Política de protección de datos personales

25 de marzo de 2025

El Consejo de Administración de IBERDROLA, S.A. (la "**Sociedad**") tiene atribuida la competencia de diseñar, evaluar y revisar con carácter permanente el Sistema de gobernanza y sostenibilidad y, específicamente, de aprobar y actualizar las políticas, las cuales contienen las pautas que rigen la actuación de la Sociedad y, además, en lo que sea de aplicación, informan las políticas que, en ejercicio de su autonomía de la voluntad, decidan aprobar las sociedades integradas en el grupo cuya entidad dominante es, en el sentido establecido por la ley, la Sociedad (el "**Grupo**").

En el ejercicio de estas competencias y en el marco de la normativa legal, de los Estatutos Sociales y del Propósito y Valores del Grupo Iberdrola, el Consejo de Administración aprueba esta Política de protección de datos personales (la "**Política**") que respeta, desarrolla y adapta, en relación con la Sociedad, los Principios éticos y básicos de gobernanza y de sostenibilidad del Grupo Iberdrola.

1. Ámbito de aplicación

Esta Política es de aplicación a la Sociedad. Sin perjuicio de lo cual, incluye principios básicos que complementan, en materia de protección de datos personales, los contenidos en los Principios éticos y básicos de gobernanza y de sostenibilidad del Grupo Iberdrola y, en esta medida, deben informar la actuación y los desarrollos normativos que, en el ejercicio de sus competencias y al amparo de su autonomía de la voluntad, lleven a cabo las demás sociedades del Grupo en esta materia.

En la medida en que formen parte del Grupo sociedades *subholding* cotizadas, ellas y sus filiales, al amparo de su propio marco especial de autonomía reforzada, podrán establecer principios y normas que deberán tener un contenido conforme a los principios de esta Política.

Estos principios deberán informar también, en lo que proceda, la actuación de las entidades de naturaleza fundacional vinculadas al Grupo.

La Sociedad promoverá, igualmente, en aquellas otras compañías en las que participe y que no formen parte del Grupo, así como en las *joint ventures*, uniones temporales de empresas y otras entidades en las que asuma la gestión, el alineamiento de su normativa, con los principios básicos en materia de protección de datos personales contenidos en esta Política.

2. Finalidad

La finalidad de esta Política es establecer los principios básicos de actuación que deben regir en la Sociedad en materia de protección de datos personales, garantizando, en todo caso, el cumplimiento de la normativa aplicable.

En particular, la Política garantiza el derecho a la protección de los datos de todas las personas físicas que se relacionan con la Sociedad, asegurando el respeto del derecho al honor y a la intimidad en el tratamiento de las diferentes tipologías de datos personales, procedentes de diferentes fuentes y con fines diversos en función de su actividad empresarial, todo ello en cumplimiento de la Política de respeto de los derechos humanos de la Sociedad.

3. Principios básicos de actuación

La Sociedad asume y promueve los siguientes principios básicos de actuación que deben informar sus actividades en materia de protección de datos personales:

a. Principios de legitimidad, licitud y lealtad en el tratamiento de datos personales.

   El tratamiento de datos personales será legítimo, lícito y leal, conforme a la normativa aplicable. En este sentido, los datos personales deberán ser recogidos para uno o varios fines específicos y legítimos conforme a la normativa aplicable.

   En los casos en los que resulte obligatorio, conforme a la normativa aplicable, deberá obtenerse el consentimiento de los interesados antes de recabar sus datos.

Asimismo, cuando lo exija la normativa legal, los fines del tratamiento de datos personales serán explícitos y determinados en el momento de su recogida.

En particular, la Sociedad no recabará ni tratará datos personales relativos al origen étnico o racial, a la ideología política, a las creencias, a las convicciones religiosas o filosóficas, a la vida u orientación sexual, a la afiliación sindical, a la salud, ni datos genéticos o biométricos dirigidos a identificar de manera unívoca a una persona, salvo que la recogida de los referidos datos sea necesaria, legítima y requerida o permitida por la normativa aplicable, en cuyo caso serán recabados y tratados de acuerdo con lo establecido en aquella.

b. Principio de minimización.

