Normas corporativas vinculantes do Grupo Iberdrola

Novembro 2024

Iberdrola

Índice

INTRODUÇÃO

As Normas Corporativas Vinculantes (doravante denominadas "**NCV**") demonstram o compromisso global de todas as empresas que compõem o Grupo Iberdrola e que aderiram a essas NCV (Iberdrola, S.A., a empresa controladora, e todas as suas empresas controladas que também aderiram a essas NCV, doravante denominadas "**Grupo Iberdrola**" e cada uma de suas empresas aderentes, as "**Empresas do Grupo**") com a privacidade e a proteção de dados e estabelecem o marco de garantias adequadas para a transferência e o tratamento de dados pessoais entre elas.

Estas NCV são adotadas de acordo com as disposições contidas no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (doravante, o "**GDPR**").

Estas SLCs se aplicam a todos os dados pessoais que, sendo processados no Espaço Econômico Europeu (doravante denominado "**E.E.A**."), por Empresas do Grupo atuando como controlador ou processador de um controlador dentro do Grupo, e transferidos direta ou indiretamente de Empresas do Grupo localizadas no E.E.A. para Empresas do Grupo localizadas fora do E.E.A., e se relacionam com o processamento de dados pessoais que se enquadram no escopo destas SLCs.

As obrigações estabelecidas nestas NCV se aplicam a todas as empresas do Grupo que atuam como Controladores e também às empresas do Grupo que atuam como Processadores internos.

Ao aderir a essas NCVs, as empresas do Grupo se comprometem a respeitar e cumprir suas disposições na coleta, compilação e processamento de dados pessoais para seus próprios fins e a garantir que todos os seus funcionários as cumpram.

O Coordenador Global de Proteção de Dados de Segurança Corporativa deverá garantir que as empresas do Grupo cumpram essas CSV de forma coordenada e de acordo com critérios interpretativos comuns.

Essas NCVs e as empresas do Grupo são publicadas no site www.iberdrola.com e na Intranet do Grupo Iberdrola.

1. DEFINIÇÕES

a. "**Dados pessoais**": significa qualquer informação relacionada a uma pessoa física identificada ou identificável ("titular dos dados"); uma pessoa física identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador, como nome, número de identificação, dados de localização, identificador on-line ou a um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa.

b. "**Categorias especiais de dados pessoais**": categorias especiais de dados pessoais são origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos que permitem a identificação exclusiva de um indivíduo, dados relativos à saúde, à vida e à orientação sexual.

c. "**Processamento**" significa qualquer operação ou conjunto de operações executadas sobre dados pessoais ou sobre dados pessoais, seja ou não por meios automáticos, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou qualquer outra forma de disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição.

d. "**Controlador**" significa a pessoa física ou jurídica, autoridade pública, serviço ou outro órgão que, sozinho ou em conjunto com outros, determina as finalidades e os meios do processamento.

   Nessas NCVs, o Controlador será a Empresa do Grupo que transfere os dados pessoais e a Empresa do Grupo que recebe os dados pessoais quando os dados forem processados pela Empresa para seus próprios fins.

e. "**Processador**" significa a pessoa física ou jurídica, autoridade pública, serviço ou outro órgão que processa dados pessoais em nome do controlador.

   Para os fins dessas NCVs, a empresa do Grupo que presta os serviços de acordo com o contrato de prestação de serviços relevante também será o processador de dados.

f. "**Destinatário**" significa a pessoa física ou jurídica, autoridade pública, agência ou outro órgão a quem os dados pessoais são divulgados, seja ou não um terceiro.

g. "**Terceiro**" significa uma pessoa física ou jurídica, autoridade pública, serviço ou outro órgão que não seja o titular dos dados, o controlador, o processador e as pessoas autorizadas a processar dados pessoais sob a autoridade direta do controlador ou do processador.

h. "**Grupo Iberdrola ou Grupo**" significa um grupo composto pela Iberdrola, S.A., a empresa controladora, e todas as suas empresas controladas.

i. "**Empresa(s) do Grupo**": cada uma das empresas do Grupo Iberdrola que aderiram às NCVs por meio da assinatura do Acordo Intragrupo sobre as NCVs.

j. "**Sociedade controladora**": de acordo com o Código Comercial espanhol, no Grupo Iberdrola, a sociedade controladora é a sociedade do Grupo que cumpre qualquer um dos requisitos em relação às demais sociedades controladas:

   1. Ela detém a maioria dos direitos de voto.
   2. Ter o poder de nomear ou demitir a maioria dos membros do órgão de administração.
   3. Pode dispor, em virtude de acordos celebrados com terceiros, da maioria dos direitos de voto.

4. Nomeou com seus votos a maioria dos membros do órgão de administração em exercício no momento em que as contas consolidadas devem ser elaboradas e durante os dois exercícios financeiros imediatamente anteriores.

k. "**Sociedade *subholding***": sociedade que agrupa na Espanha, no Reino Unido, nos Estados Unidos, no México e no Brasil as sociedades do Grupo Iberdrola domiciliadas nesse país e que não reportam diretamente à Iberdrola, S.A. Excepcionalmente, a Iberdrola Energía Internacional, S.A. agrupa as sociedades do Grupo Iberdrola que não respondem a nenhuma das sociedades *subholding* do país mencionadas anteriormente e que não respondem diretamente à Iberdrola, S.A. A sociedade *subholding* do país responde diretamente à Iberdrola, S.A. e, portanto, suas filiais fazem parte do Grupo Iberdrola.

l. "**Regras Corporativas Vinculantes**" significa as políticas de proteção de dados pessoais adotadas por um controlador ou processador estabelecido no território de um Estado Membro para transferências ou um conjunto de transferências de dados pessoais para um controlador ou processador em um ou mais países terceiros, dentro de um grupo de empresas ou um grupo de empresas envolvidas em uma atividade econômica conjunta.

m. "**Autoridade de Supervisão**" significa a autoridade pública independente estabelecida por um Estado-Membro para supervisionar e coordenar a aplicação do GDPR.

n. "**Autoridade pública**" significa a autoridade pública estabelecida no país importador que, em conformidade com a lei desse país, solicita acesso aos Dados Pessoais do Exportador de Dados dos Dados transferidos nos termos do LCS.

o. "**Agência Espanhola de Proteção de Dados**": autoridade supervisora competente para supervisionar e coordenar o procedimento de autorização dos NCVs, para proceder à sua aprovação e para informar as autoridades supervisoras interessadas sobre qualquer atualização dos NCVs ou da lista de membros dos NCVs.

p. "**Titular dos dados**" significa uma pessoa física identificada ou identificável à qual pertencem os dados pessoais que são transferidos do EEE para países terceiros.

q. "**Exportador de dados**" significa uma empresa do Grupo estabelecida em um país da União Europeia que transfere, direta ou indiretamente, dados pessoais para outra empresa do Grupo não estabelecida em um país da União Europeia.

r. "**Importador de dados**" significa uma Empresa do Grupo que, não estando em um país do E.E.E., recebe dados pessoais de um exportador de dados.

s. "**Medidas de segurança**" significa medidas técnicas e organizacionais apropriadas para garantir um nível de segurança adequado ao risco.

t. "**Consentimento**" significa qualquer indicação dada livremente, específica, informada e inequívoca pela qual o titular dos dados concorda, seja por uma declaração ou por uma ação afirmativa clara, com o processamento de dados pessoais relacionados a ele.

u. "**Terceiro país**" significa um país estabelecido fora do EEE.

v. "**Lei do Estado Membro**": refere-se à lei nacional de um estado membro da União Europeia e à lei dos países da União Europeia.

Quando não previsto neste parágrafo, as Empresas do Grupo interpretarão essas NCVs de acordo com o GDPR.

2. ESCOPO DE APLICAÇÃO

2.1. ESCOPO MATERIAL DE APLICAÇÃO DA NCV

O processamento de dados pessoais a seguir é coberto pela LCA:

- **Candidatos a um posto de trabalho no Grupo Iberdrola:** Dados de identificação e curriculares do candidato a um posto de trabalho e estágio, que se registre no portal de emprego do Grupo Iberdrola, com o objetivo de permitir sua participação em possíveis processos de seleção de pessoal ou estágios de estudantes. Seus dados pessoais poderão ser transferidos a qualquer empresa do Grupo, inclusive fora da E.E.E., que esteja interessada em seu perfil, produzindo assim uma transferência internacional de dados.
- **Funcionários:** dados pessoais dos funcionários obtidos como resultado da relação de emprego, no processo de formalização da relação e durante o período em que a relação é mantida. Esses dados podem ser comunicados a empresas do Grupo, incluindo aquelas fora da E.E.E., para procedimentos internos de preenchimento de vagas, para a gestão do vínculo empregatício, em conformidade com contratos de serviço e para a gestão e organização de equipes. Todas essas transferências internacionais são necessárias para o gerenciamento e o cumprimento do vínculo empregatício com o funcionário.
- **Fornecedores:** Dados de identificação pessoal, características pessoais e profissionais, informações comerciais, dados financeiros e dados relativos a transações que envolvam bens e serviços de fornecedores, todos com a finalidade de gerenciamento global de fornecedores. Esses dados são comunicados às empresas do Grupo, incluindo aquelas fora da E.E.E. A transferência internacional é realizada como resultado do uso de um banco de dados comum para todas as empresas do Grupo Iberdrola.
- **Voluntários:** Dados pessoais que identificam os voluntários para a gestão do programa de voluntariado da Iberdrola e atividades relacionadas. Esses dados são comunicados às empresas do Grupo Iberdrola, inclusive fora da E.E.E., que oferecem uma ação de voluntariado. A transferência internacional é realizada pela Iberdrola, S.A., que é responsável pelo tratamento dos dados pessoais dos voluntários do Grupo Iberdrola incluídos em um arquivo global, e por outras empresas do Grupo estabelecidas no EEE, que são responsáveis pelo tratamento dos dados dos voluntários.

- **Participantes de eventos:** Dados pessoais que identificam os participantes do evento com a finalidade de gerenciar eventos corporativos. Esses dados serão comunicados a outras empresas do Grupo Iberdrola para fins de administração interna. A transferência internacional é realizada pela Iberdrola, S.A. e por outras empresas do Grupo estabelecidas no EEE como responsáveis pelo tratamento dos dados dos participantes do evento.
- **Participantes de concursos de bolsas de estudo de mestrado e beneficiários das mesmas:** Identificação pessoal, dados acadêmicos e profissionais dos participantes em candidaturas a bolsas de estudo de mestrado: para a gestão e concessão de bolsas de estudo. Os dados fornecidos pelo solicitante são incluídos em um banco de dados ao qual terá acesso a subholding do Grupo que concede a bolsa de estudos para a qual foi apresentada a solicitação. Esses dados pessoais também são acessados pela Iberdrola, S.A. como entidade encarregada da gestão administrativa interna global das bolsas de estudo do Grupo Iberdrola.

2.2. ESCOPO GEOGRÁFICO DE APLICAÇÃO DAS NCVS

Estas NCV se aplicam às transferências dos dados pessoais especificados no escopo de aplicação destas NCV, realizadas pelas Empresas do Grupo em sua capacidade de Controladores ou Processadores. Portanto, essas NCV se aplicam à Empresa do Grupo localizada em um país da União Europeia que exporta dados pessoais direta ou indiretamente e à Empresa do Grupo não localizada em um país da União Europeia que importa os dados pessoais.

As LCAs se aplicam às primeiras transferências de dados pessoais e às transferências posteriores.

Essas LCOs são obrigatórias para as empresas do Grupo que assinaram o Acordo de LCO Intragrupo (doravante, o "**IA**") no qual expressam sua aceitação e que está incluído como um anexo a este acordo. Além disso, o Anexo I destes NICs inclui uma lista das empresas do Grupo que estão vinculadas a estes NICs, agrupadas pelas empresas do Grupo que controlam direta ou indiretamente as primeiras. No caso de

Se tiver alguma dúvida em relação às empresas do Grupo vinculadas a essas NCVs, entre em contato com o Coordenador de Proteção de Dados de Segurança Corporativa Global, cujos detalhes de contato são: dpo@iberdrola.com.

De acordo com o RGPD e a legislação trabalhista aplicável, essas NCVs são vinculantes e aplicáveis aos funcionários do Grupo Iberdrola de todas as empresas do Grupo. Os funcionários foram informados de sua existência, indicando que são normas obrigatórias e estabelecendo que, de acordo com a legislação aplicável e os contratos de trabalho com cada uma das empresas do Grupo, essas empresas poderão aplicar o sistema disciplinar correspondente em caso de descumprimento das mesmas.

