Personal Data Privacy Policy

October 15, 2025

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. Avangrid is a wholly owned subsidiary of Iberdrola, S.A. and a member of the group of companies controlled by Iberdrola, S.A. (the "Iberdrola Group"). The Board of Directors of Avangrid (the "Board of Directors") has approved this *Personal Data Privacy Policy* (this "Policy") to assist in exercising its responsibilities to Avangrid and its Stakeholders (as defined in Avangrid's *Stakeholder Engagement Policy*). 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 "Governance and Sustainability System") form the framework of governance of Avangrid and its subsidiaries (collectively, the "Avangrid Group"). Avangrid's Governance and Sustainability 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. This Policy aligns with and further develops the principles contained in the *Personal Data Protection Policy*, the *Purpose and Values of the Iberdrola Group*, and the *Ethical and Basic Principles of Governance and Sustainability of the Iberdrola Group* approved by the Board of Directors of Iberdrola, S.A. from time to time.

1. Scope of Application

This Policy applies to the Avangrid Group and reflects the basic principles established at the Iberdrola Group level and that, in the area of personal data protection, complement those contained in the *Ethical and Basic Principles of Governance and Sustainability of the Iberdrola Group* and informs the conduct and standards-setting implemented by the other companies of the Avangrid Group in this area in the exercise of their powers and in accordance with their autonomy.

For companies that do not form part of the Avangrid Group but in which Avangrid holds an interest, as well as for joint ventures, temporary joint ventures, and other entities in which it assumes management, Avangrid shall also promote the alignment of its regulations with the basic principles regarding personal data protection contained in this Policy.

2. 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. 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.

3. Main Principles of Conduct

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) Legal and Lawful. The processing of personal data shall be legitimate, lawful, and fair, in accordance with applicable laws and regulations. In this sense, personal data will be collected for one or more specific and legitimate purposes in accordance with applicable laws and regulations.

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

c) 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.

d) 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.

e) Minimization. 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.

f) Transparency. The Avangrid Group shall be transparent about its practices with respect to the processing of PII.

g) 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 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 securely dispose of such information.

h) Rights of Data Subjects. When required by applicable law or otherwise indicated in any applicable privacy notice, allow Stakeholders to exercise the rights of access, correction, deletion, restriction of processing, portability and appeal that are applicable in each jurisdiction with respect to their PII, establishing for such purpose such internal procedures as may be necessary to satisfy the legal requirements applicable in each case.

i) 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, (iii) any successor or assignee, or (iv) as required by applicable law or mandate. When required by applicable law or otherwise considered appropriate by the Avangrid Group, privacy notices provided by the Avangrid Group shall 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.

j) 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 and reporting requirements.

k) Data Quality. Take reasonable steps to maintain accurate and relevant and, where necessary, up-to-date PII.

l) Monitoring and Enforcement. Regularly monitor compliance with privacy procedures and practices.

m) Data Inventory and Mapping. The Avangrid Group shall maintain a current inventory of systems and processes that collect, store, process, or transmit PII. This inventory shall include data flow mapping to understand how PII moves across internal systems and third-party environments. The inventory shall be reviewed periodically and updated as necessary to reflect changes in business operations or technology.

n) Privacy Risk Assessment. The Avangrid Group shall conduct Privacy Impact Assessments (PIAs) or similar evaluations when implementing new systems, processes, or technologies that involve processing of PII. These assessments shall identify potential privacy risks and recommend mitigation strategies. The Corporate Security and Resilience Division shall oversee the execution and documentation of such assessments.

o) Training and Awareness. The Avangrid Group shall implement a privacy training and awareness program for employees, contractors, and relevant third parties. Training shall be tailored to roles and responsibilities and shall be conducted at onboarding and at regular intervals thereafter. The program shall include education on privacy principles, data handling procedures, and incident reporting protocols.

p) Incident Response and Breach Management. The Avangrid Group shall maintain a documented incident response plan that includes procedures for identifying, reporting, investigating, and remediating data breaches involving PII. The plan shall define roles and responsibilities, escalation paths, and timelines for notification to affected individuals and regulators, as required by applicable law.

q) Third Party Risk Management. The Avangrid Group shall assess and manage privacy risks associated with third-party vendors that process PII. This includes conducting due diligence prior to engagement, executing appropriate contractual safeguards (e.g. data processing agreements), and performing ongoing monitoring and audits. Vendors shall be required to implement security and privacy controls consistent with Avangrid's standards.

r) Data Classification. The Avangrid Group shall classify PII based on sensitivity and business impact.

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.

4. Iberdrola Group Level Coordination

The Corporate Security and Resilience Division of Avangrid, through the Security, Resilience and Digital Technology Committee of Avangrid (or such committee or division as assumes the powers thereof at any time), shall ensure appropriate coordination of the practices and management of risks in the areas of personal data protection within the Avangrid Group, and shall establish appropriate coordination procedures with the Security

and Resilience Division of Iberdrola, S.A. through the Security, Resilience and Digital Technology Committee of Iberdrola, S.A. (or such committee or division as assumes the powers thereof at any time).

4. Implementation and Monitoring

For the implementation and monitoring of the provisions of this Policy, the Board of Directors is assisted by the Corporate Security and Resilience Division (or such division as assumes the powers thereof at any time), which, through the Security, Resilience and Digital Technology Committee (or such committee as assumes the powers thereof at any time), shall develop and keep updated, in accordance with the provisions of this Policy, the internal regulations for the management of personal data protection, which shall be implemented by the Corporate Security and Resilience Division of Avangrid and which shall be mandatory for the members of the management team and the professionals of Avangrid (particularly, it shall establish a procedure for regular monitoring and reporting to the corresponding governance bodies).

Avangrid's Corporate Security and Resilience 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 and Resilience Division of such material developments. Avangrid's technology divisions shall be responsible for implementing appropriate technology controls and developments.

As appropriate, the business and corporate function divisions of the Avangrid Group shall identify data owners and shall process PII in accordance with the principles set forth in this Policy and any applicable privacy procedures, rules and practices. Members of Avangrid's Corporate Security and Resilience Division participate in Iberdrola cybersecurity committees, which assist with coordination across the 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.

The Corporate Security and Resilience Division (or such division as assumes the powers thereof at any time) shall review this Policy at least once per year to ensure that the content thereof conforms to the ongoing progress, innovations, risks and regulatory changes that are occurring in the area.