Solo serán objeto de tratamiento aquellos datos personales que resulten estrictamente necesarios para la finalidad para la que se recojan o traten y adecuados a tal finalidad.

c. Principio de exactitud.

Los datos personales deberán ser exactos y estar actualizados. En caso contrario, deberán suprimirse o rectificarse.

d. Principio de limitación del plazo de conservación.

Los datos personales no se conservarán más allá del plazo necesario para conseguir el fin para el cual se tratan, salvo en los supuestos previstos legalmente.

e. Principios de integridad y confidencialidad.

En el tratamiento de los datos personales se deberá garantizar, mediante medidas técnicas u organizativas, una seguridad adecuada que los proteja del tratamiento no autorizado o ilícito y que evite su pérdida, su destrucción y que sufran daños accidentales.

Los datos personales recabados y tratados por la Sociedad deberán ser conservados con la máxima confidencialidad y secreto, no pudiendo ser utilizados para otros fines distintos de los que justificaron y permitieron su recogida y sin que puedan ser comunicados o cedidos a terceros fuera de los casos permitidos por la normativa aplicable.

f. Principio de responsabilidad proactiva (rendición de cuentas).

La Sociedad será responsable de cumplir con los principios estipulados en esta Política y con los exigidos en la normativa aplicable y deberá ser capaz de demostrarlo, cuando así lo exija la normativa aplicable.

La Sociedad deberá hacer una evaluación del riesgo de los tratamientos que realice, con el fin de determinar las medidas a aplicar para garantizar que los datos personales se tratan conforme a las exigencias legales. En los casos en los que la normativa legal lo requiera, evaluará de forma previa los riesgos que para la protección de datos personales puedan comportar nuevos productos, servicios o sistemas de información y adoptará las medidas necesarias para eliminarlos o mitigarlos.

La Sociedad deberá llevar un registro de actividades en el que se describan los tratamientos de datos personales que lleve a cabo en el marco de sus actividades.

En el caso de que se produzca un incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizado a dichos datos, la Sociedad deberá seguir los protocolos internos establecidos a tal efecto por su Dirección de Seguridad y Resiliencia (o por la dirección que, en cada momento, asuma sus facultades) a través del Comité de Seguridad, Resiliencia y Tecnologías Digitales (o el comité que, en cada momento, asuma sus facultades) y por los que establezca la normativa aplicable. La Sociedad deberá documentar estos incidentes y adoptará medidas para solventar y paliar los posibles efectos negativos para los interesados.

La Sociedad designará un delegado de protección de datos con el fin de garantizar el cumplimiento de la normativa de protección de datos personales.

g. Principios de transparencia e información.

   El tratamiento de datos personales será transparente en relación con el interesado, facilitándole la información sobre el tratamiento de sus datos de forma comprensible y accesible, cuando así lo exija la ley aplicable.

   A fin de garantizar un tratamiento leal y transparente, la Sociedad deberá informar a los afectados o interesados cuyos datos se pretende recabar de las circunstancias relativas al tratamiento conforme a la normativa aplicable.

h. Adquisición u obtención de datos personales.

   Queda prohibida la adquisición u obtención de datos personales de fuentes ilegítimas, de fuentes que no garanticen suficientemente su legítima procedencia o de fuentes cuyos datos hayan sido recabados o cedidos contraviniendo la ley.

i. Contratación de encargados del tratamiento.

   Con carácter previo a la contratación de cualquier prestador de servicios que acceda a datos personales que sean responsabilidad de la Sociedad, así como durante la vigencia de la relación contractual, esta deberá adoptar las medidas necesarias para garantizar y, cuando sea legalmente exigible, demostrar, que el tratamiento de datos por parte del encargado se lleva a cabo conforme a la normativa aplicable.

j. Transferencias internacionales de datos.