As atividades de processamento e as categorias de dados pessoais dentro do escopo da NCV são aquelas relacionadas ao escopo de aplicação da NCV, que se aplicam tanto ao processamento manual quanto ao automatizado. As transferências de dados pessoais são feitas entre as Empresas do Grupo no curso normal de suas atividades, e esses dados podem ser armazenados em bancos de dados centralizados acessíveis pelas Empresas do Grupo a partir de qualquer parte do mundo em que o Grupo Iberdrola esteja presente.

3. PRINCÍPIOS

Qualquer tratamento de dados pessoais realizado pelas Empresas do Grupo, tanto como Controlador quanto como Processador, deverá cumprir os seguintes princípios, cuja implementação é realizada por meio das normas, procedimentos, metodologias e ferramentas corporativas do Grupo Iberdrola.

3.1. CONFORMIDADE COM A LEGISLAÇÃO LOCAL E A RGPD

Além de cumprir essas NCVs, cada Empresa do Grupo deve cumprir as leis locais aplicáveis relacionadas a dados pessoais e deve garantir que a coleta e o uso de dados pessoais sejam feitos em conformidade com essas leis.

3.2. LEGALIDADE, IMPARCIALIDADE E TRANSPARÊNCIA

Os dados pessoais devem ser processados de forma legal, justa e transparente em relação ao titular dos dados.

O processamento de dados é legal se for baseado em uma das seguintes condições previstas no GDPR:

a. **Consentimento:** o titular dos dados deu seu consentimento para o processamento de seus dados pessoais para uma ou mais finalidades específicas. Por exemplo, o processamento de imagens de funcionários por empresas do Grupo para fins de comunicação corporativa e social é realizado se o titular dos dados tiver dado seu consentimento.

   Quando o consentimento for a base legítima para o processamento, o controlador deverá garantir que esse consentimento tenha sido obtido de maneira apropriada:

   1. **Livre:** para que o consentimento seja livre, deve haver uma escolha real por parte do indivíduo de não consentir.
   2. **Específico:** as finalidades do processamento devem ser específicas e não podem ser diluídas ou ampliadas depois que o titular dos dados consentir com a coleta de dados.
   3. **Informado:** o Controlador deve informar ao titular dos dados as finalidades do processamento e, além disso, é obrigado a fornecer informações adicionais, quando necessário, para garantir que o usuário realmente compreenda as operações de processamento.
   4. **Não ambíguo:** o consentimento deve estar expressamente relacionado a cada processamento específico de dados pessoais.

   O consentimento deve ser obtido separadamente da aceitação de quaisquer cláusulas relativas aos termos e condições da relação jurídica na qual se baseia e em linguagem clara e simples.

Deve ser mantido um registro de quando e como o consentimento do titular dos dados foi obtido e para qual finalidade específica, bem como a base documental para o consentimento.

Além disso, o Controlador deve garantir que o titular dos dados possa retirar seu consentimento a qualquer momento com a mesma facilidade com que o deu.

b. **Relação contratual:** o processamento é necessário para a execução de uma relação contratual entre a Empresa do Grupo e o titular dos dados ou para a implementação de medidas pré-contratuais solicitadas pelo titular dos dados.

c. **Obrigação legal:** o processamento é necessário para que a Empresa do Grupo, atuando como controladora ou processadora, cumpra uma obrigação legal.

d. **Interesse vital:** o processamento é necessário para a proteção dos interesses vitais do titular dos dados ou de outra pessoa física.

e. **Interesse público:** o processamento é necessário para garantir que o Controlador execute uma tarefa de interesse público.

f. **Interesse legítimo:** o processamento é necessário para os fins dos interesses legítimos do controlador ou de terceiros, desde que esses interesses não sejam sobrepostos pelos interesses ou direitos e liberdades fundamentais do titular dos dados que exijam a proteção dos dados pessoais, especialmente quando o titular dos dados for uma criança.

Os titulares dos dados devem ser informados sobre as atividades de processamento realizadas em seus dados pessoais. Em particular, eles devem ser informados sobre:

a. A identidade e os detalhes de contato do Controlador e, quando aplicável, de seu representante.

b. Os detalhes de contato do Diretor de Proteção de Dados.

c. As finalidades do processamento.

d. A base legal ou a legitimação para o processamento. Caso a base legal seja o interesse legítimo do Controlador ou de um terceiro, desde que esse interesse não seja sobreposto pelos interesses ou direitos e liberdades fundamentais do titular dos dados que exijam a proteção dos dados pessoais, esse interesse deverá ser divulgado.

e. Categoria de dados pessoais em questão.

f. O período de retenção de dados ou os critérios usados para determinar o período.

g. A existência de decisões automatizadas ou criação de perfis.

h. Se os dados forem transferidos a terceiros, os destinatários ou categorias de destinatários deverão ser indicados.

i. Se o fornecimento de dados é um requisito legal ou contratual, ou um requisito necessário para a celebração de um contrato, e se o titular dos dados é obrigado a fornecer os dados pessoais e é informado sobre as possíveis consequências de não fornecer esses dados.

j. Se estão previstas ou não transferências internacionais de dados para países terceiros e, em caso afirmativo, as garantias de proteção que serão aplicadas a elas.

k. Os direitos de proteção de dados aos quais você tem direito. São eles: o direito de acesso, retificação, exclusão, restrição de processamento, o direito de ser notificado sobre o status e o resultado da solicitação de retificação, exclusão ou restrição de processamento, o direito de se opor ao processamento, o direito à portabilidade de dados e o direito de não estar sujeito a decisões baseadas exclusivamente em processamento automatizado, inclusive criação de perfis. Quando o processamento for baseado (i) no consentimento do titular dos dados para uma ou mais finalidades ou (ii) no consentimento explícito para o processamento de dados que revelem a origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas ou filiação sindical, e o processamento de dados genéticos, dados biométricos destinados a identificar exclusivamente uma pessoa física, dados relativos à saúde ou dados relativos à vida sexual ou orientações sexuais de uma pessoa física, o direito de retirar o consentimento deverá ser informado a qualquer momento.

l. O direito de apresentar uma reclamação às autoridades de supervisão caso o titular dos dados considere que seus direitos à proteção de dados pessoais previstos na legislação aplicável ou nestas NCAs não foram respeitados.

m. A existência de decisões automatizadas, incluindo a criação de perfis e informações significativas sobre a lógica aplicada, e a importância e as consequências desse processamento para o titular dos dados.

n. Caso o controlador pretenda continuar a processar os dados pessoais para uma finalidade diferente daquela para a qual eles foram originalmente coletados, deverão ser fornecidas informações sobre essa outra finalidade e quaisquer informações relevantes de acordo com os parágrafos acima.

o. No caso de os dados não serem obtidos do próprio titular dos dados, além do indicado nas seções anteriores, deverão ser fornecidas informações sobre a fonte de origem dos dados pessoais e, se aplicável, se eles são provenientes de fontes acessíveis ao público.

3.3. LIMITAÇÃO DE PROPÓSITO

Os dados pessoais são coletados para fins específicos, explícitos e legítimos e não serão processados para fins incompatíveis com aqueles para os quais foram originalmente coletados. Por exemplo, o registro de um fornecedor requer apenas as informações necessárias para manter e gerenciar o relacionamento comercial (identificação geral e detalhes de contato, dados bancários e transacionais, como faturas e contratos) e é processado apenas para essa finalidade, não sendo processado para finalidades para as quais não se destina.

3.4. MINIMIZAÇÃO DE DADOS

Os dados pessoais devem ser adequados, relevantes e limitados ao que é necessário em relação às finalidades do processamento. Somente as informações estritamente necessárias para os fins do processamento devem ser coletadas. Especificamente, cada empresa do Grupo tem acesso aos dados completos de seus fornecedores, e o acesso das outras empresas do Grupo é restrito aos dados gerais dos fornecedores (identificação, contato e dados bancários).

3.5. ACURACIDADE

Os dados pessoais devem ser precisos e mantidos atualizados. Em particular:

a. Todos os repositórios de informações, incluindo aplicativos, bancos de dados, planilhas, etc., devem, na medida do possível, incluir um mecanismo de validação de dados para garantir que as informações sejam precisas e completas.

b. Os processos de revisão regular e melhoria contínua das informações serão implementados para garantir que os dados sejam precisos e atualizados.

3.6. LIMITAÇÃO DO PERÍODO DE RETENÇÃO

Os dados pessoais devem ser mantidos em um formato que permita a identificação dos titulares dos dados por um período não superior ao necessário para os fins do processamento. Em particular:

a. Todo o processamento de dados pessoais está vinculado a períodos de retenção implementados por meio de um processo manual ou automático e registrados no Registro de Atividades de Processamento.

b. Os dados pessoais não são retidos por mais tempo do que o período implementado por meio de processos manuais ou automáticos.

c. Os períodos obrigatórios de retenção de dados, sem prejuízo de seu bloqueio após a conclusão do processamento para o qual os dados foram coletados, são aqueles resultantes da legislação, normas e outros regulamentos aplicáveis, tanto estaduais quanto setoriais, em cada caso.

3.7. PROCESSAMENTO DE DADOS DE CATEGORIAS ESPECIAIS DE DADOS PESSOAIS

As Empresas do Grupo estão proibidas de processar categorias especiais de dados pessoais, a menos que haja uma base legítima para o processamento, conforme previsto no Artigo 6.1 do GDPR, e que exista uma das circunstâncias previstas no Artigo 9.2 do GDPR, que isenta a proibição geral de processar categorias especiais de dados. Essas circunstâncias são:

a. **O titular dos dados deu seu consentimento explícito** para o processamento de tais dados pessoais de categoria especial para uma ou mais das finalidades especificadas, e tal consentimento é considerado válido de acordo com as leis e regulamentos aplicáveis;

b. **O processamento é necessário para o cumprimento de obrigações e para o exercício de direitos específicos** do controlador ou do titular dos dados no campo da legislação trabalhista e da seguridade social e proteção social, na medida em que isso seja autorizado pela lei aplicável que prevê garantias adequadas para o respeito aos direitos e interesses fundamentais do titular dos dados;

c. **O processamento é necessário para proteger os interesses vitais** do titular dos dados ou de outra pessoa física, quando o titular dos dados não for legal ou fisicamente capaz de dar consentimento;

d. **O processamento está relacionado a dados pessoais** que o titular dos dados tenha manifestamente tornado públicos;

e. **O processamento é necessário para a formulação, o exercício ou a defesa de reivindicações** ou quando os tribunais estiverem atuando em suas funções judiciais.

3.8. INTEGRIDADE E CONFIDENCIALIDADE

Os dados pessoais são processados de forma a garantir sua segurança por meio da aplicação de medidas técnicas e organizacionais apropriadas.

Para garantir esse princípio, os dados pessoais para os quais uma empresa do Grupo é a controladora ou processadora devem ser processados:

a. De forma segura e com proteção adequada contra processamento não autorizado ou ilegal e contra perda, destruição ou alteração acidental ou ilegal. Para essas finalidades, as medidas de segurança consideradas necessárias, dependendo do nível de risco da atividade de processamento em questão, devem ser implementadas em cada caso.

b. Em condições que garantam a confidencialidade, a integridade, a disponibilidade e a resiliência contínuas dos sistemas e serviços de processamento.

c. Em condições que garantam a capacidade de restaurar a disponibilidade e o acesso aos dados pessoais rapidamente no caso de um incidente físico ou técnico

As medidas técnicas e organizacionais desenvolvidas e implementadas para garantir a segurança dos dados pessoais e seu processamento devem estar sujeitas a verificação, avaliação e apreciação regulares de sua eficácia.

As Empresas do Grupo devem cumprir o Marco de Cibersegurança do Grupo Iberdrola, que define o programa, as políticas, as normas e os processos necessários para gerenciar os riscos de cibersegurança no ambiente operacional da Iberdrola.

3.9. VIOLAÇÕES DE SEGURANÇA DE DADOS PESSOAIS

Em caso de violação da segurança que provoque a destruição, perda, alteração acidental ou ilícita de dados pessoais, bem como qualquer comunicação ou acesso não autorizado a dados pessoais transmitidos, armazenados ou processados de qualquer outra forma, a empresa do Grupo responsável ou encarregada do processamento deverá proceder de acordo com as disposições do procedimento interno do Grupo Iberdrola: Procedimento de resposta a incidentes de dados pessoais, que determina a organização e os critérios de ação para a detecção, contenção, avaliação de riscos, comunicação e notificação de incidentes de segurança que envolvam dados pessoais.

