Política de Proteção de Dados Pessoais

Atualizada em 16 de outubro de 2025

O Conselho de Administração da NEOENERGIA S.A. (a "**Sociedade**") tem o poder de elaborar, avaliar e revisar, constantemente, o Sistema de Governança e Sustentabilidade da Sociedade, bem como aprovar e atualizar as políticas que contêm as diretrizes que regem a atuação da Sociedade e informam, ainda, no que for aplicável, as políticas que, no exercício de sua autonomia, resolvam aprovar as sociedades que integram o grupo, cuja entidade dominante é, no sentido estabelecido pela lei, a Sociedade (o "**Grupo**").

No exercício destas competências e no âmbito da legislação, do Estatuto Social da Sociedade e do Propósito e Valores do Grupo Neoenergia, bem como da sua Estratégia de Desenvolvimento Sustentável, o Conselho de Administração aprova esta Política de Proteção de Dados Pessoais (a "**Política**"), que respeita, desenvolve e adapta, em relação à Sociedade, os Princípios Éticos e Básicos de Governança e de Sustentabilidade do Grupo.

1. Âmbito de Aplicação

Esta Política é aplicável à Sociedade. Não obstante, a Política informa as ações e os desenvolvimentos normativos que devam ser realizados pelas demais sociedades do Grupo, observadas suas competências e sua autonomia nesta matéria.

Esses princípios devem nortear também, quando aplicável, a atuação das entidades de natureza fundacional vinculadas ao Grupo.

A Sociedade promoverá o alinhamento dos normativos das sociedades nas quais participe, mas que não façam parte do Grupo, bem como das joint ventures, associações temporárias de empresas e demais entidades nas quais assuma a gestão com os princípios contidos nesta Política.

2. Finalidade

A finalidade desta Política é estabelecer os princípios que devem reger a atuação da Sociedade, em matéria de proteção de dados pessoais, garantindo, em todo caso, o cumprimento da normativa aplicável.

Em particular, a Política garante o direito à proteção dos dados das pessoas físicas que se relacionam com na Sociedade, garantindo o respeito do direito à honra e à intimidade no tratamento das diferentes tipologias de dados pessoais procedentes de diferentes fontes e com fins diversos em função de sua atividade empresarial, tudo isto em cumprimento da Política de Respeito aos Direitos Humanos.

3. Princípios de atuação

A Sociedade assume e promove os seguintes princípios de atuação que devem fazer parte de suas atividades em matéria de proteção de dados pessoais:

a) Princípios de legitimidade, licitude e lealdade no tratamento de dados pessoais: O tratamento de dados pessoais será leal, legítimo e lícito conforme a normativa aplicável. Neste sentido, os dados pessoais deverão ser recolhidos para um ou vários fins específicos e legítimos conforme a normativa aplicável.

Nos casos em que for obrigatório, conforme normativa aplicável, deverá obter o consentimento dos interessados antes de solicitar seus dados.

Do mesmo modo, quando o exigir a lei, os fins do tratamento de dados pessoais serão explícitos e determinados no momento de sua coleta.

Em particular, a Sociedade não solicitará nem tratará dados pessoais relativos à origem étnica ou racial, à ideologia política, às crenças, às convicções religiosas ou filosóficas, à vida ou orientação sexual, à filiação sindical, à saúde, nem dados genéticos ou biométricos dirigidos a identificar de maneira unívoca a uma pessoa, salvo que o recolhimento dos referidos dados seja necessário, legítimo e requerido ou permitido pela normativa aplicável, em cujo caso serão solicitados e tratados de acordo com o estabelecido naquela.

b) Princípio de minimização: Somente serão objeto de tratamento aqueles dados pessoais que resultem estritamente necessários para a finalidade para os quais se recolham ou tratem e adequados a tal finalidade.

c) *Princípio de exatidão*: Os dados pessoais deverão ser exatos e estar atualizados. Em caso contrário, deverão ser suprimidos ou retificados.

d) Princípio de limitação do prazo de conservação: Os dados pessoais não serão conservados além do prazo necessário para atingir o fim para o qual se destinam, salvo nas hipóteses previstas legalmente.

e) Princípios de integridade e confidencialidade: No tratamento dos dados pessoais, será necessário garantir, mediante medidas técnicas ou organizacionais, segurança adequada que os proteja do tratamento não autorizado ou ilícito e que evite sua perda, sua destruição e que sofram danos acidentais.

Os dados pessoais solicitados e tratados pela Sociedade deverão ser conservados com a máxima confidencialidade e sigilo, não podendo ser utilizados para

outros fins distintos dos quais justificaram e permitiram sua coleta e sem que possam ser comunicados ou cedidos a terceiros fora dos casos permitidos pela normativa aplicável.

f) Princípio de responsabilidade proativa (prestação de contas): A Sociedade será responsável por cumprir com os princípios estipulados nesta Política e os exigidos na normativa aplicável e deverão ser capazes de demonstrá-lo, quando assim o exigir a legislação aplicável.

A Sociedade deverá fazer uma avaliação do risco dos tratamentos que realize, com o fim de determinar as medidas a serem aplicadas para garantir que os dados pessoais sejam tratados conforme exigências legais. Nos casos nos quais a lei assim o exigir, serão avaliados de forma prévia os riscos que novos produtos, serviços ou sistemas de informação possam comportar para a proteção de dados pessoais e serão adotadas as medidas necessárias para eliminá-los ou mitigá-los.

A Sociedade deverá manter registro das atividades que descrevam os tratamentos de dados pessoais que realizem no âmbito de suas atividades.

