SIEMENS

Legal and Compliance

EU Binding Corporate Rules
BCR for Siemens Group Companies for the Protection of Personal Data

Contents

1 Introduction

Siemens is committed to protecting personal data and respecting privacy rights across all its global operations. To support this commitment, Siemens has established these Binding Corporate Rules (BCRs) to provide the appropriate safeguards required by Article 46 of the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR). The BCR's purpose is to ensure adequate protection when such data is transferred to and further processed by Siemens group companies located in countries outside the European Economic Area. By establishing harmonized data privacy and data security standards across the Siemens group, these BCRs extend the level of protection afforded by the GDPR to all such international transfers and processing operations.

2 Scope of application of the BCR

Siemens group companies in scope

The BCR apply to all Siemens group companies worldwide.

They apply to the processing of personal data by:

a) Group companies that are 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;
b) Group companies established outside an EEA country, if they offer goods or services to natural persons within an EEA country and/or monitor the behavior of natural persons within an EEA country; and
c) Group companies established outside an EEA country, if they have received personal data directly or indirectly from companies that are subject to these BCR under a) or b).

A list of participating Siemens companies is contained in **Appendix 2**.

Material Scope of the BCR, including categories of data subjects, personal data, and processing activities

A description of categories of data subjects, categories of personal data, the type of processing and purposes and covered personal data transfers can be found in **Appendix 3**.

3 Definitions

The terms used in these BCR are defined as follows

- **Applicable law** means the law of the European Union, the law of member states of the European Economic Area or the law of third countries provided that such law respects the essence of fundamental rights and freedoms as recognized in the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights, is based on clear and accessible rules, and is necessary and proportionate in a democratic society to safeguard legitimate objectives (such as national security, public interest, or judicial independence).
- **BCR** the present Binding Corporate Rules and the regulations contained in them;
- **CDPO** Chief Data Privacy Officer of Siemens AG;
- **Consent** any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

- **Controller** the legally independent company which alone or jointly with others, 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;
- **Supervisory authority** refers to the data protection supervisory authority within the European Economic Area (EEA) that has jurisdiction and enforcement powers over the data exporter's data processing activities. This authority is typically determined by the main establishment or single establishment of the data exporter in the EEA.
- **Data exporter** any Siemens group company that

  (a) is 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; or

  (b) offers goods or services to natural persons within an EEA country and/or monitors the behavior of natural persons within an EEA country

  and transfers personal data to a data importer located in a third country;
- **Data importer** any Siemens group company located in a third country receiving Personal Data from a data exporter;
- **Data subject** any identified or identifiable natural person whose data is processed. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- **DPM** Data Privacy Manager, i.e. the person with responsibility for implementation of and compliance with the BCR, determined by the participating company. In some cases this might be the appointed Data Protection Officer;
- **DPE** Data Privacy Executive of a Siemens group company; this role is performed by the CEO of the Siemens group company in question;
- **EEA / EEA country** the member states of the European Union (EU) and the other signatories to the Treaty on the European Economic Area (EEA);
- **General Data Protection Regulation or GDPR** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;
- **Group company or Siemens group company** Siemens Aktiengesellschaft and any company, in Germany or elsewhere, in which Siemens Aktiengesellschaft, directly or indirectly, has a majority holding or owns or controls the majority of the voting rights;
- **LC CO DP** the global data privacy function of Siemens AG which has the operational responsibility for the Siemens data privacy program and the implementation of data privacy requirements; the team of LC CO DPs is led by the CDPO;
- **Participating company** a Siemens group company for which implementation of these BCR is mandatory;
- **Personal data** any information relating to an identified or identifiable natural person;

- **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 country** any country where the level of protection of personal data is not declared adequate by an adequacy decision of the EU Commission;
- **Third party** any natural or legal person or other entity other than the data subject, processor or controller, or persons who, under the direct authority of the controller or processor, are authorised to process personal data; and
- **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 GDPR 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 given consent to the processing of his or her personal data for one or more specific purposes;
- Processing is necessary for the performance of 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 under applicable law (as defined in Section 3) to which 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.

If processing is based on consent: The data subject has the right to withdraw his or her consent at any time. The controller shall provide simple, fast and efficient procedures that allow the data subject to withdraw his/her consent at any time. It shall be as easy for the data subject to withdraw as to give consent.

4.2 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.