Este procedimento estabelece a obrigação das Empresas do Grupo que tenham sido afetadas por uma Violação de Segurança de Dados Pessoais relacionada a dados pessoais transferidos do E.E.E. de notificar, sem atrasos indevidos, as Empresas do Grupo que aceitam a responsabilidade por qualquer violação das NCVs por qualquer uma das Empresas do Grupo estabelecidas fora do E.E.E., e o Coordenador Global de Proteção de Dados de Segurança Corporativa.

Caso a Violação de Segurança de Dados Pessoais possa constituir um risco para os direitos e liberdades dos titulares de dados, o Coordenador de Proteção de Dados de Segurança Corporativa Local ou, conforme o caso, o Coordenador de Proteção de Dados de Segurança Corporativa Global deverá notificar a Autoridade Supervisora competente no prazo máximo de 72 horas após ter tomado conhecimento do fato.

Quando for provável que a violação de segurança de dados pessoais constitua um alto risco para os direitos e liberdades dos titulares dos dados, as Empresas do Grupo afetadas deverão notificar os titulares dos dados diretamente, sem atrasos indevidos.

As notificações de uma violação de segurança devem ser documentadas e incluir, no mínimo:

a. Descrição da natureza da violação de segurança: número de titulares de dados afetados, categoria de titulares de dados afetados, número aproximado de registros de dados pessoais afetados, etc.

b. Nome e detalhes de contato do responsável pela proteção de dados ou outro ponto de contato onde possam ser obtidas mais informações.

c. Efeitos e possíveis consequências da violação de segurança.

d. Descrição das medidas tomadas ou propostas para remediar a violação de segurança, incluindo, quando apropriado, medidas tomadas para mitigar possíveis efeitos negativos.

Essa documentação deve ser disponibilizada para a Agência Espanhola de Proteção de Dados e para qualquer outra Autoridade de Supervisão, mediante solicitação.

3.10. PROCESSAMENTO REALIZADO POR PROCESSADORES DE DADOS

As Empresas do Grupo não podem contratar os serviços de um provedor para acessar dados pessoais dos quais a Empresa é a Controladora sem antes garantir que o processador implementará medidas técnicas e organizacionais adequadas para garantir a proteção dos direitos e liberdades dos titulares dos dados.

Deve ser assinado um contrato ou outro ato jurídico semelhante que vincule o Processador ao Controlador e estabeleça a finalidade, a duração, a natureza e o objetivo do processamento, o tipo de dados pessoais e as categorias de titulares de dados a que se referem, os direitos e as obrigações do Controlador e do Processador. As obrigações do Processador devem ser, no mínimo e expressamente previstas no contrato ou ato legal semelhante, as seguintes:

a. Processar dados pessoais somente de acordo com as instruções documentadas do Controlador, inclusive com relação a transferências de dados pessoais para um terceiro país ou uma organização internacional, a menos que seja obrigado a fazê-lo de acordo com a legislação da União Europeia ou do Estado Membro aplicável ao Processador.

   Nesse caso, e a menos que essa lei o proíba por motivos de interesse público, o Controlador deverá informar o Controlador sobre essa exigência legal antes do processamento.

b. Garantir que as pessoas autorizadas a processar dados pessoais tenham se comprometido a respeitar a confidencialidade ou estejam sujeitas a uma obrigação de confidencialidade de natureza estatutária.

c. Tomar todas as medidas necessárias para garantir a segurança do processamento.

d. Não permitir o acesso aos dados pessoais a outro Processador sem a prévia autorização específica ou geral por escrito do Controlador. Em qualquer caso, o processamento de dados pessoais realizado pelo novo subprocessador deve estar em conformidade com as instruções do Controlador, e o Processador deve assinar um contrato com o novo subprocessador de acordo com o Artigo 28 do GDPR.

e. Auxiliar o Controlador, levando em conta a natureza do processamento, por meio de medidas técnicas e organizacionais apropriadas, quando possível, para permitir que o Controlador cumpra sua obrigação de responder a solicitações para o exercício dos direitos dos titulares dos dados.

f. Auxiliar o Controlador a garantir a conformidade com as obrigações estabelecidas no GDPR, levando em consideração a natureza do processamento e as informações disponíveis para o Processador:

   – Levando em consideração o estado da técnica, os custos de implementação e a natureza, o escopo, o contexto e as finalidades do processamento, bem como os riscos de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas físicas, o controlador deverá implementar medidas técnicas e organizacionais apropriadas para garantir um nível de segurança adequado ao risco.
   – O Controlador deverá, sem atrasos indevidos após ter tomado conhecimento, notificar o Controlador sobre violações de segurança de dados pessoais.
   – O Controlador fornecerá apoio razoável ao Controlador na realização de qualquer Avaliação de Impacto sobre a Proteção de Dados e em consultas prévias às Autoridades de Supervisão ou outras autoridades competentes de proteção de dados, quando apropriado.

g. A critério do Controlador, exclua ou devolva todos os dados pessoais após o término da prestação dos serviços de processamento e exclua as cópias existentes, a menos que a retenção de dados pessoais seja exigida pela legislação da União Europeia ou do Estado Membro.

h. Disponibilizar ao Controlador todas as informações necessárias para demonstrar o cumprimento das obrigações que lhe cabem, bem como permitir e contribuir para a realização de auditorias, inclusive inspeções, pelo Controlador ou outro auditor autorizado pelo Controlador.

i. Informar imediatamente o Controlador em caso de não conformidade com suas obrigações como Controlador de Dados.

3.11. PROCESSAMENTO INTERNACIONAL DE DADOS PESSOAIS

O tratamento de dados pessoais que implique uma transferência de dados para Responsáveis e Subcontratantes que não façam parte do Grupo Iberdrola e que estejam localizados em países fora do EEE deve estar sujeito a garantias adicionais para assegurar que o nível de proteção seja adequado. Portanto, somente poderá ser realizada a transferência de dados pessoais de uma Empresa do Grupo para Empresas do Grupo não afiliadas ou para empresas terceiras:

1. Quando os países nos quais as empresas-alvo (Grupo ou terceiros) estão localizadas oferecerem um nível adequado de proteção, de acordo com uma decisão de adequação da Comissão Europeia.

2. Quando os países em que as empresas destinatárias estiverem localizadas forem diferentes daqueles listados no parágrafo (1), o Controlador ou Processador deverá tomar as medidas adequadas para compensar a falta de proteção de dados no país de destino. A título de exemplo:

   - Cláusulas contratuais padrão de proteção de dados adotadas pela Comissão Europeia ou por uma autoridade de supervisão;
   - Regras corporativas vinculantes para processadores;
   - Códigos de conduta vinculantes, que estabelecem as obrigações das empresas aderentes em relação à transferência internacional de dados de acordo com o GDPR; juntamente com compromissos vinculantes e executáveis com o controlador ou processador do terceiro país para implementar proteções adequadas, incluindo aquelas relacionadas aos direitos dos titulares dos dados.
   - Certificação de proteção de dados pessoais demonstrando que as empresas certificadas estão em conformidade com o GDPR em relação às transferências internacionais; juntamente com compromissos vinculativos e executáveis com o controlador ou processador do terceiro país para implementar proteções adequadas, incluindo aquelas relacionadas aos direitos dos titulares dos dados.
   - Instrumentos juridicamente vinculativos e executáveis contra autoridades ou órgãos públicos.

Além dos casos previstos nas duas seções anteriores, as transferências internacionais de dados só podem ser feitas por empresas do Grupo para empresas não pertencentes ao Grupo ou para terceiros se:

- O titular dos dados deu seu consentimento explícito e informado.
- A transferência internacional é necessária para (i) a celebração ou a execução de um contrato entre o titular dos dados e o controlador ou para a execução de medidas pré-contratuais tomadas a pedido do titular dos dados; (ii) a celebração ou a execução de um contrato, no interesse do titular dos dados, entre o controlador e outra pessoa física ou jurídica; (iii) a proteção dos interesses vitais do titular dos dados ou de outras pessoas, quando o titular dos dados for física ou legalmente incapaz de dar consentimento; ou (iv) a formulação, o exercício ou a defesa de reivindicações.
- A transferência internacional foi autorizada pela autoridade supervisora antes da transferência e com base em cláusulas contratuais acordadas entre o controlador ou processador e o controlador, processador ou destinatário dos dados pessoais no terceiro país.
- A transferência internacional é baseada em um interesse legítimo do Controlador sobre o qual os interesses ou direitos e liberdades fundamentais do titular dos dados não são sobrepostos, e a transferência (i) não é repetitiva, (ii) envolve um número limitado de titulares de dados e (iii) são adotadas salvaguardas específicas e adequadas de proteção de dados. A autoridade supervisora e o titular dos dados também devem ser informados. Isso só é admissível em circunstâncias excepcionais e quando nenhum dos três motivos acima para transferência se aplicar.

O fato de a transferência internacional de dados resultar da prestação de serviços não isenta a obrigação de firmar um contrato com o processador de acordo com as disposições do GDPR.

O procedimento interno do Grupo Iberdrola, denominado Procedimento sobre transferências internacionais de dados pessoais, estabelece as diretrizes a serem seguidas de acordo com o GDPR quando uma empresa do Grupo localizada no EEE precisar fazer transferências internacionais de dados pessoais para destinatários fora do EEE.

3.12. REGISTRO DE ATIVIDADES DE PROCESSAMENTO

Cada Controlador e Processador mantém um Registro de Atividades de Processamento, que deve ser feito por escrito, inclusive em formato eletrônico, registrando todo o processamento de dados pessoais realizado por eles. O Registro de Atividades de Processamento deverá ser disponibilizado à autoridade supervisora mediante solicitação.

O Registro de Atividades de Processamento deve incluir:

a. O nome e os detalhes de contato do controlador de dados e, quando aplicável, da pessoa corresponsável, do representante do controlador de dados e do responsável pela proteção de dados.

b. As finalidades do processamento.

c. Uma descrição das categorias de titulares de dados e categorias de dados pessoais.

d. As categorias de destinatários para os quais os dados pessoais são divulgados, incluindo destinatários em países terceiros.

e. Quando aplicável, transferências de dados pessoais para um terceiro país, incluindo a identificação desse terceiro país ou organização internacional e, no caso das transferências mencionadas no parágrafo 3.11.

f. Os prazos previstos para a exclusão das diferentes categorias de dados.

g. Descrição das medidas técnicas e organizacionais implementadas para proteger os dados pessoais.

h. A identificação de processadores, tanto internos quanto externos.

O Registro de Atividades de Processamento do Processador inclui todas as categorias de atividades de processamento realizadas em nome do Controlador, contendo:

a. O nome e os detalhes de contato do(s) processador(es) e de cada controlador em cujo nome o processador está agindo e, quando aplicável, do representante do controlador ou do processador e do responsável pela proteção de dados.

b. As categorias de operações de processamento realizadas em nome de cada controlador.

c. Transferências internacionais de dados pessoais para um terceiro país ou organização internacional, incluindo a identificação desse terceiro país ou organização internacional e, no caso das transferências mencionadas no parágrafo 3.11, a documentação das proteções adequadas.

d. Uma descrição geral das medidas de segurança técnicas e organizacionais apropriadas em vigor.

O Registro de Atividades de Processamento deve ser revisado pelo menos anualmente e, em qualquer caso, sempre que houver uma alteração significativa em qualquer uma das atividades de processamento.

Não serão realizadas atividades de processamento que possam comprometer os direitos e as liberdades dos titulares dos dados. Para esses fins, e de acordo com o GDPR, será realizada uma análise objetiva dos riscos de cada operação de processamento, conforme descrito na cláusula a seguir.

3.13. AVALIAÇÃO OBJETIVA DO RISCO À PRIVACIDADE E AVALIAÇÃO DO IMPACTO DA PROTEÇÃO DE DADOS (DPAA)

As atividades de processamento que se enquadram no escopo dessas DPCs devem estar sujeitas a uma avaliação objetiva do risco à privacidade. Nos casos em que for identificado um alto risco para os direitos e liberdades dos titulares dos dados, deverá ser realizada uma Avaliação de Impacto sobre a Proteção de Dados (doravante denominada "**DPIA**"). Caso a DPIA mostre que o processamento envolve um alto risco e o controlador não tome medidas para mitigar esse risco, a autoridade supervisora deverá ser consultada antes que o processamento seja realizado.

