DIRETRIZ DE PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE DA GASPETRO.

ABERTO

ATA DE APROVAÇÃO

Aprovada pela Diretoria Executiva da Gaspetro - Ata RDE, item 11, Pauta 122/21, de 11/05/2021.

1. OBJETIVO

Orientar sobre o tratamento de dados pessoais, inclusive nos meios digitais, nos quais a Gaspetro atue como Controlador ou Operador, visando à proteção dos direitos dos titulares de dados, à privacidade, e à conformidade com as regulamentações e legislações de proteção de dados pessoais aplicáveis.

2. ABRANGÊNCIA

Aplica-se à Petrobras Gás S.A. - Gaspetro, podendo ser desdobrada em suas investidas, respeitando-se os trâmites societários.

3. DESCRIÇÃO

3.1 Governança de proteção de dados pessoais

3.1.1 Papéis e Responsabilidades

As atividades do Encarregado pelo tratamento de dados pessoais são exercidas na Gaspetro pelo Gerente de Conformidade e demais áreas indicadas abaixo.

3.1.1.1 Compete ao Encarregado

O Encarregado é o responsável pela disseminação da cultura em proteção de Dados Pessoais e privacidade, monitoramento e governança do Tratamento dos Dados Pessoais e da privacidade na Companhia. Destacam-se, em suas atribuições, as seguintes atividades: aceitar reclamações e comunicações do Titular do Dado Pessoal, prestar esclarecimentos e adotar providências; receber comunicações da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e adotar providências; orientar colaboradores da Companhia a respeito das práticas a serem tomadas em relação à proteção de dados pessoais e privacidade; monitorar a conformidade dos Tratamentos de Dados Pessoais e privacidade realizados pelos Colaboradores da Companhia, no exercício de suas atribuições, com a Lei Geral de Proteção de Dados Pessoais (LGPD) e com as normas internas.

3.1.1.2 Compete à Auditoria Interna

Realizar auditorias periódicas com foco em proteção de dados pessoais e privacidade com o objetivo de determinar o nível de conformidade com a legislação, regulamentação, políticas, diretrizes e procedimentos internos.

3.1.1.3 Compete à Gerência de Conformidade

O titular da gerência de conformidade, além de acumular a função de Encarregado, deverá definir os controles e o monitoramento do nível de conformidade dos processos para atendimento à LGPD; realizar ciclos periódicos de avaliação dos controles implementados nos processos que envolvam o Tratamento de Dados Pessoais, coerentemente com os esforços de manutenção do processo de proteção de dados pessoais e privacidade.

Deverá atuar, ainda, na avaliação dos instrumentos relacionados à privacidade e demais termos de uso e compromisso da Companhia relacionados ao tema, bem como na promoção de formação e manutenção de cultura de proteção de dados pessoais e privacidade.

3.1.1.4 Compete aos Gestores

Identificar a existência de Tratamento de Dados Pessoais nos processos sob sua responsabilidade, além de informações associadas, tais como finalidade, embasamento legal, compartilhamento e mecanismos de segurança, tratados nos processos pelos quais é responsável; obter validação do embasamento legal com o Jurídico e parecer de segurança com a área responsável pela segurança da informação; estabelecer plano de mitigação de riscos a violações de dados pessoais e direitos relacionados à privacidade; apoiar o Encarregado na formação e manutenção de cultura na proteção de Dados Pessoais e privacidade.

3.1.1.5 Compete aos Colaboradores

Realizar corretamente o Tratamento de Dados Pessoais, em conformidade com a LGPD e com os normativos internos aplicáveis aos Tratamentos de Dados Pessoais e a privacidade realizados no exercício de suas funções em nome da Gaspetro.

3.1.1.6 Compete ao Jurídico

Prestar assessoria legal à Companhia no tema proteção de Dados Pessoais e privacidade; realizar disseminação do conhecimento sobre aspectos jurídicos da LGPD, bem como a análise de quaisquer questionamentos jurídicos relativos à lei e normas correlatas; auxiliar o Encarregado no suporte legal a manifestações e respostas aos requerimentos do titular dos dados pessoais e da ANPD; revisar, sob a ótica jurídico-legal, cláusulas contratuais, políticas de privacidade, diretrizes de privacidade e termos de uso, e outros documentos sobre o tema; monitorar mudanças regulatórias informando às unidades responsáveis para adoção de medidas cabíveis.