When assessing compatibility with original purposes, the following factors shall be taken into account:

- links between the purposes for which the personal data have been collected and the further respective processing purposes;
- the context of the original data collection, with a particular focus on the relationship between participating company and individuals;
- the nature of the personal data, in particular, if the data in question is sensitive personal data;
- possible consequences for individuals if their data are processed further; and
- appropriate safeguards which may include encryption or pseudonymization.

4.3 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 following information:

- the name of the relevant participating company and contact details;
- the contact details of the Data Privacy Officer or designated data privacy contact;
- the purposes for which the participating company intends to use such data and the legal basis for processing the data and where the processing is based on the fifth bullet point of Section 4.1 above, the legitimate interests pursued by the controller or by a third party;
- the recipients or categories of recipients of the data;
- any relevant information about international transfers of the data, including – where applicable – the intent to transfer personal data to a third country or an international organisation and the existence/absence of an adequacy decision by the EU Commission or, in case of transfers not based on an adequacy decision, a reference to the appropriate safeguards in place, which are capable of ensuring data subjects a level of protection essentially equivalent to that which is guaranteed within the European Union, and how or where to obtain a copy of these safeguards;
- the retention period and/or any relevant retention criteria;
- information about the data subject's rights (as further specified in section 5);
- information about any automated decisions/profiling including the logic involved and significance of such processing for the individual;
- the individual's right to withdraw consent, if applicable;
- the right to lodge a complaint with the supervisory authority;
- the consequences of failing to supply data where the processes relate to a statutory or contractual requirement;
- the right to object as set out in section 5 (presented clearly and separately from any other information); and
- any additional information the participating company deems necessary to process the data fairly and lawfully.

Timing and Format
This information must be provided to data subjects free of charge, in a concise, transparent, intelligible and easily accessible form, in clear and plain language.

When personal data is collected directly from the data subject, information shall be provided at the time of collection.

When personal data is obtained from a third party, the participating company shall provide this information within a reasonable period after obtaining the data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed, unless:

- the data subject already has the information; or
- the provision of such information proves impossible or would involve a disproportionate effort. In such cases, the controller shall take appropriate measure to protect the data subject's rights, freedoms and legitimate interests, including making the information publicly available.

4.4 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 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. Statistical evaluations or studies based on anonymized data are not relevant for data privacy protection purposes, provided that such data cannot be used to identify the data subject.

4.5 Limited storage periods

Personal data may only be stored for as long as it is necessary for the purpose for which the data is being processed. This means that personal data must be deleted or anonymized as soon as the purpose of its processing has been fulfilled or otherwise lapses, unless retention obligations under applicable law apply.

4.6 Onward transfer of data

The transfer of personal data from a participating company (i.e. a Siemens group company) to a non participating company 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 by data importers of personal data from the third country or an international organization to another third country or to another international organization. This regularly includes an assessment whether the transfer tool is effective in context of surveillance laws, in particular whether the transfer tool in that relevant case "transports" the EU level of protection to the recipient. Depending on the receiving country, there might be the need for supplementary measures to exclude access to personal data by government authorities.

4.7 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 one of the following alternatives are applicable,

- 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 defense 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 DPM of the participating company shall be consulted prior to the processing of special categories of personal data.

4.8 Criminal conviction data

Processing of personal data relating to criminal convictions and offences, or related security measures will, in addition to the requirements mentioned in 4.1., be carried out only under the control of an official authority or when the processing is authorized by applicable law that provides appropriate safeguards for the rights and freedoms of data subjects.

4.9 Automated individual decisions

Data subjects have the right not to be subject to decisions based solely on **automated processing**, including profiling, which produces legal effects or similarly significant effects, except where this decision (a) is necessary for entering into, or performance of a contract to which the data subject is party, (b) is required or authorized by applicable law which also lays down suitable measures to public safeguard the Data Subject’s rights and freedoms and legitimate interests or, (c) is based on the Data Subject's explicit consent. In the cases referred to in (a) and (c), the Controller implements suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. Automated individual decisions shall not be based on special categories of personal data referred to in 4.7. unless data subject has given explicit consent or processing is necessary for reasons of substantial public interest, and suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests are in place.

4.10 Data security and data privacy by design

Data Security

Participating companies 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. 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 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.