A DPIA consiste em uma análise mais abrangente dos riscos associados a uma atividade de processamento, que permite a identificação de medidas de mitigação de riscos, por meio de

a. Avaliação de ameaças e vulnerabilidades, tanto legais quanto tecnológicas, incluindo sua probabilidade e impacto potencial;

b. Obtenção do risco inerente;

c. Avaliação do grau de maturidade das salvaguardas;

d. Obtenção do risco residual;

e. Implementação do Plano de Ação.

3.14. PROTEÇÃO DE DADOS POR PROJETO E POR PADRÃO

O Controlador, tanto no momento de determinar os meios de processamento quanto no momento do processamento em si, implementa medidas técnicas e organizacionais apropriadas para cumprir os requisitos do GDPR e da NCV e para proteger os direitos e liberdades dos titulares dos dados.

O Controlador deverá implementar medidas técnicas e organizacionais adequadas para garantir que, por padrão, somente os dados pessoais necessários para os fins específicos do processamento sejam processados.

Antes de iniciar uma nova operação de tratamento ou modificar uma já existente, devem ser analisados os requisitos legais e técnicos exigíveis e necessários para determinar se a operação de tratamento do Grupo Iberdrola é viável de acordo com o RGPD, seguindo o procedimento interno do Grupo Iberdrola denominado Procedimento para garantir a proteção de dados desde a concepção e por padrão.

4. DIREITOS DAS PARTES INTERESSADAS

Com relação ao processamento de dados pessoais, as empresas do Grupo garantem os seguintes direitos irrenunciáveis aos titulares dos dados:

a. Direito de acesso, que envolve o fornecimento de informações sobre dados pessoais mantidos sobre um titular de dados.

b. Direito de retificação, em virtude do qual o titular dos dados pode exigir a retificação de dados pessoais imprecisos ou incompletos.

c. O direito de apagar ou "direito de ser esquecido", pelo qual o titular dos dados pode exigir que seus dados pessoais sejam apagados quando as circunstâncias previstas no GDPR forem atendidas.

d. O direito à limitação do processamento, em virtude do qual o titular dos dados pode solicitar a limitação do processamento de seus dados pessoais, quando as circunstâncias previstas no GDPR forem atendidas.

e. O direito à portabilidade de dados, por meio do qual o titular dos dados pode receber dados pessoais relacionados a ele que tenha fornecido a um controlador de dados, em um formato estruturado, e transmiti-los a outro controlador de dados.

f. O direito de objeção, pelo qual o titular dos dados pode se opor ao processamento de seus dados pessoais para uma finalidade específica.

g. O direito de não estar sujeito a uma decisão baseada exclusivamente em processamento automatizado, incluindo a criação de perfis, que produza efeitos legais sobre os titulares dos dados ou que os afete significativamente de forma semelhante.

h. O direito de ser notificado sobre o status e o resultado da solicitação de retificação, exclusão ou restrição de processamento.

As Empresas do Grupo somente tomarão decisões baseadas em processamento automatizado, incluindo a criação de perfis, que produzam efeitos legais sobre o titular dos dados ou que o afetem significativamente, se uma das seguintes condições for atendida:

- É necessário para a conclusão ou execução de um contrato entre o titular dos dados e uma Empresa do Grupo que atue como Controladora de Dados.
- Ela é autorizada pelos regulamentos aplicáveis ao Controlador e medidas apropriadas são implementadas para proteger os direitos e liberdades e os interesses legítimos do titular dos dados.
- Ele se baseia no consentimento explícito do titular dos dados.

No primeiro e no terceiro casos, o titular dos dados terá, no mínimo, o direito de obter intervenção humana do Controlador, de declarar o que considera apropriado e de contestar a decisão.

O exercício dos direitos acima mencionados deve ser realizado de acordo com as disposições dos regulamentos de proteção de dados aplicáveis e, em qualquer caso, de acordo com as disposições do GDPR.

5. DIREITOS DE TERCEIROS BENEFICIÁRIOS

As Empresas do Grupo garantirão aos titulares dos dados o exercício dos direitos de aplicar estas NCV como terceiros beneficiários. Os titulares dos dados poderão invocar os direitos previstos nos parágrafos 3, 4, 7, 10, 11, 12 e 13 destas NCV, aos quais têm direito como terceiros beneficiários em relação ao processamento de seus dados, nos termos previstos neste parágrafo. Os titulares dos dados também têm o direito de ter acesso fácil à presente NCV.

Os titulares de dados cujos dados pessoais são coletados e/ou processados no EEE por uma Empresa do Grupo (Exportador) e transferidos para uma Empresa do Grupo fora do EEE (Importador) terão o direito de exigir o cumprimento das presentes NCV como terceiros beneficiários.

Para esse fim:

- **Eles podem apresentar uma reclamação à autoridade supervisora competente** (à sua escolha, a autoridade supervisora do país de residência, do país do local de trabalho ou do local da suposta infração) **e ao tribunal competente do EEE** (à sua escolha, aqueles do país do EEE no qual a Empresa do Grupo tem um estabelecimento ou aqueles do país no qual o titular dos dados tem sua residência). Os titulares dos dados também podem ser representados por uma entidade, organização ou associação sem fins lucrativos nas condições estabelecidas no Artigo 80(1) do GDPR.
- No caso de a Empresa do Grupo que alegadamente violou as NCVs estar estabelecida fora do E.E.E., a parte interessada poderá, nos termos previstos na seção anterior, **exercer os seus direitos e apresentar as suas reclamações**, de acordo com o regime de responsabilidade definido na seção 12 destas NCVs, contra a Empresa do Grupo que assume a responsabilidade em caso de violação das NCVs pela Empresa do Grupo domiciliada fora do E.E.E., a qual será considerada responsável pela violação. Para esses fins, a violação será considerada como tendo ocorrido no domicílio da Empresa do Grupo que assume a responsabilidade.

- Da mesma forma, a Empresa do Grupo que, de acordo com o esquema de responsabilidade definido no parágrafo 12 destes CSV, assumir a responsabilidade em caso de violação dos CSV pela Empresa do Grupo domiciliada fora do EEE, assumirá a **responsabilidade civil por danos sofridos por qualquer parte interessada** pela violação destes CSV pela Empresa do Grupo ou outra empresa importadora de dados, desde que tal responsabilidade tenha sido declarada por um tribunal ou outra autoridade competente.

Para identificar a empresa à qual o titular dos dados deve dirigir sua reclamação e que é responsável por uma violação das NCVs, o titular dos dados deve entrar em contato com o Coordenador de Proteção de Dados de Segurança Corporativa Global, cujos detalhes de contato são: dpo@iberdrola.com, que fornecerá ao titular dos dados informações sobre a Empresa Responsável.

Para os fins acima, essas NCVs estão constantemente disponíveis e são facilmente acessíveis às partes interessadas por meio de sua publicação no site www.iberdrola.com.

6. TREINAMENTO

As Empresas do Grupo devem promover, atualizar e fornecer a todos os seus funcionários programas de treinamento específicos sobre os princípios de proteção de dados pessoais e, especificamente, sobre essas NCVs e as consequências da não conformidade.

Todos os funcionários do Grupo devem concluir as atividades de treinamento anualmente e passar por um teste de avaliação.

Deve ser fornecido treinamento específico aos funcionários que tenham acesso permanente ou regular a dados pessoais ou que estejam envolvidos na coleta de dados pessoais ou no desenvolvimento de ferramentas usadas para processar dados pessoais.

O Anexo II das LCAs inclui requisitos sobre o treinamento dos funcionários do Grupo sobre proteção de dados pessoais e, especialmente, sobre as LCAs como um mecanismo de transferência entre as empresas do Grupo.

7. GERENCIAMENTO DE RECLAMAÇÕES

Os titulares dos dados podem, a qualquer momento, entrar em contato com o Coordenador de Proteção de Dados de Segurança Corporativa Global, que é responsável pelo tratamento e processamento de reclamações sobre a não conformidade de uma Empresa do Grupo com as NCV e que é independente no exercício de suas funções. As empresas do Grupo devem cumprir o Procedimento de Reclamações incluído no Anexo III da NCV.

Depois que uma reclamação for apresentada, o recebimento da reclamação deverá ser confirmado. A reclamação deverá ser resolvida em um mês após o recebimento. Esse período pode ser estendido até um máximo de dois meses, tendo em vista a complexidade e o número de solicitações recebidas.

No caso de uma reclamação desencadear uma investigação pela autoridade supervisora competente, a empresa do Grupo em questão deverá cumprir a decisão tomada.

8. PROGRAMA DE AUDITORIA E MONITORAMENTO

O programa de auditoria de privacidade das Empresas do Grupo inclui expressamente a verificação do cumprimento dessas NCVs, sendo os mecanismos de verificação definidos no procedimento interno do Grupo Iberdrola denominado Modelo de evaluación de cumplimiento del RGPD. O Procedimento de Auditoria de RSC está incluído no Anexo IV.

O Coordenador de Proteção de Dados de Segurança Corporativa Global determina o escopo da auditoria das NCVs, que inclui todos os aspectos das NCVs, bem como a designação do pessoal interno responsável pela realização da auditoria e os métodos para garantir que as ações corretivas sejam executadas.

A auditoria das NCVs pode ser realizada internamente ou por meio de uma auditoria externa. O relatório de auditoria deve ser levado ao conhecimento dos Conselhos de Administração das empresas do Grupo que assumem a responsabilidade em caso de não conformidade com as NCVs, do Coordenador Local de Proteção de Dados de Segurança Corporativa e do Coordenador Global de Proteção de Dados de Segurança Corporativa, especificando medidas corretivas, recomendações e um prazo para sua implementação.

A auditoria dos LCIs é realizada anualmente. Os Conselhos de Administração das empresas do Grupo que assumem a responsabilidade em caso de não conformidade com os LCIs também podem solicitar uma auditoria dos LCIs.

A Iberdrola fornecerá, por meio do Coordenador Global de Proteção de Dados de Segurança Corporativa, acesso aos resultados da auditoria dos NCVs à Autoridade Europeia de Proteção de Dados competente, mediante solicitação. As Autoridades Europeias de Proteção de Dados competentes poderão realizar uma auditoria de proteção de dados de qualquer membro dos NCVs se considerarem apropriado fazê-lo.

As empresas do Grupo devem ajustar suas ações às recomendações que as autoridades de proteção de dados possam fazer com relação ao escopo e à conformidade com essas NCVs.

9. CONFORMIDADE

O Coordenador Global de Proteção de Dados de Segurança Corporativa é responsável por supervisionar e garantir que as Empresas do Grupo cumpram as NCVs de forma coordenada e seguindo critérios interpretativos comuns, com a ajuda dos profissionais que compõem a equipe de Privacidade do Grupo Iberdrola.

As empresas do Grupo assumem as seguintes obrigações:

- Não fazer nenhuma transferência de dados para outra empresa do Grupo, a menos que essa empresa adira à NCV e tenha mecanismos para garantir a conformidade.
- Ao atuar como importador de dados, informar o exportador de dados o mais rápido possível caso, por qualquer motivo, incluindo as situações descritas no parágrafo 11, não possa cumprir as CSVs.

- Ao atuar como exportador de dados, suspender a transferência de dados caso o importador de dados não cumpra ou seja incapaz de cumprir as NCVs.
- Ao atuar como importador de dados, a critério do exportador, excluir ou devolver os dados pessoais transferidos ou quaisquer cópias deles quando:
  - o exportador de dados tiver suspendido a transferência e a conformidade com o CSV não puder ser restabelecida em um prazo razoável e, em qualquer caso, dentro de um mês após a suspensão;
  - o importador de dados estiver violando substancialmente ou repetidamente o CSV; ou
  - o Importador de dados não cumprir uma decisão vinculante de um tribunal ou autoridade supervisora com relação às obrigações previstas nas NCVs.

  O importador de dados deverá certificar ao exportador de dados a exclusão dos dados pessoais. Até que tal medida seja tomada, o Importador de dados deverá continuar a garantir a conformidade com a NCV. Caso as leis locais aplicáveis ao Importador de dados proíbam a devolução ou o descarte dos dados pessoais recebidos, o Importador de dados deverá continuar a cumprir o LCS e deverá processar os dados somente na medida permitida pela lei local.

