Siemens Gamesa Renewable Energy

Business Partner Privacy Notice

As a current, past or future customer, supplier, vendor, partner, intermediaries, reseller, consortium partners and land developers (herein after referred to as "**Business Partner**") of Siemens Gamesa Renewable Energy (SGRE), there are some practices in relation to the personal data of contact persons (herein after referred to as "**Business Partner Contact**") that affects you. Therefore, SGRE prepared this Privacy Notice to describe what the company does with the personal data it collects, and how it protects it from breaches. This document also summarizes the rights of Business Partner in regards to this data. If required, SGRE may also:

a) Provide additional information on the specific processing activity surrounding the collected data. Depending on the application, details on why and how the personal data is processed could be given;

b) Inform Business Partner about the different privacy notices which affect different processing activities – Some global tools may have their own privacy notices in addition to or separate from this notice.

Within this document, the following topics are discussed:

1. Purpose and categories of personal data processed
2. Legal basis for processing
3. Transfer and disclosure of personal data
4. Retention of personal data
5. Withdrawal of consent
6. Business Partner rights
7. SGRE data protection team.

Processing of personal data is an integral part of our business; therefore, SGRE takes data protection seriously, and processes personal data in such a way that is in compliance with the applicable laws on data protection.

Data Protection

Purpose and Legal Basis for Processing

1. Purpose and categories of personal data processed:

For the purpose of conducting business with SGRE, the personal data is processed for:

a) Communication – By responding to inquiries or requests from Business Partner about products, services and projects of SGRE;
b) Contract planning, management and performance – facilitating transactions and orders of products and services, auditing, billing, deliveries, servicing etc.;
c) Organizational and Administration – Planning of workflows, processes, surveys, marketing campaigns, market analysis, promotional events etc.;
d) Accounting for and protecting the security of SGRE products, services and websites – Physical and IT assets (e.g., fraud prevention or other illegal activities), detecting security threats, fraud or other criminal or malicious activities;
e) Compliance purposes – Business Partner auditing, record keeping obligations, export control and customs, compliance screening obligations (to prevent money laundering and other white-collar crimes), and Siemens Gamesa policies or industry standards;
f) Dispute resolution – Enforcing our contractual agreements and to establish, exercise or defend legal claims.

Personal data held by SGRE consist primarily of information willfully given by Business Partner, or generated as a result of contractual relationship with SGRE and consist of the following categories:

a) Contact information – full name, work address, work telephone and fax number, work email address;
b) Payment data – e.g, credit/debit cards, bank details, security code numbers, and other information required for billing and fraud prevention;
c) Further information necessarily processed in a project or contractual relationship with Siemens Gamesa or voluntarily provided by the Business Partner Contact, such as orders placed, payments made, requests, and project milestones;
d) Data log from the use of SGRE IT assets – e.g., log files containing device identifiers, browser type, etc
e) Publicly available information – e.g., information available from integrity data bases and credit agencies; and
f) If legally required for Business Partner compliance screening – e.g. date of birth, ID numbers, identity cards, CVs, information about relevant and significant litigation or other legal proceedings against Business Partners.

2. Legal basis for processing:

Processing of personal data by SGRE is necessary because of:

a) SGRE exercising its rights and performing its obligations and/or in connection with any contract we make with Business Partner (Article 6 (1)(b) General Data Protection Regulation - GDPR);
b) Compliance with SGRE's legal obligations (Article 6 (1)(c) GDPR); and/or
c) Legitimate interests pursued by SGRE (Article 6 (1) (f) GDPR).

In some cases, SGRE may ask for consent before using the personal data of Business Partner. The legal basis for such cases is in compliance with Article 6 (1) (a) of the GDPR.

Data Protection

Data Transfer, Consent and Business Partner Rights

3. Transfer and disclosure of personal data:

Personal data may be transferred by SGRE to:

a) Other SGRE companies as a result of Business Partner contractual relationship with SGRE;
b) Other third parties – e.g., to regulators or attorneys, SGRE consultants, law enforcement authority, etc. if necessary to comply with the law or for the establishment, exercise or defense of legal claims;
c) SGRE IT providers (those who process such data only for such services contractually bound to act in compliance with applicable data protection law), such as hosting or IT maintenance service providers.

Some recipients to whom SGRE transfers the personal data may be located in countries whose applicable laws regarding data protection may not offer the same level of data protection as the laws in Business Partner's home country. In such cases, there are appropriate safeguards put in place by SGRE for the protection of the personal data. For instance:

a) Personal data is shared with SGRE companies in such countries only if they have implemented SGRE's Binding Corporate Rules (BCR) for the protection of personal data;
b) In cases where personal data is to be transferred to external recipients, such a transfer occurs only if the recipient has:

I. Entered into Data Protection Agreements;
II. Entered into EU Standard Contractual Clauses with SGRE;
III. Implemented BCR in its organization; or
IV. In the case of US recipients, has been certified under the Privacy Shield.

4. Retention of personal data:

Personal data will be erased if the retention of such data is no longer necessary for:

a) The purpose for which it was collected; or
b) Compliance with legal obligations (such as tax or commercial law); or
c) Unless otherwise indicated (not to erase such data) at the time of the collection of personal data (which Business Partner Contact would have agreed to).

5. Withdrawal of consent:

In case consent is given for the processing of the personal data, it can be withdrawn at anytime. The lawfulness of processing due to a prior consent is not affected by the withdrawal of this consent. However, SGRE may only further process the personal data where there is another legal ground for the processing.

6. Business Partner rights:

As an entity based in the European Economic Area, Business Partners are entitled to:

a) Procuring information regarding the processing of the personal data, and if applicable access to the personal data, as well as data portability;
b) Requesting the update of old or inaccurate personal data;
c) Requesting that the personal data be erased;
d) Requesting a restriction on the processing of the personal data, as well as objecting "on grounds relating to Business Partner's particular situation," to processing of the personal data.

7. SGRE data protection contacts:

The data protection team at SGRE provides support with any data privacy related questions, comments or concerns. Please find out more information by contacting dataprotection@siemensgamesa.com or by visiting www.siemensgamesa.com