3.1.1.7 Compete à área responsável pela tecnologia da informação e de telecomunicações:

Promover a implementação de mecanismos de controle de segurança da informação adequados aos exigidos por esta Diretriz, oferecer suporte à Gaspetro e ao Encarregado, no exercício de suas atribuições, quando envolvidas questões técnicas e específicas de tecnologia da informação relacionadas ao assunto.

3.2 Diretrizes para o Tratamento de Dados Pessoais

3.2.1 Princípios norteadores do Tratamento de Dados Pessoais

O Tratamento de Dados Pessoais, pela Gaspetro, seus Colaboradores e partes relacionadas, deve observar os princípios elencados no art. 6º da LGPD, citados abaixo:

- **Finalidade**: os Dados Pessoais tratados devem guardar correlação com a finalidade para a qual foram coletados, a qual deve ser explicitamente informada aos Titulares;

- **Adequação**: o Tratamento de Dados Pessoais somente pode ser realizado quando houver compatibilidade com a finalidade informada ao titular do dado, de acordo com o contexto do Tratamento;

- **Necessidade**: o Tratamento de Dados Pessoais deve ser necessário ao atendimento da finalidade para a qual foram coletados e se ater aos dados pertinentes, proporcionais, não excessivos e minimamente necessários ao referido atendimento;

- **Qualidade dos dados**: o Tratamento de Dados Pessoais deve possuir como insumo dados pessoais claros, exatos, atualizados, necessários à finalidade para qual foram coletados;

- **Livre acesso**: o Titular do dado tem garantia de consulta, facilitada e gratuita, sobre a forma, integralidade e duração do Tratamento realizado sobre seus dados pessoais;

- **Transparência**: o Titular dos dados tem garantia de acesso a informações claras, precisas e facilmente acessíveis sobre o Tratamento de Dados Pessoais realizado sobre seus dados pessoais, bem como sobre os agentes de Tratamento envolvidos, observados os segredos comercial e industrial;

- **Segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. São exemplos de medidas de segurança:

    I) uso de senhas complexas e fatores de autenticação para o acesso aos nossos sistemas;

    II) limitação de acesso aos dados pessoais aos Colaboradores que efetivamente necessitem do acesso;

    III) armazenamento de dados somente em locais aprovados e homologados, e somente pelo tempo necessário;

    IV) reporte de suspeitas de vazamentos de dados

- **Prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do Tratamento de Dados Pessoais;

- **Não discriminação:** impossibilidade de realização do Tratamento para fins discriminatórios ilícitos ou abusivos;

- **Responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de Dados Pessoais e, inclusive, da eficácia dessas medidas. São exemplos disso:

I) Adoção de medidas de segurança da informação em linha com as exigências administrativas e tecnológicas mais atuais;

II) Manutenção atualizada de registros de operações de Tratamento de dados pessoais, facilitando a fiscalização da ANPD e o exercício dos direitos dos titulares;

III) Elaboração de Relatórios de Impacto de Proteção de Dados (RIPD), nas hipóteses em que o Tratamento de dados puder acarretar risco às liberdades civis e aos direitos fundamentais dos titulares; e

IV) Treinamento e comunicação constantes sobre a importância, para a Companhia, de o Tratamento dos dados pessoais ser realizado em conformidade com a LGPD e com as normais internas.

3.2.2 Direitos do Titular do Dado Pessoal

A Gaspetro deverá observar os direitos listados na LGPD e normas correlatas.

O exercício dos direitos não é absoluto, cabendo à Gaspetro analisar a legalidade, razoabilidade e a presença de situações impeditivas, modificativas ou extintivas dos direitos do titular do dado pessoal, para que as eventuais negativas, mesmo que parciais, sejam informadas de forma fundamentada aos Titulares requerentes.

Para garantir o exercício dos direitos dos Titulares de Dados Pessoais a Gaspetro disponibiliza, nos termos da lei, canais de comunicação para o atendimento de requisições dos Titulares de Dados Pessoais.

3.3 Tratamento de Dados Pessoais

3.3.1 Situações em que o Tratamento de Dados Pessoais é permitido

O Tratamento de Dados Pessoais, pela Gaspetro, somente poderá ser realizado quando presente uma das seguintes hipóteses abaixo:

a) Cumprimento de obrigação legal ou regulatória pelo controlador;

b) Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do Titular dos dados;

c) Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

d) Para a proteção da vida ou da incolumidade física do Titular ou de terceiro;

e) Pela administração pública, para o Tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da LGPD;

f) Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a Anonimização dos Dados Pessoais;

g) Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

h) Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente;

i) Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do Titular que exijam a proteção dos Dados Pessoais;

j) Mediante o fornecimento de Consentimento pelo Titular do Dado Pessoal em formato livre, informado e inequívoco, nos termos do item 3.3.1.2 desta Diretriz.