O Anexo V contém informações sobre a estrutura operacional, os mecanismos de coordenação e as responsabilidades da equipe de Privacidade do Grupo Iberdrola, que garante o cumprimento da proteção de dados pessoais em todo o Grupo e a ausência de conflitos de interesse no desempenho de suas funções.

10. ASSISTÊNCIA MÚTUA E COOPERAÇÃO COM AS AUTORIDADES DE PROTEÇÃO DE DADOS

As empresas do Grupo comprometem-se a cooperar e auxiliar umas às outras em caso de reclamações de um titular de dados ou de investigações e inquéritos das autoridades de supervisão em relação a violações das NCVs.

As Empresas do Grupo também se comprometem a cooperar com as Autoridades de Proteção de Dados competentes, dentro do escopo de aplicação das LCAs, e responderão às solicitações feitas por essas Autoridades em relação às LCAs na forma correspondente e dentro do prazo correspondente e cumprirão as decisões e recomendações feitas por essas Autoridades. Para esse fim, deverão seguir o Procedimento para cooperação com as autoridades de supervisão, conforme estabelecido no Anexo VI.

As Empresas do Grupo concordam em se submeter a auditorias de proteção de dados realizadas pelas Autoridades de Proteção de Dados.

Qualquer controvérsia relacionada ao exercício dos poderes da autoridade supervisora em relação à supervisão e execução dos NCVs será resolvida pelos tribunais do Estado-Membro ao qual pertence a autoridade supervisora em questão, de acordo com as leis processuais desse Estado-Membro. As Empresas do Grupo concordam em se submeter à jurisdição de tais tribunais.

11. RELAÇÃO ENTRE CVNS E REGULAMENTOS LEGAIS LOCAIS

As Empresas do Grupo devem cumprir as regulamentações locais de proteção de dados aplicáveis, sem prejuízo da observância destas NCV, na medida em que as NCV ofereçam um nível de proteção mais elevado do que as regulamentações locais. Em todos os assuntos cobertos por estas LSAs em que a lei local aplicável preveja um nível mais alto de proteção, a lei local deverá ser aplicada.

- Avaliação do impacto da devolução: regulamentos e práticas de países terceiros

As Empresas do Grupo usarão as NCV como uma ferramenta para transferências internacionais de dados somente após avaliar que as regulamentações e práticas locais do país de destino aplicáveis ao processamento dos dados, incluindo quaisquer requisitos de divulgação de dados ou qualquer autorização de acesso aos dados por autoridades públicas, não impedem o cumprimento das obrigações do Importador de Dados conforme estabelecido nas NCV.

Em particular, as Empresas do Grupo avaliarão se as leis e práticas locais do país de destino respeitam essencialmente os direitos e as liberdades fundamentais e se as medidas legislativas previstas são necessárias e proporcionais em uma sociedade democrática para proteger os interesses legais do Artigo 23(1) do GDPR.

Ao avaliar as regulamentações e práticas locais no país terceiro, que podem ter implicações para o cumprimento das obrigações e compromissos estabelecidos no LQRS, as empresas do Grupo devem levar em conta:

- As circunstâncias específicas da transferência ou do conjunto de transferências e transferências posteriores previstas dentro do país terceiro ou para outro país terceiro, incluindo as finalidades da transferência, o tipo de entidades envolvidas, o setor econômico afetado pela transferência, as categorias e o formato dos dados pessoais transferidos, o local de processamento e armazenamento e os canais de transmissão utilizados.
- As leis e práticas locais relevantes do país terceiro, levando em consideração as circunstâncias da transferência, incluindo aquelas que preveem a divulgação de dados a autoridades públicas ou que autorizam seu acesso, bem como aquelas que regulam o acesso aos Dados Pessoais durante a transmissão entre o país do Exportador de Dados e o Importador de Dados, juntamente com quaisquer limitações e proteções aplicáveis.
- Quaisquer salvaguardas contratuais, técnicas ou organizacionais implementadas para complementar as salvaguardas dos NCVs, incluindo medidas implementadas durante a transmissão e o processamento dos Dados Pessoais no país de destino.

Caso as Empresas do Grupo decidam adotar proteções adicionais àquelas contidas nas NCV, elas deverão informar o Coordenador de Proteção de Dados de Segurança Corporativa Global e envolvê-lo na avaliação feita.

As Empresas do Grupo devem documentar as avaliações das regulamentações e práticas do país de destino, bem como as salvaguardas adicionais adotadas e implementadas. Essas evidências devem ser disponibilizadas para a autoridade supervisora competente.

Caso o Importador de Dados esteja sujeito, ou tenha motivos para acreditar que esteja sujeito, a regulamentos ou práticas, incluindo alterações legislativas de terceiros países ou solicitações de acesso a dados, que impeçam ou possam impedir o cumprimento das NCVs, ele deverá notificar o Exportador de Dados e as Empresas do Grupo sobre esse fato.

Após a análise da notificação acima, o Exportador de dados, juntamente com o Coordenador de proteção de dados de segurança corporativa global, identificará medidas técnicas ou organizacionais adicionais para garantir a segurança e a confidencialidade dos dados. Essas medidas deverão ser implementadas pelo Exportador de dados e/ou Importador de dados. O mesmo deverá se aplicar se uma Empresa do Grupo atuando como Exportador de Dados tiver motivos para acreditar que outra Empresa do Grupo atuando como Importador de Dados não possa cumprir as NCV.

No entanto, se o Exportador de Dados, juntamente com o Coordenador de Proteção de Dados de Segurança Corporativa Global, determinar que as CSVs, mesmo que medidas adicionais tenham sido implementadas, não podem ser cumpridas para uma determinada transferência ou conjunto de transferências, ou se assim for considerado pelas Autoridades de Supervisão competentes, a transferência ou conjunto de transferências em questão, bem como todas as transferências para as quais a avaliação e o raciocínio conduzidos levariam a uma conclusão semelhante, serão suspensos até que a conformidade com as CSVs seja novamente assegurada ou a transferência seja encerrada.

Caso tenha se passado um mês desde a suspensão da transferência sem que tenha sido possível retomar a transferência sem garantir a conformidade com as NCV, o exportador de dados encerrará a transferência ou o conjunto de transferências. Os dados pessoais que tenham sido transferidos antes de tal suspensão, e quaisquer cópias dos mesmos, deverão ser devolvidos em sua totalidade ao Exportador de Dados aderindo ao CSV ou destruídos, a critério do Exportador de Dados.

O Coordenador Global de Proteção de Dados de Segurança Corporativa informará todas as Empresas do Grupo sobre a avaliação de impacto da transferência realizada e seus resultados, para que quaisquer salvaguardas ou medidas adicionais tomadas possam ser aplicadas a transferências semelhantes ou, caso, embora medidas adicionais tenham sido tomadas, a transferência não esteja em conformidade com as NCVs, a transferência seja suspensa ou encerrada.

Por fim, o exportador de dados, em cooperação com outros importadores, se necessário, realizará um monitoramento contínuo para detectar quaisquer desenvolvimentos nos países terceiros para os quais os dados são transferidos, que possam influenciar o resultado da avaliação inicial do impacto da transferência.

- Conflito regulatório:

Em caso de conflito entre a legislação local aplicável e estas CSVs, de modo que a última não possa ser adequadamente cumprida ou tenha um efeito material sobre as proteções previstas nestas CSVs, a Empresa do Grupo afetada deverá informar o Coordenador de Proteção de Dados de Segurança Corporativa Global assim que tomar conhecimento de tal conflito.

O Coordenador de Proteção de Dados de Segurança Corporativa Global deverá, após o recebimento da comunicação apropriada, registrar o conflito e informar imediatamente a Empresa Responsável e as Empresas do Grupo que tenham transferido dados anteriormente para a Empresa do Grupo que esteja levantando o conflito.

O Coordenador Local de Proteção de Dados de Segurança Corporativa levará a disputa ao conhecimento da Autoridade Supervisora da E.E.E. competente e, juntamente com a Empresa do Grupo em questão, promoverá a solução mais compatível com os princípios do GDPR.

Quando o conflito surgir com as regulamentações aplicáveis de um terceiro país, ele deverá ser levado ao conhecimento da autoridade supervisora competente da E.E.E. No caso de a empresa ter sido solicitada a divulgar dados, a comunicação deverá incluir informações sobre os dados solicitados, o órgão solicitante e a base legal para a divulgação.

Caso a notificação à Autoridade Supervisora da E.E.E. competente seja proibida, a Empresa do Grupo solicitada envidará seus melhores esforços para superar tal proibição e demonstrará que o fez. Se, mesmo assim, a Empresa do Grupo solicitada não puder notificar a Autoridade de Supervisão da União Europeia competente, a Empresa do Grupo solicitada se comprometerá a fornecer informações gerais sobre as solicitações recebidas anualmente.

As transferências de dados pessoais de uma Empresa do Grupo para qualquer Autoridade Pública não podem ser maciças, desproporcionais e indiscriminadas.

12. RESPONSABILIDADE

Com relação à responsabilidade, o Grupo Iberdrola designa as seguintes empresas do Grupo como empresas responsáveis ("**Empresas Responsáveis**") que concordam em assumir a responsabilidade por qualquer violação das NCVs por qualquer uma das empresas do Grupo domiciliadas fora do EEE:

- Iberdrola España, S.A. (Sociedade Unipessoal), que assumirá a responsabilidade por qualquer violação da NCV quando a entidade exportadora dos dados for qualquer empresa domiciliada na Espanha que seja uma filial da Iberdrola España, S.A. (Sociedade Unipessoal). Da mesma forma, a Iberdrola España, S.A. (Sociedade Unipessoal) assumirá a responsabilidade por qualquer violação da NCV quando a entidade exportadora dos dados for a Iberdrola S.A., e qualquer entidade de propriedade direta ou indireta da Iberdrola, S.A. que não seja subsidiária de nenhuma das empresas indicadas nos parágrafos seguintes como Empresas Responsáveis.
- Iberdrola Participaciones, S.A. (Sociedad Unipersonal), que assumirá a responsabilidade por qualquer violação das NCVs quando a entidade que exportar os dados for uma subsidiária da empresa localizada em qualquer país da E.E.E.E.
- Iberdrola Energía Internacional, S.A. (Sociedad Unipersonal), que assumirá a responsabilidade por qualquer violação das NCVs quando a entidade que exportar os dados for qualquer uma de suas subsidiárias localizadas em qualquer país da E.E.E.

Sociedade responsável	Entidade exportadora
Iberdrola España, S.A.(1)	Empresa do Grupo dependente da Iberdrola España, S.A. e localizada na Espanha (*)
	Iberdrola, S.A.
	Qualquer empresa do Grupo, de propriedade direta ou indireta da Iberdrola, S.A., que não dependa de nenhuma das empresas (2) ou (3) (*)
Iberdrola Participaciones, S.A.(2)	Empresa do grupo dependente da Iberdrola Participaciones e localizada em qualquer país da E.E.E. S.A. (*)
Iberdrola Energía Internacional, S.A.(3)	Empresa do Grupo dependente da Iberdrola Energía Internacional, S.L. e localizada em qualquer país da E.E.E.E. S.A. (*)

(*) O Anexo I contém as empresas do Grupo que aderiram às NCVs, agrupadas pelas empresas do Grupo que as controlam direta ou indiretamente.

Em qualquer caso, as reclamações sobre o descumprimento da NCV por parte de uma Empresa do Grupo poderão ser apresentadas pelo titular dos dados por escrito ao Coordenador Global de Proteção de Dados de Segurança Corporativa, cujos dados de contato são: dpo@iberdrola.com, ou à Iberdrola - Calle Tomás Redondo 1 Madrid -28033- Espanha, conforme descrito no Anexo III - Procedimento de tratamento de reclamações.

As empresas responsáveis aceitam:

- Que a pessoa em questão terá os direitos e recursos contra eles perante os tribunais com jurisdição ou outras autoridades competentes da UE com jurisdição de acordo com o parágrafo 5 destas NCVs, como se a violação tivesse sido causada por eles no Estado Membro em que estão sediados, e não pela Empresa do Grupo não pertencente à UE que os violou.
- Que pagarão indenização por quaisquer danos materiais ou imateriais resultantes da violação das NCVs pelas Empresas do Grupo.
- Que eles terão o ônus da prova para demonstrar que a Empresa do Grupo que não seja da E.E.E.E. não é responsável por qualquer violação das regras da qual tenha surgido uma reivindicação de danos por uma parte interessada.
- Concordar em tomar as medidas necessárias para remediar violações das NCVs de outras empresas do Grupo.