Data Privacy by Design

Beyond security, all participating companies shall also implement technical and organizational measures designed to embed data protection principles into processing activities and systems, in accordance witch the principal data protection by design and by default. These measures shall ensure, in particular:

- Data minimization: systems and processes must be designed to collect and process only the personal data necessary for the specified purposes.
- Purpose limitation and storage limitation: mechanisms are in place to restrict processing to the intended purposes and to delete or anonymize data when no longer needed.
- Default privacy settings: applications and services are configured by default to the most privacy-friendly settings.
- Transparency and accountability: processing activities are documented and designed to enable auditing, and systems facilitate the provision of required information to data subjects regarding their personal data.

4.11 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.

4.12 Commissioned data processing

If participating companies commission another company, including another participating 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; this contract sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.
- That contract or other legal act shall stipulate, in particular, that the processor:
    - processes the personal data only on documented instructions from the controller;
    - ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
    - implements appropriate technical and organizational measures to protect the personal data;
    - shall not engage another processor without prior specific or general written authorisation of the controller and where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract between the controller and the processor shall be imposed on that other processor;
    - taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Section 5;
    - assists the controller in ensuring compliance with the obligations pursuant to applicable law taking into account the nature of processing and the information available to the processor;
    - at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless applicable law requires storage of the personal data; and
    - makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Section and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

- 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.

- **Right of access:** Each data subject has a right of access to personal data processed by any participating company under these BCR. In particular, the data subject is entitled to:

  Confirmation of processing: Obtain from the controller confirmation as to whether or not personal data concerning them are being processed.

  Access to personal data: If personal data are being processed, obtain access to the personal data (including the right to receive a copy of the data undergoing processing) and be informed of the following:

  - the purposes of the processing;
  - the categories of personal data concerned;
  - the recipients or categories of recipients to whom the personal data have been or will be disclosed, including any recipients in third countries or international organizations (and, where personal data are transferred outside the EEA, information on the appropriate safeguards for such transfers);
  - the envisaged period for which the personal data will be stored, or if not known, the criteria used to determine that period;
  - where the personal data were not collected from the data subject, any available information as to their source;
  - the existence of any automated decision-making and, where such processing occurs, meaningful information about the logic involved as well as the significance and envisaged consequences of that processing for the data subject;
  - the data subject's right to request rectification or erasure of the personal data or restriction of processing concerning them, and to object to such processing; and

  the right to lodge a complaint with a supervisory authority.

  Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may restrict the data subject's right to information and refuse to act on the request or charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested.

  The right of access is subject to limitations to protect the rights and freedoms of others. In particular, the controller may restrict the information provided in response to an access request to the extent such disclosure would adversely affect the rights or freedoms of other individuals or reveal trade secrets or other confidential business information. Any such limitation will only be applied in accordance with applicable data protection laws and requires a documented balancing of the relevant interests, rights and freedoms of the data subject and the ones to be protected.

- **Right to rectification**: The data subject can demand **rectification** if his/her personal data is found to be incorrect or incomplete without undue delay. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- **Right to restrict processing**: The data subject has the right to demand from the controller restriction of processing in the following circumstances:
    - Accuracy contested: When the data subject contests the accuracy of his or her personal data, the controller must restrict processing for a period enabling verification of the data's accuracy.
    - Unlawful processing: When processing is unlawful and the data subject opposes deletion, the data subject may request restriction of use instead of erasure.
    - Data no longer needed: When the controller no longer needs the personal data for its original purposes, but the data subject requires it for establishing, exercising, or defending legal claims, the data subject may request restriction instead of erasure.
    - Objection to legitimate interest processing: When the data subject has objected to processing based on public interest or the controller's legitimate interest, and the controller is determining whether its interests override those of the data subject.
- **Right to Erasure ('Right to be Forgotten')**: The data subject has the right to demand that his/her personal data be erased without undue delay if one of the following grounds applies:
    - the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
    - the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
    - the data subject validly objects to the processing according to the paragraph “right to object” below), and there are no overriding legitimate grounds for the controller to continue processing;
    - data subject objects to the processing for direct marketing purposes;
    - the personal data have been unlawfully processed;
    - the personal data have to be erased for compliance with a applicable law to which the controller is subject; or
    - the personal data have been collected in relation to the offer of information society services to a child.

  The right to erasure shall not apply to the extent that processing is necessary:
    - for exercising the right of freedom of expression and information;
    - for compliance with a legal obligation which requires processing by applicable law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
    - for reasons of public interest in the area of public health;

- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- for the establishment, exercise or defence of legal claims.

