Data Protection FAQs

1) ***Do you have a Data Privacy Organization?*** Siemens has created a Data Privacy Organization to ensure the development of tools, processes, and polices, which safeguard the protection of personal data. The Data Privacy Organization covers all of Siemens, from business product development to administrative activities.

2) ***How do you comply with the various Data Protection requirements (e.g., General Data Protection Regulation and California Consumer Privacy Act)?*** To ensure trust of customers, business partners and employees, Siemens has developed comprehensive data privacy policies, tools, and guidelines to go beyond what is required by law.

3) ***Do your employees receive Data Privacy Training?*** The sustainable implementation of data protection requirements must involve our employees from all departments. For this reason, internal regulations, such as our Business Conduct Guidelines, require every employee to comply with our data protection requirements. Siemens employees receive both overview and detailed training in the handling of personal data. In addition, employees have access to multiple online resources and tools to assist with their data protection requirements.

4) ***Do you have an incident management system?*** Siemens has developed and implemented a global Data Privacy Incident Process that ensures central reporting channels and the involvement of relevant stakeholders.

5) ***Can you identify the non-DISW sub processors and Central Services on your list which are relevant for the offerings I am interested in?*** Please review of list of our sub processors.

6) ***How does SISW ensure that personal information is appropriately protected, especially against government access?*** Siemens scrutinizes all data requests to ensure they are appropriate and valid. We will not disclose data to a 3rd party including government entities unless required by law or given permission by the data owner.

7) **What does Privacy by Design mean to Siemens?** For Siemens, Privacy by Design means that legality, transparency, informational self-determination, data economy and data security are already taken into account when developing our Siemens products and services. Privacy by Design is therefore firmly integrated into our product development processes. We consider Choice and Consent, Data minimization, Access, Security, Data Accuracy and quality and Access when developing our products and services.

8) **Does Siemens conduct Privacy Impact Assessments?** Siemens utilizes Privacy Impact Assessments to identify and manage the privacy risks associated from new products and services as required under GDPR Art. 35(3).

9) **Does Siemens have a policy to ensure that persons authorized to access and/or process personal data are held to an appropriate obligation of confidentiality*?*** All Siemens employees are bound to comply with the Siemens Business Conduct Guidelines, which are a binding code of conduct. The Business Conduct Guidelines state: "All of us who handle the personal data of employees, customers, or third-parties bear a high level of responsibility". Please visit our Business Conduct Guidelines for more information.

10) **Do you have a policy that limits the access to customer personal data?** Siemens has developed their Binding Corporate Rules which allow multinational companies to make EU data protection law the standard for intra-group transfers of personal data across borders. In 2014, Siemens was one of the first companies to introduce Binding Corporate Rules (BCRs) to ensure this high level of data protection for intra-group exchange of personal data across international borders and form an essential part of the international business activities. As part of our BCRs, a Confidentiality of data processing rule has been established which limits access rights to data. Please review section 3.10 of our Third Party Rights of our Binding Corporate Rules for more information.