Caso haja dúvidas quanto à prevalência dos direitos e liberdades fundamentais do Titular, na hipótese prevista na alínea "i", o Jurídico deverá ser consultado.

O Tratamento de Dados Pessoais oriundos de bases de dados públicas é permitido, desde que respeitada a finalidade para a qual os dados pessoais foram tornados públicos, a boa-fé e o interesse público, resguardados os direitos do Titular do Dado Pessoal.

3.3.1.1. Tratamento baseado em Legítimo Interesse

O Legítimo Interesse somente poderá fundamentar o Tratamento de Dados Pessoais não sensíveis para finalidades legítimas, consideradas a partir de situações concretas, tais como apoio e promoção de atividades da Gaspetro e a proteção do exercício regular dos direitos do Titular de Dados Pessoais ou a prestação de serviços que o beneficiem, respeitadas as suas legítimas expectativas e os seus direitos e liberdades fundamentais

A utilização do Legítimo Interesse como base legal para o Tratamento de Dados Pessoais deve ocorrer somente caso nenhuma das demais situações expostas no item 3.3.1 esteja presente, à exceção do Consentimento do Titular (alínea "j").

Sempre que o Tratamento de Dados Pessoais estiver baseado em Legítimo Interesse, deverá ser elaborado o correspondente RIPD, nos termos do item 3.6 desta diretriz.

3.3.1.2 Tratamento baseado no Consentimento

O Consentimento torna o Tratamento de Dados Pessoais válido quando concedido de forma prévia, livre, informada e inequívoca.

O Consentimento é inequívoco quando decorre de uma ação positiva do titular do dado pessoal, capaz de demonstrar cabalmente seu entendimento e vontade de consentir para o tratamento de seus dados pessoais.

O Consentimento é informado quando fornecido em conformidade com a autodeterminação do Titular do Dado Pessoal.

O Consentimento deve ser obtido antes de se realizar qualquer atividade de Tratamento de Dados Pessoais.

O Titular deverá ser informado sobre as consequências da negativa de Consentimento.

A obtenção do Consentimento do Titular deve ser evidenciada e armazenada para possibilitar a comprovação da conformidade do Tratamento de Dados Pessoais.Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

O dado pessoal obtido por consentimento descrito neste item que necessitar ser compartilhado deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas em Lei.

É dispensada a exigência do consentimento disciplinado neste item para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Diretriz.

O Consentimento pode ser revogado a qualquer momento pelo Titular dos Dados Pessoais, hipótese em que deve cessar o Tratamento de Dados Pessoais nele baseado.

A utilização do Consentimento do Titular como base legal para o tratamento de dados deve ocorrer somente no caso de nenhuma das outras hipóteses estar presente, conforme item 3.3.1.

3.3.1.3 Tratamento de Dados Pessoais Sensíveis

O Tratamento de Dados Pessoais sensível pela Gaspetro somente poderá ser realizado nas seguintes hipóteses:

I) Quando o Titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II) Sem fornecimento de Consentimento do Titular nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo Controlador,

b) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível a Anonimização dos Dados Pessoais Sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

e) proteção da vida ou da incolumidade física do Titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do Titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do Titular que exijam a proteção dos Dados Pessoais.

Caso haja dúvidas quanto à prevalência dos direitos e liberdades fundamentais do Titular, na hipótese prevista na alínea “g”, o Jurídico deverá ser consultado.

Diante da relevância dos Dados Pessoais Sensíveis, o Tratamento de dados desta natureza deve observar controles de segurança adicionais de privacidade e proteção de Dados Pessoais, conforme normas de segurança da informação existentes, com atenção especial ao (s) documento (s) que regula (m) a identificação do grau de sigilo e o tratamento da informação respectiva.

Além disso, deverá ser elaborado RIPD, nos termos do item 3.6 desta Diretriz. O prazo para que as

gerências concluam os RIPD de todos os processos gerenciais da Gaspetro que envolvam Dados Pessoais Sensíveis é de 180 (cento e oitenta dias) a contar da aprovação desta Diretriz.

3.3.1.4 Tratamento de Dados Pessoais de crianças e adolescentes

Exceto no caso de estar presente base legal diversa do Consentimento, disposta nos itens 3.3.1 (para Dados Pessoais) ou 3.3.1.1 (para Dados Pessoais Sensíveis), o Tratamento de Dados Pessoais de crianças só é permitido mediante o Consentimento específico e destacado dos pais ou responsáveis legais dos menores.