Where the controller has made the personal data public and is obliged to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

- **Notification of recipients**: The participating company shall communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The participating company shall inform the data subject about those recipients if the data subject requests it.
- **The right to object**: In the scenarios described below, the data subject has the right to object to the processing of their personal data. The controller will abide by any valid request from an individual who objects to the processing of their data.
    - Where personal data are processed for direct marketing purposes, including profiling related to direct marketing, the data subject has the right to object at any time to such processing. Upon such an objection, the personal data will no longer be processed for these purposes.
    - A data subject also has the right to object, on grounds relating to their particular situation, to the processing of their personal data where the processing is based on the legitimate interests of the controller or the performance of a task carried out in the public interest.
    - The data subject shall be explicitly informed of their right to object at the latest at the time of the first communication, and this information shall be presented clearly and separately.

  Under certain circumstances, the controller shall have the right to continue specific types of processing despite an objection. This applies where the controller can demonstrate compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject, or where the processing is necessary for the establishment, exercise, or defence of legal claims. If the objection cannot be processed, a notification explaining the reasons why will be provided. This exception does not apply to the first bullet point above.
- **Right to data portability**: The data subject has the right to receive personal data concerning them in a structured, commonly used, and machine-readable format, and has the right to transmit those data to another controller without hindrance, where:
    - the processing is based on consent or contract; and
    - the processing is carried out by automated means.

  The data subject also has the right to have the personal data transmitted directly from one controller to another, where technically feasible

The right to data portability shall not adversely affect the rights and freedoms of others, including trade secrets or other confidential business information of the participating company or third parties. Any such limitation will only be applied in accordance with applicable data protection laws and requires a documented balancing of the relevant interests, rights and freedoms of the data subject and the ones to be protected

How to exercise data subject rights: The data subject can assert the above rights in writing (e-mail is sufficient) vis-à-vis the participating company, the competent DPM 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, delegation services, 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 fulfilment of reporting duties, for the fulfilment 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 Business Company and country level or at a global level in the course of global business transactions and projects.

A detailed description of categories of data subjects, categories of personal data and covered personal data transfers can be found in **Appendix 3**.

7 Procedural issues

7.1 Binding nature of the BCR

The BCR are comprehensively binding.

7.1.1 Binding nature for Siemens group 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, 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 accept 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 the global data privacy function (LC CO DP) of Siemens AG. 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 CO DP) by the Siemens group company, citing the reason. LC CO DP will decide the merits of the application and will notify the group company of its decision.

LC CO 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. The latest version of the electronic register (**status overview as Appendix 2**) 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 Chapter V GDPR.

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 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, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 5, 7.1.3, 7.8, 7.11, 7.12 and 8 as well as Section 7.10 insofar as it concerns the duty to inform data subjects about any update of the BCR or to the list of participating companies.

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 7.8 of these BCR.

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 supervisory 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 a supervisory authority, in particular in the EEA Member State of the data subject's habitual residence, place of work or place of the alleged infringement; or
- before the competent court of the EEA Member State where the controller or processor has an establishment or where the data subjects has their habitual residence.

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 (see Section 8), as if the breach had been committed by this company itself.

The participating companies accept that data subjects may be represented by a not-for-profit body, organization or association which has been properly constituted in accordance with the law of an EEA Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data (as envisaged in Article 80(1) of the GDPR).

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.

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 DPM 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 DPM.

Siemens has established a worldwide network of DPMs. On issuing the Declaration of Commitment to the BCR each participating company designates the competent DPM and sends the DPM's contact details to LC CO DP. The participating company shall notify LC CO DP without undue delay of any changes in the identity of the DPM.

The DPM 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 DPM reports on matters including specifically the degree of implementation of the BCR in the individual participating company. The DPM has the local 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 reporting major privacy issues to the CDPO), risk assessments and handling local complaints from data subjects.

The CDPO of Siemens AG reports once a year to the managing board of Siemens AG. In addition, the CDPO can inform the managing board of Siemens AG if any questions or problems arise during the performance of their duties.

The CDPO is the Chief Data Privacy Officer of Siemens AG and has been appointed as such through a managing board announcement which has been signed by the CEO. 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 on a global level, in particular through training measures and monitoring including incident management and risk assessments, and deals with supervisory authorities' investigations. As the head of such unit, the CDPO has the responsibility to monitor compliance with the BCR on a global level and is supported by further employees of such unit who are recruited by and report to him.