Caso se produza um incidente que ocasione a destruição, perda ou alteração acidental ou ilícita de dados pessoais, ou a comunicação ou acesso não autorizado a esses dados deverão ser observados os protocolos internos estabelecidos pela área de Segurança e Resiliência Corporativa (ou pela área que, em cada momento, assuma suas funções) através do Comitê de Segurança, Resiliência e Tecnologias Digitais e pela legislação aplicável. Esses incidentes deverão ser documentados e serão adotadas medidas para resolver e minimizar os possíveis efeitos negativos para os interessados.

Nos casos previstos na lei, será designado um Encarregado pelo Tratamento de Dados Pessoais (DPO) com o fim de garantir o cumprimento das normas de proteção de dados nas sociedades do Grupo.

g) Princípios de transparência e informação: O tratamento de dados pessoais será transparente em relação ao interessado, facilitando a informação sobre o tratamento de seus dados de forma compreensível e acessível, quando assim o exigir a legislação aplicável.

A fim de garantir um tratamento leal e transparente, A Sociedade deverá informar aos afetados ou interessados, cujos dados se pretende solicitar, as circunstâncias relativas ao tratamento, conforme normativa aplicável.

h) Aquisição ou obtenção de dados pessoais: Fica proibida a aquisição ou

obtenção de dados pessoais de fontes ilegítimas, de fontes que não garantam suficientemente sua legítima procedência ou de fontes cujos dados tenham sido solicitados ou cedidos transgredindo a lei.

i) Contratação de operadores do tratamento dos dados: Previamente à contratação de qualquer prestador de serviços que acesse dados pessoais que estejam sob controle da Sociedade, assim como durante a vigência da relação contratual, esta deverá adotar as medidas necessárias para garantir e, quando for legalmente exigível, demonstrar, que o tratamento de dados por parte do operador se realize conforme legislação aplicável.

j) Transferências internacionais de dados: Todo tratamento de dados pessoais sujeito à normativa da União Europeia que implique uma transferência de dados fora do Espaço Econômico Europeu deverá realizar-se com estrito cumprimento dos requisitos estabelecidos na lei aplicável na jurisdição de origem.

k) Direitos dos interessados: A Sociedade deverá permitir que os interessados possam exercer os direitos de acesso, retificação, supressão, limitação do tratamento, portabilidade e oposição que sejam de aplicação em cada localidade, estabelecendo, para este fim, os procedimentos internos que resultem necessários para satisfazer, ao menos, os requisitos legais aplicáveis em cada caso.

4. Coordenação a nível do Grupo

A área de Segurança e Resiliência Corporativa, através da Comissão de Segurança, Resiliência e Tecnologias Digitais (ou as áreas que, em cada momento, assumam suas funções) velará pela adequada coordenação, a nível de Grupo, das práticas e da gestão dos riscos no âmbito da proteção dos dados pessoais e estabelecerá os procedimentos de coordenação adequados com os comitês de segurança, resiliência e tecnologias digitais ou com as áreas de segurança (ou o comitê ou área que, em cada momento, assuma suas faculdades) do Grupo.

A área de Serviços Jurídicos (ou a área que, em cada momento, assuma suas funções) será responsável por reportar à área de Segurança e Resiliência Corporativa, através da Comissão de Segurança, Resiliência e Tecnologias Digitais (ou ao comitê que, em cada momento, assuma suas faculdades) os desenvolvimentos e novidades normativas que ocorram no âmbito da proteção de dados pessoais.

Adicionalmente, os negócios e diretorias corporativas deverão: (i) designar as pessoas responsáveis pelos dados pessoais, que atuarão coordenadamente e sob a supervisão da área de Segurança e Resiliência Corporativa (ou da área que, em cada momento, assuma suas faculdades) e da Comissão de Segurança, Resiliência e Tecnologias Digitais (ou o

comitê que, em cada momento, assuma suas faculdades) e (ii) coordenar com a área de Segurança e Resiliência Corporativa (ou a área que, em cada momento, assuma suas funções) qualquer atividade que implique ou envolva a o tratamentos de dados pessoais.

5. Implementação e acompanhamento

Para a implementação e acompanhamento do previsto nesta Política, o Conselho de Administração conta com a Área de Segurança e Resiliência Corporativa (ou a área que, em cada momento, assuma suas funções) que, através da Comissão de Segurança, Resiliência e Tecnologias Digitais (ou o comitê que, em cada momento, assuma suas funções) desenvolverá e manterá atualizada, conforme o disposto nesta Política, a normativa interna de gestão da proteção de dados pessoais, que será implementada pela área de Segurança e Resiliência Corporativa e que será de cumprimento obrigatório para os membros da equipe diretiva e de todos os profissionais do Grupo.

Sem prejuízo do anterior, será a área de Transformação Digital do Grupo (ou a área que, em cada momento, assuma suas funções) a responsável por velar por que os sistemas de informação do Grupo sejam corretamente implementados, dos controles e desenvolvimentos informáticos que sejam adequados para garantir o cumprimento da normativa interna de proteção de dados e que esses desenvolvimentos estejam atualizados em cada momento.

A área de Segurança e Resiliência Corporativa (ou a área que, em cada momento, assuma suas funções) avaliará, pelo menos uma vez ao ano, o cumprimento e a eficácia desta Política.

Além disso, para verificar o cumprimento desta Política serão realizadas auditorias periódicas com auditores internos ou externos.

*** * ***

Esta Política foi aprovada inicialmente pelo Conselho de Administração em 28 de junho de 2018 e atualizada pela última vez em Reunião do Conselho de Administração de 16 de outubro de 2025.