POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

Atualizada em 15 de junho de 2020.

O Conselho de Administração da NEOENERGIA, S.A (a "**Sociedade**") tem a competência de desenhar, avaliar e revisar em caráter permanente do Sistema de Governança Corporativa e especificamente, de aprovar as políticas corporativas, que desenvolvam os princípios previstos no *Propósito e Valores* do Grupo Neoenergia e as demais normas do Sistema de Governança Corporativaassim como de organizar os sistemas de controles internos. No exercício destas competências, e com o propósito de estabelecer os princípios gerais que devem reger o tratamento dos dados pessoais em todas as companhias pertencentes ao grupo cuja entidade controladora, no sentido estabelecido pela lei, é a Companhia (o "**Grupo**"), o Conselho de Administração aprova esta Política de proteção de dados pessoais (a "*Política*").

1. Finalidade

Esta *Política* estabelece os princípios e pautas comuns de atuação que devem reger o Grupo em matéria de proteção de dados pessoais, garantindo, em todo caso, o cumprimento da legislação aplicável.

Em particular, esta *Política* tem a finalidade de garantir o direito à proteção de seus dados de todas as pessoas físicas que se relacionam com as companhias pertencentes ao Grupo, 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 a *Política de Respeito de Direitos Humanos* da Companhia

2. Âmbito de aplicação

A Política será de aplicação à Companhia, às demais companhias do Grupo, aos seus administradores, diretores e colaboradores, assim como a todas as pessoas que se relacionem com as companhias pertencentes àquele.

Naquelas companhias ou entidades participadas, direta ou indiretamente, que não sejam controladas pelo Grupo, seus representantes nos órgãos da administração procurarão que se observem as previsões desta *Política* e promovam, na medida do possível, a aplicação de seus princípios.

3. Princípios do tratamento dos dados pessoais

Os princípios pelos quais se rege esta *Política* são os seguintes:

a) Princípios gerais:

As companhias do Grupo cumprirão criteriosamente a legislação aplicável de sua localidade em matéria de proteção de dados, a que resulte aplicável em função do tratamento de dados pessoais que se realize e a que se determine conforme normas ou acordos vinculantes adotados no âmbito do Grupo.

As companhias do Grupo atuarão para que os princípios abrangidos nesta *Política* sejam levados em conta (i) no desenho e implementação de todos os procedimentos

que impliquem o tratamento de dados pessoais, (ii) nos produtos e serviços oferecidos por tais companhias, (iii) em todos os contratos e obrigações formalizadoscom pessoas físicas e (iv) na implantação dos sistemas e plataformas que permitam o acesso por parte de colaboradores do Grupo ou de terceiros a dados pessoais e ao recolhimento ou tratamento desses dados.

b) Princípios relativos ao tratamento de dados pessoais:

(i) Princípios de legitimidade, licitude e lealdade no tratamento de dados pessoais.

O tratamento de dados pessoais será leal, legítimo e lícito conforme a legislação aplicável. Neste sentido, os dados pessoais deverão ser recolhidos para um ou vários fins específicos e legítimos conforme a legislação aplicável.

Nos casos em que for obrigatório, conforme legislação 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 seu recolhimento.

Em particular, as companhias do Grupo não solicitarão nem tratarão 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 legislação aplicável, em cujo caso serão solicitados e tratados de acordo com o estabelecido naquela.

(ii) 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.

(iii) Princípio de exatidão.

Os dados pessoais deverão ser exatos e estar atualizados. Em caso contrário, deverão suprimir-se ou retificar-se.

(iv) Princípio de limitação do prazo de conservação.

Os dados pessoais não serão conservadosalém do prazo necessário para atingir o fim para o qual se destinam, salvo nashipóteses previstas legalmente.

(v) 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 pelas companhias do Grupo deverão ser

conservados com a máxima confidencialidade e sigilo, não podendo ser utilizados para outros fins distintos dos quais justificaram e permitiram seu recolhimento e sem que possam ser comunicados ou cedidos a terceiros fora dos casos permitidos pela legislação aplicável.

(vi) Princípio de responsabilidade proativa (prestação de contas).

As companhias do Grupo serão responsáveis por cumprir com os princípios estipulados nesta *Política* e os exigidos na legislação aplicável e deverão ser capazes de demonstrá-lo, quando assim o exigir a legislação aplicável.