Accountability and other tools

All participating companies shall be responsible for and able to demonstrate compliance with the BCR. As part of this, they shall maintain a record of all processing activities carried out under these BCR in any capacity (controller or processor). The record shall include name and contact details of the participating company and its data protection officer / data privacy manager, purposes of processing, description of categories of data subjects and personal data, categories of recipients, transfers to third countries, envisaged time limits for erasure and general description of technical and organizational security measures. This record shall be made available to the supervisory authority on request.

Further, they shall carry out a data protection impact assessment (DPIA) for processing operations carried out under these BCR that are likely to result in a high risk to the rights and freedoms of a natural person, taking into account the nature, scope, context and purposes of the processing.

A DPIA is in particular required in the following cases:

- Systematic and extensive evaluation of personal aspects based on automated processing, including profiling, where decisions are made that produce legal or similarly significant effects concerning the data subject;
- Large-scale processing of special categories of personal data or personal data relating to criminal convictions and offences;
- Systematic monitoring of a publicly accessible area on a large scale.

The DPIA shall include:

- A systematic description of the envisaged processing operations and the purposes of the processing;
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- An assessment of the risks to the rights and freedoms of data subjects;
- The measures envisaged to address the identified risks, including safeguards and security measures.

Participating companies shall seek the advice of their DPM. The DPIA shall be carried out prior to the commencement of processing and reviewed where necessary to assess compliance with the DPIA, particularly when there are changes in the risk profile.

7.4 Non-compliance with these BCR

A 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 agreed to an effective Declaration of Commitment to the BCR.

The data importer shall promptly inform the data exporter if it is unable to comply with the BCR.

Where the data importer is in breach of or unable to comply with these BCR or ceases to be bound by them, the data exporter shall suspend the transfer.

The data importer shall, at the choice of data exporter, immediately return or delete the personal data and any copies of the data that have been transferred under the BCR in their entirety where:

- The data exporter has suspended the transfer and compliance with this BCR is not restored within a reasonable time and in any event within one month of suspension; or
- The data importer is in substantial or persistent breach of the BCR; or
- The data importer fails to comply with a binding decision of a competent court or competent supervisory authority regarding its obligations under the BCR.

The data importer shall certify the deletion of the data to the data exporter upon request.

Until the data is deleted or returned the data importer shall continue to ensure compliance with the BCR.

In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer shall warrant that it will continue to ensure compliance with the BCR and will only process the data to the extent and for as long as required under that local law.

7.5 Monitoring of compliance with BCR

Compliance with the BCR by the participating companies is subject to regular review primarily by the DPM appointed by executive management of the participating company. Executive management of the participating company supports the DPM 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 DPM 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 DPM in connection with the implementation of and compliance with the BCR in the participating company, either by requesting a written self-assessment by the DPM 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.

7.6 Notification and documentation of data breaches

In the event of a personal data breach, the participating company that has suffered the breach must promptly notify the CDPO at Siemens AG and the relevant DPM about the breach. If the participating company acts as a processor, it shall also inform the respective participating company acting as controller for the affected personal data.

In the event of a personal data breach the respective participating company shall notify the competent supervisory authority without undue delay (where feasible, not later than 72 hours) after becoming aware of the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the natural persons affected.

In case of a data breach which is likely to result in a high risk to the rights and freedoms of natural persons, the respective participating company will notify the data breach to the data subject without undue delay.

Any personal data breach (including the facts relating to the personal data breach, its effects, and the remedial action taken) shall be documented. This documentation shall be made available to the competent supervisory authority upon request.

7.7 Training

Siemens maintains a mandatory web-based training curriculum. Data protection training is one of the very few mandatory, appropriate and up-to-date trainings which needs to be taken by every employee (excluding factory workers without team responsibility). The training cycle period for data protection is two years and the content, the look & feel as well as the questions for passing the training differ from one training cycle to the other. The training covers, among others, procedures of managing requests for access to personal data by public authorities and other third parties.

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. In addition, Siemens offers voluntary and mandatory demand-based training measures that address new developments in data protection law and jurisprudence if necessary.

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.

7.8 Complaint process

Data subjects can contact the competent complaint handling department in Siemens AG (LC CO DP; for contact details and the various contact options, see Section 9) or the participating company's competent DPM (to be found in the Siemens Organisation), at any time, with complaints about a breach of the BCR by a participating company or with any questions.

