens group companies and other adopting companies

The BCR have been adopted by Siemens Aktiengesellschaft (Siemens AG) and put into effect by publication of a Siemens Corporate Circular.

Responsibility for implementation of the BCR in the participating company rests with Executive Management of the participating company, execution in individual cases rests with the entity within that company which processes personal data as part of its specialist role. In Siemens group companies, responsibility rests with the CEO of the Siemens group company in his/her capacity as Data Privacy Executive (DPE).

The BCR are to be observed and complied with by all Siemens group companies and by the other adopting companies, with binding effect.

In order to document acceptance and implementation of the BCR, in the case of group companies, the executive management of the group company in question shall issue an explicit written Declaration of Commitment to the regulations of the BCR. The issuing of this written Declaration of Commitment makes the BCR regulations individually binding for the group company. The Declaration of Commitment is to be signed by the executive management of the group company and returned to LC C DP. The Declaration of Commitment is attached as Appendix 1 to the BCR.

In principle, all Siemens group companies are required to sign the Declaration of Commitment and implement the BCR at the latest within two years from the date of publication of the respective Siemens Corporate Circular (it being understood that during the transition period the group company shall strive to comply to the extent reasonably possible), unless a Siemens group company has been granted an exemption from implementing the BCR for a valid reason, (e.g. mandatory supervisory finance/banking laws and regulations, no business activity, no employees, no processing of personal data, imminent liquidation or divestment). An application for an exemption must be submitted by e-mail to Siemens AG (LC C DP) by the Siemens group company, citing the reason. LC C DP will decide the merits of the application and will notify the group company of its decision.

Companies other than Siemens group companies, in which Siemens AG maintains a direct or indirect holding, may voluntarily make a legally binding commitment to comply with BCR regulations, if the company so wishes and if Siemens AG (LC C DP) agrees to such participation (the “other adopting

companies"). Whether companies other than Siemens group companies are granted the opportunity to participate voluntarily in the BCR process, is at the complete discretion of Siemens AG.

In order to document acceptance and implementation of the BCR by such other adopting company, an Adoption Agreement is concluded between Siemens AG (LC C DP) and the participating company; the BCR are attached as an Annex to the Adoption Agreement. Upon conclusion of the Adoption Agreement, the BCR regulations are individually binding for the participating company. Thus, such other adopting companies will have a transition period for reaching and ensuring compliance with these BCR which shall not exceed two years from the date of execution of the Adoption Agreement (it being understood that during the transition period the other adopting company shall strive to comply to the extent reasonably possible). The text of the Adoption Agreement is attached as an Appendix to the BCR.

LC C DP maintains on the Siemens intranet an electronic register of participating companies which have given an undertaking to comply with the provisions of the BCR by signing a Declaration of Commitment or Adoption Agreement. The latest version of the electronic register (**status overview**) can be viewed at any time on the LC CO DP intranet pages. The status overview also includes and identifies accordingly those group companies that have exceptionally been granted exemption from the obligation to sign and implement the BCR for a valid reason. The status overview also records and identifies the group companies that have not (yet) fulfilled their obligation to accept and implement the BCR.

If a group company has not (yet) issued a Declaration of Commitment to the BCR, the legitimacy of data transfer to that group company is to be reviewed in each individual case and is to be assured through appropriate special measures in accordance with the requirements of Articles 25, 26 of the Directive 95/46/EC. This also applies to other adopting companies as long as they have not yet entered into an Adoption Agreement.

The commitment to comply with the BCR can be ended by withdrawal, cancellation or termination on the part of Siemens AG or on the part of the participating company. The loss of group company status does not automatically mean an end to the obligations arising from the BCR. In this case, termination of the BCR by Siemens AG or the (former) group company is necessary. Also, in the event of withdrawal/cancellation of the Declaration of Commitment or of the declaration to conclude the Adoption Agreement or in the event of termination of the BCR, the obligations arising from the BCR with respect to the personal data processed up until withdrawal, cancellation or termination shall remain, until this data has been erased by the company in question, in compliance with the statutory regulations.