As companhias do Grupo deverão fazer uma avaliação do risco dos tratamentos que realizem, 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 quenovos produtos, serviços ou sistemas de informaçãopossam comportar para a proteção de dados pessoais e serão adotadas as medidas necessárias para eliminá-los ou mitigá-los. As companhias do Grupo deverão 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 áreade Segurança Corporativa e a 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, serão designados delegados de proteção de dados, com o fim de garantir o cumprimento das normasde proteção de dados nas companhias do Grupo.

(vii) 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 legislaçãoaplicável.

A fim de garantir um tratamento leal e transparente, a companhia do Grupo responsável pelo tratamento deverá informar aos afetados ou interessados, cujos dados se pretende solicitar, as circunstâncias relativas ao tratamento, conforme legislação aplicável.

(viii) 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.

(ix) Contratação de encarregados do tratamento dos dados.

Previamente à contratação de qualquer prestador de serviços que acesse dados pessoais que sejam responsabilidade das companhias do Grupo, assim como durante a vigência da relação contratual, estas deverão adotar as medidas necessárias para

garantir e, quando for legalmente exigível, demonstrar, que o tratamento de dados por parte do encarregado se realize conforme legislação aplicável.

(x) 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. As companhias do Grupo se localizadas fora da União Europeia deverão cumprir com os requisitos estabelecidos para as transferências internacionais de dados pessoais que sejam, conforme o caso, de aplicação em sua localidade.

(xi) Direitos dos interessados.

As companhias do Grupo deverão 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. Implementação

A área de Segurança Corporativa, conjuntamente com os Serviços Jurídicos da Companhia, desenvolverá e manterá atualizadas, conforme o disposto nesta *Política*, as normas internas do Grupo relativas à gestão global de proteção de dados, que será implementada pela Direção de Segurança Corporativa e será de cumprimento obrigatório para todos os diretores e colaboradores da Companhia.

A áreade Serviços Jurídicos será responsável por reportar à áreade Segurança Corporativa os desenvolvimentos e atualizaçõesnormativas que se produzam neste âmbito.

A áreade Sistemas, ou a área que assuma suas funções, será a encarregada de implementar, nos sistemas de informação das companhias do Grupo, os controles e desenvolvimentos tecnológicos que sejam adequados para garantir o cumprimento das normas internas de gestão global de proteção de dados e garantirá que esses desenvolvimentos estejam atualizados em cada momento.

Adicionalmente, os negócios e diretorias corporativas deverão (i) designar, sujeito ao que estabeleça a legislação aplicável em cada caso, as pessoas responsáveis pelos dados, que atuarão coordenadamente e sob a supervisão da áreade Segurança Corporativa e (ii) coordenar com a áreade Segurança Corporativa qualquer atividade que implique ou suporte a gestão de dados pessoais.Por fim o Comitê de Cibersegurança, constituído, conforme o disposto na Política de Riscos de Cibersegurança, dará prosseguimento ao acompanhamento geral da proteção de dados pessoais nas companhias do Grupo e velará pela adequada coordenação, no âmbito do Grupo, das práticas e gestão dos riscos de proteção dos dados pessoais, assessorando a Diretoria de Segurança Corporativa na aprovação da norma referente ao assunto de cibersegurança e proteção de dados.

5. Controle e avaliação

a) Controle

Competeà áreade Segurança Corporativa, ou à áreaque assuma suas funções, fiscalizar o cumprimento do disposto nesta *Política* por parte da Companhia e as demais companhias do Grupo, sem prejuízo das responsabilidades que correspondam a outros órgãos e áreas da Companhia e, conforme o caso, aos órgãos de administração das demais companhias do Grupo.

Para verificar o cumprimento desta *Política*, serão realizadas auditorias periódicas com auditores internos ou externos.

b) Avaliação

A áreade Segurança Corporativa, ou a diretoria que assuma suas funções, avaliará, ao menos uma vez ao ano, o cumprimento e a eficácia desta Política e informará o resultado à Diretoria de Recursos, ou à áreaque assuma tais funções em cada momento.

* * *

Esta *Política de proteção de dados pessoais* foi aprovada inicialmente pelo Conselho de Administração em 28 de junho de 2018 e atualizada na Reunião do Conselho de Administração realizado em 15 de junho de 2020.