Independently from this complaint mechanism, the data subject has always the right to (i) use the Siemens whistle blower hotline, the various contact forms. which are linked on the footer of every Siemens Internet webpage and (ii) address a complaint before a supervisory authority or to lodge a claim before the competent court, while such right does not depend on the data subject having used the complaint handling process beforehand. The use of the above mentioned contact options is encouraged but not mandatory for data subjects

The complaint shall be processed without undue delay and within one (1) month of receipt of the complaint; due to the complexity and number of requests 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 the Siemens group company, e.g. in case of a failure of the data subject to timely provide information that is reasonably necessary. If the data subject is not given a timely answer, the data subject has the right to escalate this to the Chief Data Privacy Officer of Siemens AG. The participating companies accept that data subjects may be represented by a not-for-profit body, organization or association which has been properly constituted in accordance with the law of an EEA Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data (as envisaged in Article 80(1) of the GDPR).

If the complaint is considered justified, LC CO DP or the participating company's competent DPM shall monitor implementation of the measures taken to remedy the complaint and, as necessary, advise on the appropriate measures to achieve compliance with the BCR. The data subject shall be informed about the result of the investigation and the resolution of the complaint.

If the complaint is rejected or the data subject is not satisfied with the reply, the data subject always has the right to address a complaint before a supervisory authority or to lodge a claim before the competent court.

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 competent supervisory authority of the country and to respect their opinions.

7.9 Data Privacy Audits

Alongside other existing internal audit and control systems in the Siemens group of companies, Siemens has established and carries out a data privacy audit program on a yearly basis – taking into account the risks posed by the processing activities - which covers different risk areas in the group of companies. Such audits are planned yearly in advance by the CDPO of Siemens AG together with the Siemens audit organization (C FA) which consists of several hundred experienced auditors with different fields of expertise. The persons in charge are guaranteed independence as to the performance of their duties related to these audits.

The CDPO of Siemens AG is entitled, in accordance with the Siemens audit charta, to request audits; the audits will be conducted by the Siemens audit organization with the support of the Siemens data protection organization (e.g. data protection subject matter experts). If necessary, a BCR audit can also be initiated by the Siemens internal audit department (CF A), by the Audit Committee of Siemens AG~~,~~ or by the executive management.

The yearly audit plans cover different topics related to people (training, behavior etc.), products and services and include all countries where Siemens is located. The audits cover all aspects of the BCR (for instance, applications, IT systems, databases that process personal data, or onward transfers, decisions taken as regards mandatory requirements under national laws that conflict with the BCR, review of the contractual terms used for the transfers out of the group to controllers or processors of data).

Each audit ends with a detailed audit report with clear findings and clear management action items to be implemented within a prescribed timeline. CF A and the CDPO will monitor that the necessary corrective actions are implemented.

The CDPO, the managing board of Siemens AG and the responsible management of the audited department / entity as well as further relevant management members receive the full BCR audit report.

The results of the audit are made available to the relevant competent supervisory authority (i.e. the authorities of those EEA countries from which personal data have been transferred to the audited company) upon request.

7.10 BCR updating & change management

Siemens shall continuously update and maintain these BCR to reflect the current legal requirements, the Siemens group structure or requirements imposed by the competent supervisory authorities. Siemens therefore reserves the right to change and/or update these BCR at any time. If a modification to the BCR could potentially be detrimental to the level of protection offered by the BCR or significantly affect them (e.g., changes to the binding nature, change of the liable participating company as determined in section 8. of these BCR), it shall be communicated in advance to the relevant supervisory authorities, along with a brief explanation of the reasons for the update. In such cases, the supervisory authorities will also assess whether the changes necessitate a new approval All other changes to the BCR are possible without new approval by the competent supervisory authorities.

In any case changes of the BCR shall be reported to all participating companies without undue delay.

Data subjects are informed of updates to the BCR on the Siemens internet pages, currently at http://www.siemens.com as follows:

- Any updated version of the BCR is uploaded to the internet pages without undue delay; and
- The updated version will contain a summary of all updates affecting elements of the BCR which are enforceable by data subjects.

LC CO DP maintains a list of all changes/updates to the BCR since the BCR came into force. LC CO DP also maintains a regularly updated list of all participating companies which are effectively bound by the BCR (status overview, see Appendix 2, cf. Section 7.1.1), and provides the necessary information to data subjects and, upon request, to competent supervisory authorities. 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 CO DP.