Todo Tratamento de Dado Pessoal de criança ou adolescente deve ser feito no melhor interesse do menor e deve ser de conhecimento do Encarregado via mapeamento prévio.

3.3.2 Garantia de qualidade no Tratamento de Dados Pessoais

Onde os Dados Pessoais forem armazenados, processados ou transmitidos deve haver um processo para garantir que cada dado seja:

a) preciso (ou seja, registrado corretamente e atualizado);

b) mantidos em sigilo, ou seja, protegidos contra a divulgação não autorizada;

c) protegidos em todo o seu ciclo de vida (desde a coleta até sua eliminação);

d) processados de maneira justa, legal e transparente e usados apenas para fins especificados, explícitos e legítimos;

e) restrito a um conjunto mínimo necessário à realização do propósito da atividade (minimização);

f) compartilhado somente com partes externas que possam demonstrar conformidade com os requisitos legais e regulamentares para manipulação de Dados Pessoais e desde que exista base legal autorizativa para o referido compartilhamento.

g) recuperável no caso de uma solicitação legítima de acesso do Titular de dados;

h) eliminado conforme item 3.3.5.

3.3.3 Transferências Internacionais de Dados Pessoais

A Transferência Internacional de Dados Pessoais é permitida somente quando presentes as seguintes situações:

a) O país para o qual o Dado Pessoal será transferido proporciona um nível adequado de proteção para os direitos e liberdades do Titular, de acordo com a avaliação da ANPD;

b) Por meio da comprovação de adoção de garantias de cumprimento dos princípios, dos direitos do Titular e do regime de proteção de dados previsto na LGPD, na forma de:

   I) cláusulas contratuais específicas para determinada transferência;

   II) cláusulas-padrão contratuais;

III) normas corporativas globais;

IV) selos, certificados e códigos de conduta regularmente emitidos;

c) Quando a transferência for necessária para a proteção da vida ou da incolumidade física do Titular ou de terceiro;

d) Quando o Titular fornecer seu Consentimento específico e em destaque para a transferência, devendo ser devidamente informado do caráter internacional da operação.

e) Quando a ANPD autorizar a transferência; ou

f) Quando a Transferência Internacional for necessária para o atendimento das alíneas “a”, “b” e “c” do item 3.3.1.

A cláusula-padrão prevista na alínea “b” refere-se àquela elaborada pela ANPD. A definição do conteúdo de cláusulas-padrão contratuais, e as cláusulas contratuais específicas para uma determinada transferência, as normas corporativas globais ou selos, certificados e códigos de conduta, todos referidos na alínea “b”, devem ser homologadas pela ANPD para a utilização como mecanismo de Transferência Internacional.

Em hipótese de dúvidas com relação à legislação aplicável, o Jurídico deve ser consultado sobre a compatibilidade das legislações dos países envolvidos.

3.3.4 Tratamento de Dados Pessoais nas relações da Gaspetro

Qualquer parte relacionada em alguma iteração com a Gaspetro também deverá observar o atendimento dos requisitos e princípios referentes à proteção de Dados Pessoais e privacidade, listados na LGPD.

Os contratos entre a Gaspetro e terceiros que, de forma direta ou indireta, envolvam o Tratamento de Dados Pessoais, serão regidos por cláusula contratual padrão de proteção de Dados Pessoais, que estipula as responsabilidades e deveres de cada uma das partes contratantes no Tratamento de Dados Pessoais.

Qualquer necessidade de alteração da cláusula padrão de proteção de Dados Pessoais nos contratos deve ser previamente submetida à avaliação do Jurídico.

Qualquer necessidade de criação de documento formal para regular as relações da Gaspetro, diferente das minutas já existentes, deve ser previamente submetida à avaliação do Jurídico.

3.3.5 Eliminação dos Dados Pessoais

Para todo Dado Pessoal, haverá tempo de retenção previamente estabelecido pelo gestor e a eliminação deve seguir tais parâmetros.

Portanto, após o cumprimento da finalidade para a qual foram tratados, os Dados Pessoais devem ser eliminados, a menos:

I) que haja fundamento jurídico para a manutenção dos Dados Pessoais, ou

II) que os dados sejam Anonimizados.

Em caso de dúvidas sobre a existência de fundamento jurídico que ampare a manutenção dos dados

pessoais, o Jurídico deverá ser consultado.

