Personal Data Privacy Policy

February 13, 2019

The Board of Directors of Avangrid, Inc. ("AVANGRID") oversees the management of AVANGRID and its business with a view to enhance the long-term value of AVANGRID for its shareholders. The Board of Directors of AVANGRID (the "Board of Directors") has adopted this Personal Data Privacy Policy (this "Policy") to assist in exercising its responsibilities to AVANGRID and its shareholders. This Policy is subject to periodic review and modification by the Board of Directors from time to time. This Policy and AVANGRID's certificate of incorporation, by-laws, corporate governance guidelines and other policies pertaining to corporate governance and regulatory compliance, risk, sustainable development, and social responsibility (collectively, the "Corporate Governance System") form the framework of governance of AVANGRID and its subsidiaries (collectively, the "AVANGRID Group"). AVANGRID's Corporate Governance System is inspired by and based on a commitment to ethical principles, transparency and leadership in the application of best practices in good governance and is designed to be a working structure for principled actions, effective decision-making and appropriate monitoring of both compliance and performance.

1. Purpose

In the context of the AVANGRID Group's business activities, the AVANGRID Group processes Personally Identifiable Information ("PII") from different groups of stakeholders such as customers, employees, and suppliers.[1] AVANGRID recognizes the importance of proper use and handling of the PII acquired, used, stored, destroyed, or disclosed in the course of the AVANGRID Group's business activities. This Policy sets forth the general principles that will guide the processing of PII by the AVANGRID Group and the basic framework for the distribution of privacy compliance related responsibilities within the different AVANGRID Group divisions. This Policy does not, and is not intended to, describe the specific privacy practices of the AVANGRID Group, but sets forth the general principles that guide the AVANGRID Group's approach towards privacy compliance. This Policy is not, and should not be construed as, a privacy notice, statement, or disclosure. This Policy contributes to the achievement of goal eight (Decent Work and Economic Growth) and goal sixteen (Peace, Justice and Strong Institutions) of the Sustainable Development Goals (SDGs) adopted by the member states of the United Nations.

[1] For the purposes of this policy:
"Personally Identifiable Information" (PII) is any information about an individual, including, without limitation, customers and employees, maintained by AVANGRID, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, personal electronic mail address, internet identification name, network password or internet password; or (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
"Sensitive Personally Identifiable Information" (SPII) is a subset of PII which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. SPII includes:

- Social Security Number (SS#)
- An individual's first and last name, first initial and last name, address OR phone number, in combination with ANY of the following:
  a. The individual's driver license number or other government-issued identification card number
  b. The individual's Tax ID number
  c. The individual's financial account number or credit or debit card number (with or without any required PIN, security code, password or access code) that would permit access to the individual's financial account
  d. Information regarding the individual's medical history, mental or physical condition, medical treatment or diagnosis by a health care professional, or payment for healthcare
  e. The individual's health insurance policy number or subscriber information number (in combination with any required PIN, security code, password or access code), any unique identifier used by a health insurer to identify the individual, or any information if an individual's insurance application and claims history, including any appeals records
  f. The individual's date of birth, place of birth and/or mother's maiden name
  g. The individual's passport number or an alien registration number
  h. The individual's unique biometric data such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data
- PII, which when combined would permit access to the above mentioned SPII.

2. Principles

AVANGRID Group companies shall comply with all applicable privacy laws and regulations in relation to the processing of PII. In addition, the AVANGRID Group shall consider the following general principles when processing PII:

a) Management. Define, document, communicate, and assign accountability for privacy practices.

b) Notice and Purpose Specification. When required by applicable law or otherwise considered appropriate by the AVANGRID Group, provide notice about privacy practices, including identifying the purposes for which PII is collected, used, retained, and disclosed.

c) Choice and consent. When required by applicable law or otherwise considered appropriate by the AVANGRID Group, describe the choices available to stakeholders and obtain implicit or explicit consent with respect to the collection, use, and disclosure of PII.