13. ATUALIZAÇÃO E EMENDAS AO CCNS

A modificação e/ou atualização dessas NCVs será realizada de acordo com as disposições do Procedimento de Atualização das Normas Corporativas Vinculantes incluído como Anexo VII, que estabelece o processo de aprovação das alterações das NCVs, a forma de comunicação das alterações às Autoridades de Proteção de Dados, às Empresas do Grupo e aos titulares dos dados. Além disso, o Grupo Iberdrola prevê a atualização anual do Marco de Segurança Cibernética do Grupo Iberdrola e dos procedimentos internos mencionados nessas NCVs.

14. RESCISÃO DE NCVS

Em caso de rescisão do GI, as obrigações relativas aos direitos dos terceiros beneficiários, em relação a quaisquer dados pessoais dentro do escopo destas RAG que tenham sido transferidos da E.E.E. antes da data efetiva da rescisão, continuarão a ser aplicadas.

No caso de uma Empresa do Grupo, como Importador de Dados, deixar de fazer parte das NCVs, ela deverá excluir ou devolver os Dados Pessoais recebidos no âmbito das NCVs. No entanto, se o Exportador de Dados e o Importador de Dados concordarem que o Importador de Dados poderá reter os dados pessoais, as disposições do Capítulo V do GDPR deverão ser observadas.

15. CONTATO

Os titulares dos dados podem encaminhar quaisquer perguntas sobre essas NCVs, seus direitos sob essas NCVs ou quaisquer outras questões de proteção de dados pessoais ao Coordenador Global de Proteção de Dados de Segurança Corporativa, cujos detalhes de contato são: dpo@iberdrola.com.

Se os titulares dos dados não estiverem satisfeitos com o processamento de seus dados pessoais pelas Empresas do Grupo, deverá ser utilizado o Procedimento de Reclamações incluído no Anexo III.

ANEXOS

ANEXO I – LISTA DE EMPRESAS QUE SE ENQUADRAM NO ESCOPO DAS REGRAS CORPORATIVAS OBRIGATÓRIAS

A lista de empresas do grupo Iberdrola relacionadas por essas NCVs está disponível no site da Iberdrola (www.Iberdrola.com). A primeira coluna reflete o nome de cada empresa e, em negrito, as empresas que controlam direta ou indiretamente as empresas listadas abaixo de cada uma delas. A segunda coluna reflete a sede registrada de cada empresa.

ANEXO II - TREINAMENTO SOBRE PROTEÇÃO DE DADOS PESSOAIS

Este documento inclui informações sobre o treinamento de funcionários do Grupo Iberdrola ("**Grupo**") sobre proteção de dados pessoais e, especificamente, sobre as NCVs como um mecanismo para a transferência de dados pessoais entre as empresas do Grupo.

O Coordenador Global de Proteção de Dados de Segurança Corporativa é o responsável por definir as necessidades de treinamento em proteção de dados do Grupo Iberdrola e, portanto, definirá o alcance e o conteúdo do mesmo para garantir a correta divulgação dos direitos, responsabilidades e obrigações dos funcionários da Iberdrola nessa área. Os departamentos de Formação e Desenvolvimento de Recursos Humanos de cada país são responsáveis, dentro do Grupo Iberdrola, pela elaboração e acompanhamento dos planos de formação do quadro de pessoal do Grupo, que inclui a formação em matéria de proteção de dados pessoais. As atividades de formação são aprovadas pelo Comitê de Qualidade da Formação de cada país, sendo a aprovação devidamente registrada no Plano de Formação anual, aprovado pela Direção de Recursos Humanos de cada país e comunicado, se for o caso, aos representantes corporativos da empresa.

Cada Departamento de Treinamento e Desenvolvimento de Recursos Humanos garante a conformidade de todos os funcionários com o plano de treinamento e informa à respectiva gerência de Recursos Humanos sobre sua implementação efetiva.

Todos os funcionários do Grupo Iberdrola serão incluídos no programa de treinamento do Grupo sobre proteção de dados pessoais e NCV.

O treinamento deverá ser on-line e, em qualquer caso, deverá ser mantido um registro documental dos detalhes da atividade de treinamento realizada e um registro dos funcionários que participaram do treinamento. Para cada curso de treinamento, deverá ser realizado um teste sobre o conhecimento adquirido. Se o teste não for aprovado, outros testes deverão ser realizados até que o treinamento seja aprovado.

Portanto, deverá haver um registro do treinamento oferecido, com registro das datas de duração, datas de início e término, conteúdo do curso e os nomes dos participantes. Além disso, a última versão do curso deverá ser mantida na Intranet da Iberdrola.

De acordo com o exposto, o Grupo Iberdrola conta com um plano anual de treinamento em proteção de dados pessoais, elaborado com base nos riscos identificados na proteção de dados pessoais no setor, para todos os funcionários das Empresas do Grupo (dentro e fora do EEE). Por meio desse treinamento, são tomadas as medidas necessárias para garantir que os funcionários estejam cientes dos requisitos derivados dos regulamentos de proteção de dados pessoais e da NCV, em estrita conformidade com suas obrigações em relação ao treinamento de funcionários.

PLANO ANUAL DE TREINAMENTO EM PROTEÇÃO DE DADOS PESSOAIS

Treinamento geral sobre proteção de dados pessoais

Todos os funcionários das empresas do Grupo são obrigados a passar por um treinamento geral anual sobre proteção de dados pessoais. Além disso, os funcionários recebem treinamento sobre outros procedimentos e regras internos relacionados à proteção de dados pessoais em geral e à NCV em particular.

Os novos funcionários recebem treinamento geral sobre proteção de dados pessoais e treinamento e informações sobre as NCVs no início de seu relacionamento com a empresa do Grupo contratante.

O treinamento geral sobre proteção de dados pessoais abrange a estrutura jurídica nacional e internacional sobre proteção de dados pessoais, políticas internas de proteção de dados pessoais, protocolos, revisão de casos práticos e procedimentos obrigatórios de privacidade e segurança na Iberdrola.

O objetivo do curso de treinamento geral sobre proteção de dados pessoais é que todos os funcionários compreendam os princípios básicos de proteção de dados pessoais, confidencialidade e segurança da informação e as políticas e procedimentos de privacidade e segurança da informação da Iberdrola.

Treinamento em padrões corporativos obrigatórios

Todos os funcionários das empresas do Grupo devem concluir anualmente o programa de treinamento NCV da Iberdrola.

O treinamento NCV abrange:

1. Conceito
2. Normas Corporativas Vinculantes do Grupo Iberdrola
3. Eficácia, vinculação e consequências do não cumprimento

De acordo com as funções e responsabilidades dos funcionários, será oferecido treinamento específico sobre os protocolos de atualização, reclamações e auditoria das NCVs da Iberdrola.

ANEXO III – PROCEDIMENTO DE RECLAMAÇÕES

A seguir, apresentamos o procedimento para lidar com reclamações que um titular de dados possa apresentar ao Grupo Iberdrola em relação ao processamento de seus dados pessoais de acordo com a NCV.

Formulação da reivindicação

As reclamações por violação da NCV por uma Empresa do Grupo podem ser apresentadas pela pessoa afetada por escrito ao Coordenador Global de Proteção de Dados de Segurança Corporativa por e-mail para: dpo@iberdrola.com ou Iberdrola Calle Tomás Redondo 1, Madrid -28033- Espanha.

Gerenciamento de reclamações

O Coordenador Global de Proteção de Dados de Segurança Corporativa será responsável por responder às reclamações de não conformidade com as NCVs pelas Empresas do Grupo.

Após o envio de uma reclamação, o Coordenador Global de Proteção de Dados de Segurança Corporativa acusará o recebimento da reclamação e avaliará se os requisitos formais para admissão foram atendidos. Em seguida, ele entrará em contato com os Coordenadores Locais de Proteção de Dados de Segurança Corporativa relacionados, que serão responsáveis por fornecer as informações necessárias para resolver a reclamação.

O Coordenador de Proteção de Dados do Global Corporate Security coordenará a resposta ao titular dos dados. A reclamação deverá ser resolvida em um mês a partir de seu recebimento. Esse período poderá ser estendido até um máximo de dois meses, tendo em vista a complexidade e o número de solicitações recebidas. No entanto, o reclamante deverá ser informado e uma explicação deverá ser fornecida. A pessoa em questão será informada das consequências no caso de a reclamação ser rejeitada ou no caso de a reclamação ser justificada.

Os titulares dos dados podem, a qualquer momento, entrar em contato com o Coordenador Global de Proteção de Dados de Segurança Corporativa, que é competente para lidar e tratar de reclamações sobre a não conformidade com as NCVs por uma empresa do Grupo e que é independente no exercício de suas funções.

Outras vias de reclamação

O titular dos dados terá o direito de exigir o cumprimento dessas NCVs por meio de uma reclamação a uma Autoridade Supervisora ou por meio de uma ação perante os Tribunais, sem a necessidade de esgotar o procedimento interno de reclamação previsto na seção anterior. Para esses fins:

- Eles podem apresentar uma reclamação à autoridade supervisora competente (à sua escolha, a autoridade supervisora do EEE do seu país de residência, do país do local de trabalho ou do local da suposta infração) e ao tribunal do EEE competente (à sua escolha, os do país do EEE em que a empresa do Grupo tem um estabelecimento ou os do país em que a pessoa em questão tem sua residência).

  No caso de uma reclamação desencadear uma investigação pela autoridade supervisora competente, a empresa do Grupo em questão deverá cumprir a decisão tomada.
- No caso de a Empresa do Grupo que supostamente violou as NCVs estar estabelecida fora da E.E.E., a parte interessada poderá, nos termos estabelecidos na seção anterior, exercer seus direitos e apresentar suas reivindicações de acordo com o esquema de responsabilidade definido nas NCVs contra a Empresa do Grupo que assume a responsabilidade em caso de violação das NCVs por qualquer uma das Empresas do Grupo domiciliadas fora da E.E.E., a qual será considerada responsável pela violação. Para esses fins, a violação será considerada como tendo ocorrido no domicílio da Empresa do Grupo que assume a responsabilidade.
- Da mesma forma, a Empresa do Grupo que, de acordo com o esquema de responsabilidade definido nos CSVs, assumir a responsabilidade em caso de violação dos CSVs por qualquer uma das Empresas do Grupo domiciliadas fora da E.E.E., assumirá a responsabilidade civil por danos sofridos por qualquer parte interessada pela violação desses CSVs por qualquer Empresa do Grupo ou outra empresa importadora de dados, desde que tal responsabilidade tenha sido declarada por um tribunal ou outra autoridade competente.

Com relação à responsabilidade, o Grupo Iberdrola designa as seguintes empresas do Grupo como empresas responsáveis ("**Empresas Responsáveis**") que concordam em assumir a responsabilidade por qualquer violação das NCVs por qualquer uma das empresas do Grupo domiciliadas fora do EEE:

- Iberdrola España, S.A. (Sociedade Unipessoal), que assumirá a responsabilidade por qualquer violação da NCV quando a entidade exportadora dos dados for qualquer empresa domiciliada na Espanha sob seu controle. Da mesma forma, a Iberdrola España, S.A. (Sociedade Unipessoal) assumirá a responsabilidade por qualquer violação do NCV quando a entidade exportadora dos dados for a Iberdrola S.A., e qualquer entidade de propriedade direta ou indireta da Iberdrola, S.A. que não seja subsidiária de nenhuma das empresas indicadas nos parágrafos seguintes como Empresas Responsáveis.
- Iberdrola Participaciones, S.A. (Sociedad Unipersonal), que assumirá a responsabilidade por qualquer violação das NCVs quando a entidade que exportar os dados for uma subsidiária da empresa localizada em qualquer país da E.E.E.E.
- Iberdrola Energía Internacional, S.A. (Sociedad Unipersonal), que assumirá a responsabilidade por qualquer violação das NCVs quando a entidade que exportar os dados for qualquer uma de suas subsidiárias localizadas em qualquer país da E.E.E.