3.3.6 Segurança dos Dados Pessoais e da privacidade

Os Dados Pessoais deverão ser protegidos segundo critérios de segurança da informação: confidencialidade, integridade, disponibilidade e autenticidade, bem como da privacidade.

A proteção de dados pessoais deve seguir os normativos internos de segurança da informação da Companhia.

Deve-se avaliar, para cada caso o uso de controles técnicos específicos que contribuam para a proteção de informações relacionadas à proteção de informações relacionadas à proteção de dados pessoais e privacidades tais como gestão de acesso, criptografia, Anonimização e Mascaramento, bem como controles administrativos como práticas de mesa limpa, controle de liberação de documentos nas impressoras, guarda de documentos em locais reservados como salas, armários e gavetas com chave.

Fica determinado que os Dados Pessoais Sensíveis são pré-classificados quanto ao grau de sigilo como confidenciais e que os demais Dados Pessoais devem ser classificados pelos gestores conforme diretriz de classificação da empresa.

3.4 Mapeamento de Dados Pessoais

Para o cumprimento da legislação, os gestores deverão manter atualizado o registro relacionados às atividades de tratamento de dados pessoais.

O mapeamento de Dados Pessoais, também chamado de inventário de Dados Pessoais ou "*data mapping*", consiste em realizar o registro das operações de Tratamento de Dados Pessoais trabalhados em cada processo da empresa, assim como, para cada Dado Pessoal: sua finalidade; seu embasamento legal; onde é armazenado; como se dá o fluxo ao longo da organização seja por sistemas, de forma não estruturada, por documentos físicos, ou por qualquer outro meio; e também quais são as medidas de segurança técnicas ou organizacionais associadas. O embasamento legal deve ser validado pelo Jurídico.

3.5 Avaliação e identificação de riscos aos Dados Pessoais e à privacidade

Alinhada à metodologia corporativa de análise de riscos e com foco em proteção de Dados Pessoais e à privacidade, sempre que for realizada a atividade de mapeamento de Dados Pessoais, deve-se realizar a identificação de lacunas e a análise de riscos tanto com relação a aspectos legais quanto referente à segurança da informação. Caso necessário, também deve-se elaborar o RIPD (vide item 3.6).

3.6 Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O RIPD é uma documentação do Controlador que contém a descrição dos processos de Tratamento de Dados Pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

A elaboração do Relatório é obrigatória sempre que:

I) o Tratamento de Dados Pessoais puder gerar riscos às liberdades civis e aos direitos fundamentais, como é o caso do Tratamento de Dados Pessoais Sensíveis;

II) o Tratamento de Dados Pessoais estiver fundamentado no Legítimo Interesse, conforme item 3.3.1, alínea “i”; ou

III) quando a ANPD assim exigir.

3.7 Definição e manutenção de controles com foco em Dados Pessoais e privacidade

Devem ser definidos e mantidos controles eficazes com foco na proteção dos Dados Pessoais e privacidade. A cada atualização do mapeamento de Dados Pessoais e realização de análise de riscos, deve-se revisar os controles existentes e, caso necessário, definir-se novos controles. Além disso, deve-se cumprir um ciclo periódico de avaliação de controles nos processos que envolvam o Tratamento de Dados Pessoais.

3.8 Realização de auditorias com foco em Dados Pessoais e privacidade

A Companhia deve realizar auditorias periódicas com foco em proteção de Dados Pessoais e privacidade com o objetivo de determinar o nível de conformidade com a legislação, regulamentação e políticas, diretrizes e procedimentos internos. Após elaboração dos relatórios de auditoria interna, as áreas pertinentes deverão elaborar planos de ação para sanar os pontos de não conformidade explicitados.

3.9 Desenvolvimento da cultura de proteção de Dados Pessoais e privacidade

Devem ser elaborados conteúdos técnicos sobre proteção de Dados Pessoais e privacidade em consonância com os normativos internos, os quais devem ser veiculados pelos canais disponíveis e pelos agentes responsáveis, visando a conscientização abrangente, o desenvolvimento da cultura, e ciclos de capacitação dos diferentes públicos de interesse.

A Gaspetro realizará treinamentos periódicos para os Colaboradores visando disseminar a cultura de privacidade e proteção de Dados Pessoais, de acordo com as normas legais.