7.1.2 Binding nature vis-à-vis employees of participating companies

Employees of the participating companies are also bound by the regulations of the BCR. The CEO of the particular participating company is obliged to ensure by appropriate means that the BCR have binding legal effect for the employees. In this sense, as the BCR are published by a Siemens Corporate Circular, the BCR become binding on all employees in the same manner (which may differ from country to country) as all other Siemens Corporate Circulars, in particular through the Siemens Business Conduct Guidelines which require the employees' compliance with all relevant Siemens circulars and policies.

The BCR regulations and all other regulations relating to data privacy protection are available at all times to the employees of the participating companies.

The participating companies inform their employees that failure to comply with the BCR regulations may result in disciplinary measures or measures under employment law (e.g. formal warning, dismissal) being taken against the employees.

7.1.3 Binding nature vis-à-vis data subjects

Certain regulations in the BCR are also binding vis-à-vis data subjects, by virtue of third-party beneficiary rights. The regulations in the following sections confer benefits on third parties: Sections 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 5, 7.1.3, 7.6, 7.9, 7.10 and 8.

Data subjects can choose to lodge a complaint for non-compliance with the relevant regulations of the BCR by a participating company either against the participating company or against Siemens AG (LC CO DP). Further details of access to redress and the internal complaint procedure are described in Section 7.6 of these BCR and also in a separate document on the complaint process (Complaint Management Concept).

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.

7.2 Publicity of BCR

The BCR and the third party beneficiary clause are easily accessible for data subjects on an ongoing basis. The data subject can contact the competent DPO of the participating company or alternatively can

contact Siemens AG directly. Siemens AG will make the BCR available to the data subjects in an appropriate manner and on an ongoing basis, specifically by publishing the current version of the BCR on the Siemens internet pages, currently at http://www.siemens.com.

7.3 Implementation of BCR in the participating companies

The Executive Management of a participating company – or the CEO of a participating group company in his/her capacity as DPE – is responsible for the proper implementation of and compliance with the BCR. The executive management of the participating company may delegate this task – but may not delegate responsibility – to the DPO.

Siemens has established a worldwide network of DPOs. On issuing the Declaration of Commitment to the BCR or concluding the Adoption Agreement on the BCR, each participating company indicates the competent DPO and sends the DPO's contact details to LC C DP. The participating company shall notify LC C DP without undue delay of any changes in the identity of the DPO.

The DPO reports at least once a year to the executive management of the relevant participating company and reports regularly – but at least once a year – to the CDPO of Siemens AG. The DPO reports on matters including specifically the degree of implementation of the BCR in the individual participating company.

The CDPO of Siemens AG reports once a year to the Managing Board of Siemens AG. This report includes specifically the degree of implementation of the BCR in all participating companies.

The CDPO is the Chief Data Privacy Officer of Siemens AG and has been appointed as such through a board announcement which has been signed by the CEO and the General Counsel of Siemens AG. CDPO heads the unit LC CO DP which has the operational responsibility for the Siemens data privacy program and the implementation of data privacy requirements, in particular through training measures and monitoring (including incident management and risk assessments). As the head of such unit, CDPO is supported by further employees of such unit who are recruited by and report to him.

7.4 Monitoring of compliance with BCR

Compliance with the BCR by the participating companies is subject to regular review primarily by the DPO appointed by executive management of the participating company. Executive management of the participating company supports the DPO in the exercise of his/her duties and involves him/her in the event of complaints being lodged by data subjects for non-compliance with the BCR.

In the event of serious data privacy breaches and on problems of fundamental importance, the DPO consults the CDPO of Siemens AG and takes account of his/her advice and decisions when remedying such data privacy breaches and problems.

LC CO DP is entitled to carry out random checks on the work of the DPO in connection with the implementation of and compliance with the BCR in the participating company, either by requesting a written self-assessment by the DPO or as part of interviews. The content of such interviews shall be documented by LC CO DP.

Any participating company that transfers data has the right to review the data processing at the recipient participating company in individual cases. In so doing, the transferring company will exercise any rights

which data subjects are ascertained to have, and will support data subjects, who have suffered damage through violations of the obligations imposed by these BCR, in the assertion of their rights against the company responsible.

7.5 Training

A key aspect of proper implementation of the BCR is appropriate provision of information and instruction to employees. This includes informing employees that breaches of the BCR may give rise to consequences for them under criminal, liability or employment law.