As empresas responsáveis aceitam:

- Que a pessoa em questão terá os direitos e recursos contra eles perante os tribunais com jurisdição ou outras autoridades competentes da UE com jurisdição de acordo com o parágrafo 5 das NCVs, como se a violação tivesse sido causada por eles no Estado Membro em que têm sua sede, e não pela Empresa do Grupo não pertencente à UE que os violou.
- Que pagarão indenização por quaisquer danos materiais ou imateriais resultantes da violação das NCVs pelas Empresas do Grupo.
- Que eles terão o ônus da prova para demonstrar que a Empresa do Grupo que não seja da E.E.E.E. não é responsável por qualquer violação das regras da qual tenha surgido uma reivindicação de danos por uma parte interessada.
- Concordar em tomar as medidas necessárias para remediar violações das NCVs de outras empresas do Grupo.

ANEXO IV – PROCEDIMENTO DE AUDITORIA DE CSV

O documento de procedimento interno do Grupo Iberdrola que estabelece claramente os mecanismos de verificação é o Modelo de avaliação do cumprimento - Regulamento Europeu de Proteção de Dados. Esse programa de verificação se baseia no modelo de conformidade do Grupo Iberdrola, que é aplicável a todas as empresas do Grupo incluídas no escopo de aplicação da NCV, e que se baseia em cinco pilares:

- Estrutura de governança;
- Metodologias e ferramentas: Registro de Atividades de Processamento, Análise de Risco e Avaliações de Impacto na Proteção de Dados (DPA);
- Procedimentos, padrões e diretrizes;
- Medidas de segurança;
- Avaliação e relatórios de conformidade

O programa de verificação envolve os responsáveis pela proteção de dados pessoais dos diferentes negócios e áreas corporativas, bem como os Coordenadores de Proteção de Dados globais e locais que compõem a Equipe de Privacidade do Grupo Iberdrola. Também participarão auditores internos e externos.

Auditores internos

O Coordenador Global de Proteção de Dados de Segurança Corporativa determinará o escopo da auditoria das CSVs, incluindo a identificação de todos os aspectos que devem ser avaliados para verificar a conformidade com as CSVs, bem como a frequência com que essa avaliação deve ser realizada, levando em consideração seu escopo. Da mesma forma, o Coordenador Global de Proteção de Dados de Segurança Corporativa designará o pessoal responsável por realizar as auditorias internamente, garantindo, em todo momento, a independência do pessoal designado para realizar a auditoria, bem como que esse pessoal tenha as habilidades e os conhecimentos técnicos necessários para realizar tais auditorias.

Auditores externos

A participação de auditores externos no procedimento de verificação da conformidade com as LCAs deve ser regida pelos seguintes princípios:

- Integridade: os auditores devem manter a honestidade, a imparcialidade e a objetividade em seu trabalho, evitando qualquer conflito de interesses que possa comprometer seu julgamento profissional.
- Competência e diligência profissional: os auditores devem demonstrar que possuem o conhecimento, as habilidades e a experiência necessários para realizar a auditoria com competência e diligência, de acordo com as normas técnicas e profissionais aplicáveis.
- Confidencialidade: os auditores respeitarão a confidencialidade das informações às quais tenham acesso durante o processo de auditoria, protegendo a privacidade das partes interessadas e os interesses legítimos do Grupo Iberdrola.
- Independência: os auditores devem manter a independência no exercício de sua função e evitar comprometer sua capacidade de fazer julgamentos imparciais e objetivos.
- Evidências suficientes: os auditores devem fundamentar suas conclusões com evidências suficientes para verificar a conformidade com o GDPR e, em particular, com as NCVs.
- Conformidade regulatória e padrões de qualidade: os auditores cumprirão rigorosamente as leis e os regulamentos aplicáveis e prestarão seus serviços de acordo com os mais altos padrões de qualidade.
- Comunicação clara e transparente: os auditores comunicarão de forma clara e transparente os resultados, conclusões e recomendações resultantes da auditoria, fornecendo informações relevantes e compreensíveis ao Grupo Iberdrola sobre o resultado da auditoria.
- Respeitar os direitos e as responsabilidades das partes interessadas: os auditores devem respeitar os direitos e as responsabilidades das partes interessadas.

Avaliação da conformidade

O sistema de avaliação de conformidade é estruturado com base nos pilares do modelo de conformidade de proteção de dados do Grupo Iberdrola.

Um dos principais elementos da Estrutura de Governança é a NCV, como um mecanismo para a transferência de dados pessoais entre as empresas do Grupo.

Sua avaliação analisará:

- Os instrumentos legais com poderes para tornar as LCAs obrigatórias em nível nacional.
- As garantias oferecidas pelas empresas do Grupo em relação aos direitos de terceiros beneficiários.
- Ações de cooperação e assistência entre as empresas do Grupo em caso de reclamações de um titular de dados ou investigações e inquéritos por autoridades de supervisão em relação a violações das NCVs.
- As ações de cooperação com as Autoridades de Proteção de Dados competentes e a resposta às solicitações feitas por essas Autoridades em relação às NCVs na forma e prazo correspondentes e a conformidade com as decisões e recomendações feitas por essas Autoridades.
- O tratamento de reclamações por não conformidade com as NCVs por uma das empresas do Grupo.
- O protocolo para atualização e alteração dos NCVs.
- A maneira pela qual as informações sobre os LQCs são fornecidas às partes interessadas.
- Conformidade com o plano de treinamento do NCV.
- Decisões tomadas em relação a requisitos obrigatórios de leis nacionais que entram em conflito com as CNVs.
- O texto do CSV será revisado para garantir o alinhamento com a Estrutura de Governança de Proteção de Dados.

Relatórios de proteção de dados

Trimestralmente, os indicadores de proteção de dados são relatados em nível local e global e contêm determinadas informações por empresa/área de negócios e país, por exemplo, em relação às NCVs:

- com a não conformidade com as NCVs;
- número de empresas que aderem às NCVs;
- Número de solicitações recebidas das autoridades de supervisão competentes com relação aos LQCs

Os relatórios para o Coordenador Global de Proteção de Dados de Segurança Corporativa e para os Conselhos de Administração das Empresas do Grupo que assumem a responsabilidade pela não conformidade com as NCVs e seu Coordenador Local de Proteção de Dados de Segurança Corporativa, juntamente com a identificação de possíveis riscos de proteção de dados, devem ser incluídos no Relatório de Riscos Principais.

ANEXO V - EQUIPE DE PRIVACIDADE DO GRUPO IBERDROLA

A seguir, é apresentada uma descrição da equipe de privacidade do Grupo Iberdrola, composta por profissionais de proteção de dados, cujo objetivo é cumprir com a proteção de dados pessoais de forma global no Grupo e, especificamente, com as NCVs.

Estrutura operacional global

Na Divisão de Segurança Corporativa do Grupo Iberdrola, foi nomeado um **Coordenador Global de Proteção de Dados de Segurança Corporativa (Coordenador Global)**, cujas responsabilidades são as seguintes:

- Propor e promover a atualização da Estrutura Global para a Proteção de Dados Pessoais (doravante denominada Estrutura Global de PDP) e dos padrões globais de proteção de dados.
- Definir o sistema global de gerenciamento de proteção de dados, que incluirá, entre outros, padrões e procedimentos globais de proteção de dados, bem como metodologias e ferramentas corporativas, e promover e supervisionar sua implementação no Grupo.
- Definir padrões globais de segurança aplicáveis à proteção de dados pessoais, tanto em processos de processamento interno quanto de terceiros.
- Fornecer aconselhamento, recomendações e esclarecimentos sobre o conteúdo de normas, metodologias e ferramentas, além de padrões globais e sobre a Estrutura Global de PDP.
- Estabelecer um sistema global de avaliação e coordenação de conformidade para avaliar os riscos de não conformidade e a eficácia da Política de Proteção de Dados e da Estrutura Global de PDP e informar o Comitê Global de Segurança Cibernética e o Escritório de Conformidade.
- Assumir o papel de interlocutor com a autoridade supervisora de Proteção de Dados para aspectos que afetam o Grupo como um todo, com o apoio dos serviços jurídicos.
- Coordenar as funções e tarefas dos Coordenadores de Proteção de Dados locais na Segurança Corporativa para promover a implementação das melhores práticas de proteção de dados e da estratégia global do Grupo.
- Cumprir com as funções do Delegado de Proteção de Dados estabelecidas no RGPD e reportar ao Conselho de Administração da Iberdrola, S.A.
- Monitorar e garantir o cumprimento das NCVs de forma coordenada e homogênea, com o apoio dos Coordenadores de Proteção de Dados globais e locais do Grupo Iberdrola.

A Diretoria de Segurança Corporativa conta com a assistência de um **Coordenador Global de Proteção de Dados dos Serviços Jurídicos**, que fornecerá suporte na definição da estrutura de governança global e na análise e definição de regulamentos e contratos em relação à transferência de Dados Pessoais intragrupo, bem como no desenvolvimento do restante de suas funções.

Além disso, os negócios e as áreas corporativas mais relevantes nomearam um **Coordenador Global de Proteção de Dados Pessoais** com o objetivo de garantir o alinhamento dos sistemas de gerenciamento de proteção de dados em sua área de responsabilidade com os padrões corporativos e a conformidade com as leis e outros regulamentos aplicáveis, como, por exemplo e quando aplicável, garantir a existência de um Registro de Atividades de Processamento, avaliações de risco de privacidade, sistema de notificação de incidentes etc., e servir como um canal de comunicação e suporte com tal negócio ou área no nível de subholding e de head of business, permitindo assim a implementação da estratégia **global em todas as Empresas do Grupo** e o compartilhamento das melhores práticas nessa área. e servir como um canal de diálogo e apoio com esse negócio ou área em nível de subholding e de matriz, possibilitando assim a implementação da estratégia global em todas as empresas do Grupo e o compartilhamento das melhores práticas nessa área.

Os vários coordenadores mencionados acima fazem parte do **Comitê Global de Segurança Cibernética**, criado de acordo com a Política de Risco de Segurança Cibernética, cuja função é supervisionar o estado geral da Segurança Cibernética e da proteção de Dados Pessoais no Grupo, facilitar sua coordenação e auxiliar a Gerência de Segurança Corporativa na implementação das medidas aprovadas por esta última, tudo de acordo com os termos estabelecidos em seus Regulamentos internos.

Estrutura operacional empresas subholding

As Divisões de Segurança Corporativa de cada uma das empresas subholding do país nomeiam um **Coordenador de Proteção de Dados de Segurança Corporativa Local** para garantir a implementação da estratégia global de proteção de dados pessoais em seu país, levando em conta as particularidades de seu território.

O Coordenador de Proteção de Dados de Segurança Corporativa Local das Empresas do Grupo é responsável pela proteção de dados em nível local, cumprindo os deveres do Diretor de Proteção de Dados estabelecidos no GDPR e reportando-se ao Conselho de Administração da empresa subholding do país relevante.

Nesse sentido, o Coordenador Local de Proteção de Dados de Segurança Corporativa deverá garantir que haja um nível adequado de coordenação com o Coordenador Global de Proteção de Dados, em relação às questões de questões relevantes de proteção de dados, incluindo iniciativas importantes, indicadores de risco e incidentes de proteção de dados.

Da mesma forma, as divisões de Segurança Corporativa das empresas subholding dos países devem garantir a implementação local da estratégia global de proteção de dados pessoais, bem como a conformidade com as regras e regulamentos aplicáveis, garantindo também a coordenação entre as diferentes áreas de negócios e corporativas.