   Todo tratamiento de datos personales sujeto a la normativa de la Unión Europea que implique una transferencia de datos fuera del Espacio Económico Europeo deberá llevarse a cabo con estricto cumplimiento de los requisitos establecidos en la ley aplicable en la jurisdicción de origen.

k. Derechos de los interesados.

   La Sociedad deberá permitir que los interesados puedan ejercitar los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición que sean de aplicación en cada jurisdicción, estableciendo, a tal efecto, los procedimientos internos que resulten necesarios para satisfacer, al menos, los requisitos legales aplicables en cada caso.

4. Coordinación a nivel del Grupo

La Dirección de Seguridad y Resiliencia, a través del Comité de Seguridad, Resiliencia y Tecnologías Digitales (o el comité o dirección que, en cada momento, asuma sus facultades) velará por la adecuada coordinación, a nivel de Grupo, de las prácticas y la gestión de los riesgos en el ámbito de la protección de los datos personales y establecerá los procedimientos de coordinación adecuados con los comités de seguridad, resiliencia y tecnologías digitales o con las direcciones de seguridad (o el comité o dirección que, en cada momento, asuma sus facultades) de las sociedades *subholding*.

Las direcciones de Servicios Jurídicos de cada país serán responsables de reportar al Comité de Seguridad, Resiliencia y Tecnologías Digitales (o al comité que, en cada momento, asuma sus facultades) los desarrollos y novedades normativas que se produzcan en el ámbito de la protección de datos personales.

Adicionalmente, los negocios y las direcciones corporativas deberán: (i) designar a las personas responsables de los datos, que actuarán coordinadamente y bajo la supervisión del Comité de Seguridad, Resiliencia y Tecnologías Digitales (o el comité que, en cada momento, asuma sus facultades) y de la Dirección de Seguridad y Resiliencia (o de la dirección que, en cada momento, asuma sus facultades); y (ii) coordinar con la Dirección de Seguridad

y Resiliencia (o con la dirección que, en cada momento, asuma sus facultades) cualquier actividad que implique o conlleve la gestión de datos personales, respetando en todo caso el marco especial de autonomía reforzada de las sociedades *subholding* cotizadas.

5. Implementación y seguimiento

Para la implementación y seguimiento de lo previsto en esta Política, el Consejo de Administración cuenta con la Dirección de Seguridad y Resiliencia (o la dirección que, en cada momento, asuma sus facultades), que, a través del Comité de Seguridad, Resiliencia y Tecnologías Digitales (o el comité que, en cada momento, asuma sus facultades) desarrollará y mantendrá actualizada, conforme a lo dispuesto en esta *Política*, la normativa interna de gestión de la protección de datos personales, que se implementará por la Dirección de Seguridad y Resiliencia y que será de obligado cumplimiento para los miembros del equipo directivo y de los profesionales de la Sociedad.

Sin perjuicio de lo anterior, será la Dirección de Sistemas de la Sociedad (o la dirección que, en cada momento, asuma sus facultades) la responsable de velar por la correcta implementación de los sistemas de información de la Sociedad, los controles y desarrollos informáticos que sean adecuados para garantizar el cumplimiento de la normativa interna de la protección de datos y que dichos desarrollos estén actualizados en cada momento.

La Dirección de Seguridad y Resiliencia (o la dirección que, en cada momento, asuma sus facultades) evaluará, al menos una vez al año, el cumplimiento y la eficacia de esta Política.

Además, para verificar el cumplimiento de esta *Política* se realizarán auditorías periódicas con auditores internos o externos.

* * *

Esta Política fue aprobada inicialmente por el Consejo de Administración el 21 de julio de 2015 y modificada por última vez el 25 de marzo de 2025.