d) Collection Limitation. When required by applicable law or otherwise considered appropriate by the AVANGRID Group, limit the collection of PII to information needed for legitimate business needs and purposes and any other purposes that may be specified in a privacy notice. If stakeholders have been provided with a privacy notice identifying the purposes for which specific PII is collected, the AVANGRID Group shall only collect the specified PII for purposes that are consistent with the privacy notice.

e) Openness. The AVANGRID Group shall strive to be transparent about its practices with respect to the processing of PII.

f) Use, retention, and disposal. When required by applicable law or otherwise considered appropriate by the AVANGRID Group, limit the use of PII to legitimate business needs and purposes and any other purposes identified in any applicable privacy notice. When appropriate, the AVANGRID Group shall strive to retain PII for only as long as necessary to fulfil legitimate business needs or stated purposes or as required by law or regulations, and thereafter appropriately dispose of such information.

g) Access. When required by applicable law or otherwise indicated in any applicable privacy notice, provide stakeholders with appropriate access to their PII for review and verification.

h) User Limitation and Disclosure to third parties. AVANGRID Group employees' right to access PII shall appropriately account for whether the employee "needs to know" and/or "needs to have" access to the PII to fulfil job responsibilities.

The AVANGRID Group may disclose PII to third parties, including, without limitation, to (i) affiliates, (ii) contractors, service providers, and other third parties used to support the AVANGRID Group's business, or (iii) any successor or assignee. As appropriate, privacy notices provided by the AVANGRID Group shall strive to describe the type of third parties that could be given access to specific PII and the circumstances thereof. When contracting with third parties that may access PII, the AVANGRID Group shall take appropriate measures to assess, monitor and control the risks associated with the processing of PII by such third party.

i) Security for privacy. The AVANGRID Group shall have in place appropriate technical and organizational security measures that aim to protect PII against unauthorized access or acquisition. In the event of a data security breach, the AVANGRID Group shall take appropriate steps to comply with applicable breach notification requirements.

j) Data Quality. When required by applicable law or otherwise considered appropriate by the AVANGRID Group, take reasonable steps to maintain accurate and relevant and, where necessary, up-to-date PII.

k) Monitoring and enforcement. When required by applicable law or otherwise considered appropriate by the AVANGRID Group, regularly monitor compliance with privacy procedures and practices.

As feasible and appropriate, the general principles set forth in this Policy shall also be considered when developing and implementing internal procedures and rules and when designing and implementing systems containing PII.

3. Organization

AVANGRID's Corporate Security division shall be responsible for (i) supervising the implementation of this Policy by the AVANGRID Group, (ii) developing and maintaining, with the support of AVANGRID's Legal Services division, appropriate privacy procedures, rules and practices, and (ii) monitoring compliance by the AVANGRID Group of this Policy and any applicable privacy procedures, rules and practices. AVANGRID's Legal Services division shall be responsible for monitoring material developments concerning privacy laws and regulations, as well as informing AVANGRID's Corporate Security division of such material developments. AVANGRID's IT division shall be responsible for implementing appropriate information technology controls and developments.

As appropriate, the business and corporate function divisions of the AVANGRID Group shall identify data owners and shall strive to process PII in accordance with the principles set forth in this Policy and any applicable privacy procedures, rules and practices. The business and corporate function divisions that regularly process PII shall designate a coordinator for data privacy related purposes that shall be responsible for supervising compliance with this Policy and any applicable privacy procedures, rules and practices within such division and coordinating privacy related actions with AVANGRID's Corporate Security division.

Members of AVANGRID's Corporate Security division participates in the Iberdrola group Cybersecurity Committee, which assists with coordination across the Iberdrola group and the implementation of best practices in personal data protection and risk management.

This basic framework for the distribution of privacy compliance related responsibilities within the different AVANGRID Group divisions may be further developed or supplemented by other internal frameworks, procedures, or rules.