D. Data Privacy

Data privacy laws are being introduced for the first time or else are being tightened up, not only in the EU in the form of the directly applicable General Data Protection Regulation adopted on April 14, 2016, but also in many other countries. At the same time, supervisory authorities are being put in place and given more rights than ever. This is accompanied by greater media coverage and an increase in the number of public tenders which request data privacy solutions. This change has a tangible impact for Siemens AG and Siemens Affiliated Companies located within or outside the EU and requires adapting Siemens' data privacy related processes to the applicable legal framework.

The "LC CO Data Deletion and Retention Policy" applicable for the LC Organization can be found here.

Data Privacy in a nutshell

- Personal data means any information that relates to an identified or identifiable natural person.
- Processing of personal data requires a legitimate legal basis. Examples of legal bases include contractual relationships, legitimate interests of the company or consent by the data subject.
- Any employee who becomes aware of a data breach must take immediate action and inform the Data Privacy Organization as described in the Data Privacy Incident Management Process.
- Applicable data privacy laws often require companies to maintain a detailed record of all processing activities of personal information. Any processing of personal information in an application or system must be documented within the Siemens CDP Center by the respective process owner with the support of IT.
- Data Privacy laws require appropriate data processing agreements that contain requirements for service providers which provide data processing services (such as hosting or similar solutions).

1. Responsibility

The first key principle - Data privacy compliance as the responsibility of each Siemens employee

Complying with the law is a fundamental principle for Siemens. All Siemens employees are required to perform their daily tasks in accordance with applicable laws and regulations, including laws and regulations on data privacy (for example sections H7 of the Business Conduct Guidelines). This chapter therefore provides support to help employees from the respective target groups to comply with this principle in their daily work. Further directives are included in SC 216 "Binding Corporate Rules (BCR) and Intercompany Agreement (ICA) for the Protection of Personal Data".

The second key principle - Collaboration between the stakeholders identified and the Data Privacy Organization

Data privacy compliance falls under the responsibility of the Controller[1] and the Processor[2]. Collaboration between Siemens entities is a key driver in Siemens' compliance with applicable laws and regulations. In addition, the Siemens Data Privacy Organization[3] supports stakeholders in the implementation of their respective tasks defined herein and acts as an intermediary between the stakeholders and external parties (e.g. supervisory authorities, data subjects, service providers and third parties).

An overview of the Siemens Data Privacy Organization including data privacy contacts in Siemens entities can be found in the Intranet.

2. Tasks – Action Items

2.1. Incident Handling / Data Breaches

Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data may trigger notification requirements to authorities and data subjects.

For this purpose, any employee who becomes aware of such a breach must take immediate action in line with the Data Privacy Incident Management Guidance and inform the Data Privacy Organization, if possible by using the data breach report form. Any communication with supervisory authorities and data subjects concerned needs to be coordinated with the Data Privacy Organization.

2.2. Register of processing activities

Applicable data privacy laws (such as the EU data protection regulation) often require companies to maintain a detailed record of all processing activities and to conduct a privacy impact assessment for certain processing operations. Such processing activities shall be documented within the Siemens CDP Center[4] by the respective Process Owner[5] with the support of the IT (responsible for describing the technical and organizational measures and the possible engagement of further sub-processors).

---

[1] Means the company which, alone or jointly with others, determines the purposes and means of the processing of personal data; e.g. the employer regularly acts as Controller for the personal data of its employees.
[2] Means a legal person which processes Personal Data on behalf of a Controller. A company regularly qualifies as Processor if it acts as external or internal IT service provider (such as the hosting of applications or the provision of IT support services).
[3] A local contact within the Data Privacy Organization can be identified here. The responsibilities within the Siemens Data Privacy Organization are described in Roles & Responsibilities document.
[4] Means the electronic application register of Siemens, available here.

Documentation in the CDP Center is mandatory if:

- the Controller is situated in a country in which an application register is required by law, or
- a Siemens entity acts as Processor for a Controller located in a country with this type of documentation requirement.

Even in other cases, a notification in the CDP Center is highly recommended in order to obtain a comprehensive overview of data privacy risks within Siemens.