Siemens AG offers specific information and special training measures on the BCR designed to provide adequate information and training to the employees of a participating company on the proper handling and protection of personal data in connection with implementation of the BCR. The training measures are targeted specifically at employees who permanently or regularly handle personal data. For these employees, attendance at training courses is mandatory. Training courses on the BCR are to be repeated at appropriate regular intervals.

Information and training measures can include, for instance, the delivery of web-based training (WBT), the provision of appropriate presentations and training material for self study, classroom-based training programs and the organization of workshops tailored specifically to employees.

Successful participation by employees in training programs is to be documented.

Further details are set out in a detailed Training Concept.

7.6 Complaint process

Data subjects can contact the competent complaint handling department in Siemens AG (LC CO DP; for contact details, see Section 9) or the participating company's competent 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 Siemens group company or other adopting 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.

Further details – form of complaint, response time, further procedure following acceptance and/or rejection of complaint, further legal remedies – are set out in a separate Complaint Management Concept which forms an Appendix to the BCR.

7.7 BCR audit

Alongside other existing internal audit and control systems in the Siemens group of companies, Siemens has established a separate BCR audit program in order to ensure that the existence of an adequate level

of data protection as required in the BCR regulations is subject to regular review in the participating companies. Such BCR audits are to be conducted regularly or at the request of the CDPO of Siemens AG; they will be conducted by the Siemens audit organization (F A) with the support of the Siemens data protection organization (e.g. data protection subject matter experts) or by an external auditor. If necessary, a BCR audit can also be initiated by the Siemens internal audit department (F A), by the Audit Committee of Siemens AG, by the executive management or the Audit Committee of the participating company or by the Information Security department (GS IT ISEC).

The BCR audit covers all aspects of the BCR. If a BCR audit concludes that corrective actions need to be taken to remedy a breach of the BCR, the CDPO will monitor that the necessary corrective actions are implemented.

The CDPO of Siemens AG, the responsible member of the Managing Board of Siemens AG and executive management of the audited participating company receive the full BCR audit report. The results of the BCR audit are made available to the relevant data protection authority (i.e. the authorities of those EEA countries from which personal data have been transferred to the audited company) upon request.

The competent data protection authority has the right to conduct its own BCR audit of a participating company. The authority may either conduct the BCR audit itself or have it conducted by an accredited independent auditor. Such official BCR audit is limited exclusively to compliance with the BCR by the participating company. Due regard shall be given to restrictions arising from confidentiality agreements or from business and trade secrets.

Details of the BCR audit are set out in a separate BCR Audit Concept.

7.8 BCR updating & change management

Siemens reserves the right to change and/or update these BCR at any time. Such updating of the BCR may be necessary specifically as a result of changed legal requirements, significant changes to the structure of the Siemens group or official requirements imposed by the competent data protection authorities.

Major changes to the BCR will require, under certain circumstances, the granting of a new approval. All other changes to the BCR are possible without new approval by the competent data protection authorities.

LC C DP maintains a list of all changes/updates to the BCR since the BCR came into force. LC C DP also maintains a regularly updated list of all participating companies which are effectively bound by the BCR (status overview, cf. Section 7.1.1). Transfer of personal data to a newly added participating company is not permitted until the participating company can deliver compliance with the BCR and has issued an effective Declaration of Commitment to the BCR or has concluded an Adoption Agreement on the BCR and has returned the duly signed agreement to LC C DP.

LC C DP notifies the data protection authority of changes to the BCR and also changes to the status overview, upon request, but at least once a year. These notifications contain a brief explanation of the reasons justifying the changes.

7.9 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.

7.10 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 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 LC C DP without undue delay. LC C DP will record the reported conflict in the status overview (cf. Section 7.1.1).

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.

8 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.

9 Contact

Data subjects can raise any concerns with the 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
E-mail: datenschutz@siemens.com
Siemens Intranet website: https://intranet.privacy.siemens.com
Internet: http://www.siemens.com

Change History

Version	Date	Changes	Approval
1.0	October 1, 2014	First publication of Siemens Circular No, 216	Hoffmann

Appendices

Appendix 1: Declaration of Commitment for Group Companies
Appendix 2: Adoption Agreement for Other Adopting Companies
Appendix 3: List of Participating Companies
Appendix 4: BCR Complaint Management