LC CO DP notifies the competent supervisory 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. LC CO DP also notifies the competent supervisory authority at least once a year that no changes to these BCR occurred since the last update.

7.11 Mutual assistance and cooperation with the supervisory 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 noncompliance with the BCR.

Siemens AG and the participating companies further undertake to trustfully cooperate with the competent supervisory authorities in the context of implementation of the BCR. They will take into account the competent supervisory authorities' advice and abide by their decisions on any issue related to these BCR. They will answer BCR-related requests from the supervisory authority within an appropriate timeframe and in an appropriate fashion and will follow the advice and decisions of the competent supervisory authority with regard to implementation of the BCR. This cooperation with the competent supervisory authorities includes accepting audits and inspections (including on-site visits where necessary), as well as providing the competent supervisory authorities with any requested information regarding processing operations covered by the BCR.

Any dispute related to the competent supervisory authority's exercise of supervision of compliance with the BCR will be resolved by the courts of the member state of that supervisory authority, in accordance with that member state's procedural law. The participating companies agree to submit themselves to the jurisdiction of these courts for such disputes. Where a data protection impact assessment under Section 7.3 above 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.

7.12 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 local law. Each participating company shall check for itself (e.g. through its DPM or by the Legal department), whether such local law (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 and the legitimacy of processing is judged on their basis.

In the event that obligations arising from the applicable local law are in conflict with the BCR, the participating company shall inform LC CO DP without undue delay. LC CO DP will record the reported conflict in the status overview (cf. Section 7.1.1). LC CO 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 CO DP will also inform the competent supervisory authority of the regulatory conflict and, together with the supervisory authority and the participating company, will seek a practical solution that comes as close as possible to the principles in the GDPR. Participating companies use these BCR as a tool for transfers only if they have assessed that the law and practices in the third country of destination applicable to the processing of personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, do not prevent it from fulfilling its obligations under these BCR.

This is based on the understanding that laws and practices, that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society to safeguard an objective mentioned below, are not in contradiction with the BCR. These objectives are:

(a) national security;
(b) national defense;
(c) public security;
(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
(e) the protection of other important objectives of general public interest of the European Union or of one of its member states, in particular an important economic or financial interest of the Union or of a member state, such as in the monetary, budgetary, fiscal, public health or social security fields;
(f) the protection of the independence of the judiciary and the protection of judicial proceedings;
(g) the prevention, detection, investigation and prosecution of infringements of the professional rules of regulated professions;
(h) control, monitoring and regulatory functions permanently or temporarily connected with the exercise of official authority for the purposes referred to in subparagraphs (a) to (e) and (g);
(i) the protection of the data subject or the rights and freedoms of others;
(j) the enforcement of civil claims.

In assessing these laws and practices of the third country which may affect the respect of the commitments contained in the BCR, the participating companies shall take into consideration the following elements:

- The specific circumstances of the transfers or set of transfers, and of any envisaged onward transfers within the same third country or to another third country. This includes:
    - The purpose for which the personal data is transferred and processed
    - The types of entities involved in the processing
    - The economic sector in which the transfer or set of transfer occurs
    - The categories and format of the personal data transferred
    - The location where the processing and storage of personal data occurs
    - The transmission channels used

- The laws and practices of the third country of destination relevant in light of the circumstances of the transfer, including those requiring the disclosure of data to public authorities or authorising access by such authorities, and those providing for access to these data during the transit between the country of the data exporter and the country of the data importer, as well as the applicable limitations and safeguards
- Any relevant contractual, technical, or organisational safeguards implemented to supplement the safeguards under the BCR, including measures applied during the transmission and the processing of the personal data in the destination country

In case any additional safeguards beyond those envisaged under these BCR are put in place, the Chief Data Privacy Officer at Siemens AG shall be informed and involved in such assessment.

Participating companies are obligated to appropriately document any assessments conducted, as well as the supplementary measures selected and implemented. Such documentation must be made available to the competent supervisory authorities upon request.

If a data importer has reasons to believe or has become subject to laws or practices that prevent it from fulfilling its obligations under these BCR, including following a change in the laws in the third country or a measure (such as a disclosure request), it shall promptly notify the data exporter as well as the Chief Data Privacy Officer at Siemens AG.