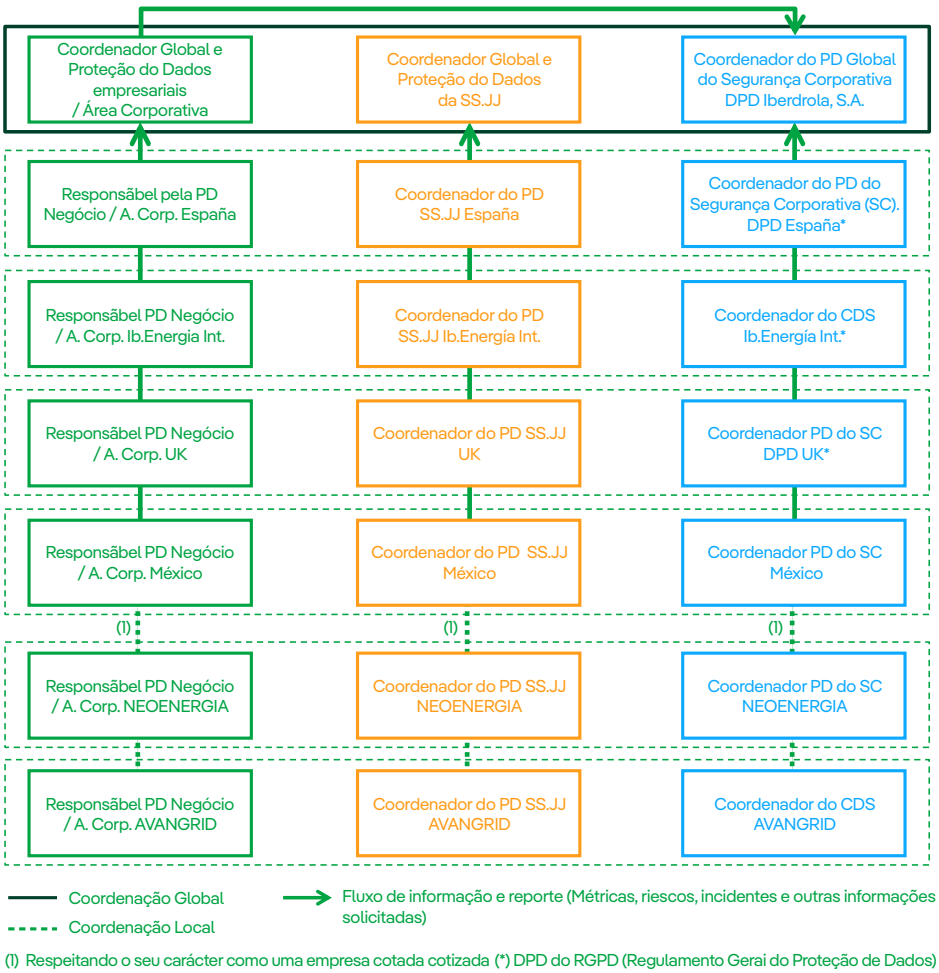
Essas Divisões de Segurança Corporativa criaram grupos locais de coordenação de Proteção de Dados para auxiliar o Coordenador Local de Proteção de Dados de Segurança Corporativa no desempenho de suas funções. Para esse fim, as empresas subholding dos países também têm um **Coordenador Local de Proteção de Dados dos Serviços Jurídicos** e seus respectivos **Diretores Locais de Proteção de Dados nos negócios e áreas corporativas relevantes**, que assumem as funções correspondentes e coordenam com sua contraparte global. Esses grupos de coordenação local se reúnem regularmente para tomar as medidas necessárias para garantir a implementação local das diretrizes e dos padrões globais de proteção de dados.

Mecanismos de coordenação

Para garantir a coordenação adequada entre as empresas do Grupo, de acordo com a estrutura corporativa do Grupo, foram estabelecidos os seguintes mecanismos:

- **Coordenação operacional em nível local** entre os Diretores Locais de Proteção de Dados das Áreas de Negócios ou Corporativas, o Coordenador Local de Serviços Jurídicos e o Coordenador Local de Proteção de Dados de Segurança Corporativa, por meio do grupo local de coordenação de proteção de dados.
- **Coordenação operacional em nível global** entre os Coordenadores Globais de Proteção de Dados para Áreas de Negócios e Corporativas, o Coordenador Global de Proteção de Dados para Serviços Jurídicos e o Coordenador Global de Proteção de Dados para Segurança Corporativa, por meio do Comitê Global de Segurança Cibernética.
- **Coordenação operacional no nível da área de negócios ou corporativa**: os coordenadores e diretores locais de proteção de dados devem se reportar aos coordenadores globais de proteção de dados correspondentes sobre métricas, incidentes e riscos relevantes de proteção de dados.

As informações a seguir refletem o esquema de coordenação e comunicação entre os responsáveis pela proteção de dados pessoais nos diferentes negócios e áreas corporativas, bem como os coordenadores globais e locais de proteção de dados.



(1) Respeitando o seu carácter como uma empresa cotada cotizada (*) DPD do RGPD (Regulamento Gerai do Proteção de Dados)

Tanto o Coordenador Global quanto os Coordenadores Locais de Proteção de Dados de Segurança Corporativa se reportam ao mais alto nível de gestão do Grupo Iberdrola.

ANEXO VI - PROCEDIMENTO PARA COOPERAÇÃO COM AUTORIDADES DE SUPERVISÃO E OUTRAS AUTORIDADES PÚBLICAS

A seguir, apresentamos o procedimento para a cooperação com as Autoridades Europeias de Supervisão para a proteção de Dados Pessoais em relação às NCVs da Iberdrola.

As Empresas do Grupo se comprometem a cooperar com as Autoridades Europeias de Proteção de Dados dentro do escopo de aplicação dos LNAs, e responderão às solicitações feitas por essas Autoridades em relação aos LNAs, de maneira apropriada e dentro do prazo prescrito, e cumprirão as decisões e recomendações feitas por essas Autoridades.

Além disso, em relação às solicitações de acesso a dados pessoais feitas ao Importador de Dados por uma Autoridade Pública do país importador, o Importador de Dados deverá:

- Notificar imediatamente o exportador de dados e, quando possível - se necessário com a assistência do exportador de dados - o titular dos dados, em caso de:
  - Receber uma solicitação de acesso de uma autoridade pública, de acordo com as leis do país de destino ou de outro país terceiro, para a divulgação de dados pessoais transferidos de acordo com os LCAs. A notificação deverá incluir informações sobre os dados pessoais envolvidos na solicitação, a autoridade solicitante, a base legal para a solicitação e a resposta fornecida.
  - Estar ciente de qualquer acesso direto por uma Autoridade Pública, de acordo com as leis do país de destino, aos dados pessoais transferidos de acordo com as NCVs. A notificação deverá incluir todas as informações disponíveis para o importador de dados.
- Caso as leis do país de destino proíbam a notificação mencionada no ponto anterior, você deverá envidar seus melhores esforços para derrogar essa proibição e comunicar o máximo de informações possível ao exportador de dados o mais rápido possível. Além disso, você deve documentar seus esforços para fornecer evidências de seus esforços em resposta a uma solicitação do exportador de dados.
- Fornecer ao exportador de dados, regularmente, todas as informações relevantes sobre as solicitações de acesso recebidas. Em particular, o número de solicitações, o tipo de dados solicitados, as autoridades solicitantes, se as solicitações foram contestadas e o resultado de tais contestações, etc. Caso o Importador de dados esteja sujeito a uma proibição de divulgar tais informações, ele deverá notificar o Exportador de dados imediatamente.
- Preservar as informações comunicadas ao exportador de dados enquanto os dados pessoais estiverem sujeitos às salvaguardas fornecidas pelas NCVs e disponibilizá-las às autoridades de supervisão competentes mediante solicitação.
- Avaliar se a solicitação de divulgação é legal, em particular se a autoridade pública solicitante tem o poder de solicitar a divulgação dos dados, e contestar ou recorrer da solicitação se, após a avaliação, concluir-se que há motivos razoáveis para considerá-la ilegal de acordo com a legislação do país de destino, as obrigações aplicáveis de acordo com o direito internacional e os princípios de cortesia internacional. No caso de uma contestação da solicitação, o importador de dados deverá buscar medidas provisórias para suspender os efeitos da solicitação até que a contestação seja resolvida pela autoridade judicial competente. Ele não divulgará os dados pessoais solicitados até que seja exigido pelas regras processuais aplicáveis.
- Documentar sua avaliação da legalidade da solicitação recebida e quaisquer questões relacionadas e, na medida do possível, disponibilizar essa documentação ao exportador de dados e às autoridades de supervisão competentes, mediante solicitação.
- Fornecer o mínimo de informações possível ao responder a uma solicitação de divulgação, com base em uma interpretação razoável da solicitação.

Em qualquer caso, as transferências de dados pessoais por uma Empresa do Grupo para qualquer autoridade pública não podem ser maciças, desproporcionais e indiscriminadas, mas devem ser limitadas ao estritamente necessário.

O Coordenador de Proteção de Dados de Segurança Corporativa Global deverá, mediante solicitação, fornecer acesso aos resultados dos relatórios de auditoria da NCV às Autoridades Europeias de Supervisão ou Autoridades de Proteção de Dados competentes.

Em aplicação do compromisso de cooperação e assistência entre as Empresas do Grupo em face de investigações e consultas das Autoridades Supervisoras de Proteção de Dados Pessoais em relação à conformidade com as NCVs, a resposta a qualquer solicitação de uma Autoridade Supervisora será gerenciada pelos Coordenadores Locais de Proteção de Dados de Segurança Corporativa, que informarão o Coordenador Global de Proteção de Dados de Segurança Corporativa que, com o apoio dos serviços jurídicos, responderá a essas solicitações.

ANEXO VII – PROCEDIMENTO PARA ATUALIZAÇÃO DAS NORMAS CORPORATIVAS OBRIGATÓRIAS DA IBERDROLA

A seguir, apresentamos o procedimento de atualização das NCVs da Iberdrola, que inclui o processo de aprovação de alterações nas NCVs, a forma de comunicação das alterações às Autoridades de Proteção de Dados, às Empresas do Grupo e às partes interessadas.

Emendas às Regras Corporativas Vinculantes

Emendas ao SFRS são aquelas que podem afetar o nível de proteção fornecido pelo SFRS ou afetar significativamente o SFRS, por exemplo, mudanças na legislação ou na estrutura do grupo.

As modificações nas NCV devem ser aprovadas pelo Coordenador de Proteção de Dados de Segurança Corporativa Global e comunicadas ao Comitê Global de Segurança Cibernética e Proteção de Dados (ou ao Comitê atuando em seu lugar) para conhecimento.

A Iberdrola, S.A. comunicará à Agência Espanhola de Proteção de Dados, em um prazo máximo de quinze (15) dias, qualquer proposta de modificação das NCVs, com uma breve explicação dos motivos da modificação, para que essa agência determine se a modificação proposta está sujeita ao procedimento de cooperação para a aprovação das NCVs. A alteração não deverá ser implementada até que tenha sido validada pela Agência Espanhola de Proteção de Dados.

Atualizações das Regras Corporativas Vinculantes

As NCV serão atualizadas regularmente para refletir a situação atual em um determinado momento. As atualizações levam em conta alterações na lista de empresas do Grupo sujeitas a elas, a inclusão de recomendações do Comitê Europeu de Proteção de Dados ou outras.

As atualizações das NCVs serão aprovadas pelo Coordenador de Proteção de Dados de Segurança Corporativa Global e comunicadas ao Comitê Global de Segurança Cibernética para seu conhecimento e implementação.

O **Coordenador Global de Proteção de Dados de Segurança Corporativa** comunicará qualquer atualização dos CSVs à Agência Espanhola de Proteção de Dados pelo menos uma vez por ano, com uma breve explicação dos motivos que justificam a atualização, e fornecerá as informações necessárias aos titulares dos dados ou às Autoridades de Proteção de Dados mediante solicitação.

O Coordenador Global de Proteção de Dados também notificará a Agência Espanhola de Proteção de Dados anualmente se não houver alterações no GDC, incorporando a confirmação de que, no caso de uma empresa membro ser responsabilizada por uma violação do GDC, ela tem ativos suficientes para cumprir essa responsabilidade.

Registro de alterações nas Regras Corporativas Vinculantes e sua comunicação

As CSVs estão sujeitas a um registro de alterações, que estabelece a data em que são revisadas e as alterações feitas como resultado dessa revisão. O **Coordenador Global de Proteção de Dados de Segurança Corporativa** manterá um registro atualizado das alterações às CSVs e uma lista atualizada das Empresas do Grupo sujeitas às CSVs e será responsável por comunicar as alterações e atualizações à Agência Espanhola de Proteção de Dados.

O **Coordenador Global de Proteção de Dados de Segurança Corporativa** também será responsável por comunicar prontamente ou sem atrasos indevidos quaisquer alterações nos CSVs por meio de notificação direta à Agência Espanhola de Proteção de Dados, bem como a qualquer outra Autoridade de Supervisão competente e às Empresas do Grupo.

As informações relativas a alterações nas NCVs serão publicadas na intranet da IBERDROLA e no site corporativo, incluindo outros meios, como comunicações gerais.

O **Coordenador de Proteção de Dados de Segurança Corporativa Global** deve garantir que todas as novas Empresas do Grupo cumpram e implementem efetivamente as NCVs, assinando o contrato de adesão relevante antes de qualquer transferência de dados pessoais para elas.

O **Coordenador de Proteção de Dados de Segurança Corporativa Global** será responsável por manter os CSVs atualizados e cumprir as disposições estabelecidas no Artigo 47 do GDPR.


Iberdrola