2.3. Data processing agreements

EU and other data privacy laws impose contractual requirements for the provision of processing services (such as SaaS, hosting or similar solutions). These requirements apply in particular to Sales, Procurement, LC and IT.
Such requirements include the obligation to

- carefully select a provider, taking into account the adequacy of the technical and organizational measures implemented and
- agree on certain contract terms for the data processing agreement (by including data processing terms with certain mandatory content).

Siemens AG or an Affiliated Company is directly bound by the statutory requirement to enter into such data processing terms even if it only acts as provider (i.e. a Processor) for customers. In regard to external customer / provider facing agreements there are sample data processing terms for "Siemens acting as Customer" and "Siemens acting as Provider" available on the intranet.

Furthermore there is an existing internal data processing agreement between all Siemens Group Companies (SC 216 "Binding Corporate Rules and Intercompany Agreement for the Protection of Personal Data").

2.4. Data privacy audits of service providers

If the provision of processing services (such as SaaS, hosting or similar solutions) involves personal data and such services are purchased from an external IT service provider, the technical and organizational measures implemented by this service provider must be audited on a regular basis by the respective Process Owner. Additional stakeholders are IT.

The intervals of such audits depend on the criticality of the personal data processed; in the case of IT applications and services containing sensitive HR data, audits should be conducted at least on an annual basis. For this purpose it is recommended that the Process Owner requests applicable and current audit

[5] Means the organizational unit at Siemens AG or an Affiliated Company that has the business responsibility for a data processing activity, such as an IT application or service.

reports and certifications from the service provider and retains a copy thereof for documentation purposes. For low risk applications the audit may be based on self-assessments.

2.5. Rights of data subjects (information rights)

Data privacy laws often grant information and access rights to individuals. The stakeholder involved is the Process Owner. Information on processing personal data shall be provided at the time when personal data is obtained (e.g. through a privacy notice in the application).

Access rights to personal data processed (including a copy thereof) shall also be considered, depending on the applicable laws. The Siemens HR Privacy Notice describes the processing of personal data of the Siemens employees.

2.6. Privacy in the product business

In the development of Siemens products, solutions and services the principles of "data privacy by design" (and by default) shall be taken into account throughout the development process. Concerned stakeholder are PSS Officers[6], PSS Experts[7], Developer of products and services and CT.

The Circular No. 232 "Product & Solution Security" requires that Siemens complies with legal and regulatory requirements, including the privacy by design and by default principle. These principles require Siemens to consider data privacy during the whole lifecycle of a product, solution and service in order to

- implement measures and product components which meet the data protection principles within products, solutions and services (Privacy by Design), and
- apply privacy friendly settings automatically, without requiring the user to make manual changes to the privacy settings ("Privacy by Default").

For further details, the Privacy by Design Checklist for Product Business and other material (including for customer requests), please refer to the Intranet.

3. Training and supporting material

- Data Privacy Management System
- Siemens Circular 216 "Binding Corporate Rules (BCR) and Intercompany Agreement (ICA) for the Protection of Personal Data"

[6] Means Product & Solution Security Officers appointed in accordance with Circular No. 232 "Product & Solution Security".
[7] Means Product & Solution Security Experts appointed in accordance with Circular No. 232 "Product & Solution Security".

- Siemens CDP Center
- Siemens Circular No. 232 “Product & Solution Security”
- Data Privacy WBT (mandatory for specific job families)
- Interactive subway plan for the General Data Protection Regulation (GDPR)
- Scribble Video

4. History of changes

Date	Author	Major changes of binding content
January 1, 2019	Achim Köhler Dr. Achim Kessler	First release through the Compliance Handbook based on Siemens Circular SC No. 226 “Global Compliance”, Appendix 14.

5. Contacts

Compliance Officer

The Compliance Officer responsible for your unit can be found through the following link.

Corporate Governance Owner

The contact persons for data privacy are:

Achim Köhler (Chief Data Privacy Officer Siemens AG)

Dr. Axel Kessler (Head of Data Privacy Legal)