Upon verification of such notification, the data exporter, along with the CDPO at Siemens AG, shall commit to promptly identify supplementary measures (e.g., technical or organizational measures to ensure security and confidentiality) to be adopted by data exporter and/or data importer, in order to enable them to fulfil their obligations under these BCR. The same applies if a data exporter has reasons to believe that a data importer can no longer fulfil its obligations under this BCR.

If the data exporter and the CDPO at Siemens AG determines that the BCR, even with supplementary measures, cannot be complied with for a specific transfer or set of transfers, or if instructed by the competent supervisory authorities, it shall suspend the transfer or set of transfers in question, as well as any other transfers where the same assessment and reasoning would lead to a similar outcome, until compliance is restored or the transfer is terminated. Following such a suspension, the data exporter must terminate the transfer or set of transfers if the BCR cannot be complied with and compliance is not restored within one month of the suspension. In such a case, any personal data transferred prior to the suspension, along with any copies, should be either returned to the data exporter or destroyed entirely, at the discretion of the data exporter.

The CDPO at Siemens AG will inform all other participating companies about the assessment conducted and its results. This ensures that the identified supplementary measures will be implemented if the same type of transfers is carried out by any other participating company. Additionally, if effective supplementary measures cannot be established, the transfers in question will be suspended or terminated

Data exporters must monitor, on an ongoing basis, and where appropriate in collaboration with data exporters developments in the third countries to which they have transferred personal data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

7.13 Disclosure of Personal Data to a Public Authority

The data importer will promptly notify the data exporter and, if feasible, the data subject (if necessary, with the help of the data exporter) if it:

- receives a legally binding request from a public authority under the laws of the country of destination or another third country for the disclosure of personal data transferred pursuant to the BCR. The notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided

- becomes aware of any direct access by public authorities to personal data transferred pursuant to the BCR in accordance with the laws of the country of destination. The notification shall include all information available to the data importing participating company.

In case of prohibition from notifying the data exporter and/or the data subject, the data importer will use its best efforts to obtain a waiver of such prohibition, with a view to communicate as much information as possible and as soon as possible and will document its best efforts in order to be able to demonstrate them upon request of the data exporter.

The data importer will provide the data exporter, at regular intervals, with as much relevant information as possible on the requests received (in particular number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenge, etc.) If the data importer is or becomes partially or completely prohibited from providing the data exporter with aforementioned information, it will, without undue delay, inform the data exporter accordingly.

The importer will preserve the abovementioned information for as long as the personal data are subject to the safeguards provided by the BCR and shall make it available to the competent supervisory authorities upon request.

The data importer will review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and principles of international comity.
Under the same conditions the data importer will pursue possibilities of appeal.
When challenging a request, the data importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the personal data requested until to do so under the applicable procedural rules.

The data importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It will also make it available to the competent supervisory authorities upon request.

When responding to a request for disclosure, data importer will provide only the minimum amount of information permissible, based on a reasonable interpretation of the request.

In any case the participating company shall take the necessary measures that any transfer of personal data to any public authority will not be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society. Transfers that are massive, disproportionate or indiscriminate constitute a violation of these BCR.

These provisions are without prejudice to the obligation of the data importer to inform the data exporter, if it has reason to believe that is not able to comply with the BCR-Cs, as stipulated under Sections 7.4 and 7.12.

8 Liability

Siemens AG assumes responsibility and liability for non-compliance with the BCR by participating companies established outside the EEA and agrees to take the necessary actions to remedy breaches of the BCR of such companies. 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 shall be liable to pay compensation for material and non-material damages resulting from a breach of these BCR by a participating company, provided that the data subject establishes that:

- a breach of these BCR has likely occurred and
- the damage is likely causally linked to such breach.

Siemens AG may be exonerated from liability by demonstrating either that:

- no breach of these BCR occurred; or
- the participating company was not responsible for the breach (i.e., the breach occurred without fault, intention or negligence on the part of the participating company).

9 Contact

Data subjects can contact the DPM of the relevant participating company or the global data privacy function of Siemens AG through this physical address or – preferably - by e-mail:

Siemens AG
LC CO DP
Werner-von-Siemens Str. 1
D-80333 Munich
E-mail: datenschutz@siemens.com or dataprotection@siemens.com
Siemens Intranet website: https://intranetsiemens.com/dp
Internet: http://www.siemens.com/privacy

Appendices

Appendix 1: Declaration of Commitment for Group Companies
Appendix 2: List of Participating Companies
Appendix 3: Material Scope of the Binding Corporate Rules / Categories of data subjects, personal data, and processing activities