3.10 Violações a Dados Pessoais e à privacidade

Na Gaspetro as violações de Dados Pessoais que envolvam quebra de confidencialidade, integridade, disponibilidade ou autenticidade serão tratados como parte do processo de tratamento de Incidente de Segurança da Informação corporativo. Demais violações envolvendo dados pessoais e privacidade serão recepcionadas e tratadas no processo de tratamento de demanda do Encarregado.

A identificação de violação da privacidade e de Dados Pessoais deve ocorrer preferencialmente de maneira proativa:

I) monitorando os *logs* de eventos ou usando a detecção de intrusões, proteção contra vazamento de informações e ferramentas forenses de rede; ou

II) por meio de controle dos processos nos meios físicos.

A resposta a uma violação de Dados Pessoais que possa acarretar relevante risco ou dano ao titular do dado pressupõe a comunicação pela Gaspetro ao titular de Dado Pessoal e à ANPD no prazo estabelecido pela mesma.

3.11 Sanções

A inobservância da presente Diretriz enseja a aplicação de medidas disciplinares, bem como de penalidades previstas na legislação em vigor, nos contratos, convênios e termos de cooperação e nas normas internas da Companhia, sem prejuízo de outras medidas cabíveis, de natureza administrativa, judicial ou extrajudicial.

4. REGISTROS

Não aplicável.

5. DEFINIÇÕES

Agentes de Tratamento: o Controlador e o Operador de dados pessoais;

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

Colaboradores: compreende os empregados da Companhia, além de estagiários e empregados de empresas prestadoras de serviço, e as pessoas com quem a Gaspetro mantenha relação de parceria.

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

A Gaspetro atua como controladora, por exemplo, quando contrata recepcionistas para os seus imóveis, pois o serviço é prestado conforme as orientações da companhia, ou seja, são solicitados os documentos e dados pessoais que a companhia exigir para o ingresso nas suas dependências e esses dados são registrados em sistemas conforme instruções e nos limites impostos pela Gaspetro à contratada.

Alguns indicativos que caracterizam a atuação da Gaspetro no papel de controladora de dados pessoais são:

- Decidimos sobre quais dados devem ser tratados (coletados, armazenados, compartilhados etc.)

- Contratamos terceiros para tratar dados pessoais em nosso nome e sob nossa responsabilidade.

Dado Pessoal: qualquer informação que identifique direta ou indiretamente uma pessoa natural, como, por exemplo, nome, CPF, RG, endereço IP, número de registro interno dentro da organização, profissão, endereço de correio eletrônico, cargo, local de trabalho, foto e até mesmo seus hábitos de comportamento. Não são considerados dados pessoais quaisquer dados relacionados a pessoas jurídicas como CNPJ, razão social, balanço financeiro etc.

Dado Pessoal Sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião

política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. Possui como principais atividades orientar e fiscalizar o cumprimento das normas e diretrizes de proteção de dados pessoais dentro do Agente de Tratamento, servindo como ponto focal para todas as demandas do tema, participando ativamente da implementação de novos projetos que possam, direta ou indiretamente, atingir direitos e garantias do Titular dado pessoal.

Incidente de Segurança da Informação: descumprimento dos padrões de segurança da informação da Companhia ou qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que sejam uma ameaça à disponibilidade, à integridade, ao sigilo ou à autenticidade das informações da Gaspetro ou sob responsabilidade da empresa.

Legítimo Interesse: tem relação com o Tratamento de Dado Pessoal cuja coleta e manipulação não estejam respaldadas em exigência legal ou regulatória, mas que possam ser justificadas por processo empresarial plausível e legítimo e/ou em favor do Titular do Dado Pessoal.

Lei Geral de Proteção de Dados Pessoais ou LGPD: Lei 13.709/2018, que dispõe sobre o Tratamento de Dados Pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. É bastante semelhante ao regulamento europeu *General Data Protection Regulation* (GDPR), que entrou em vigor em maio de 2018.

Mascaramento: técnica que permite a criação de versão semelhante aos dados originais em ternos de estrutura, mas sem revelar a sua verdadeira informação.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

A classificação como operador se verifica, também, no âmbito dos Contratos de Custos e Despesas (CCCD).

Alguns indicativos que caracterizam a atuação de Operador:

- Seguir as instruções de terceiros no Tratamento de Dados Pessoais;
- Receber demanda de Tratamento de Dados Pessoais em nome de terceiros.

Titular do Dado Pessoal ou Titular: pessoa natural a quem se referem os dados pessoais que são objeto de Tratamento.

Transferência Internacional de Dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro. O acesso a Dado Pessoal localizado em país estrangeiro ou organismo internacional do qual o país seja membro (acesso remoto) também é considerado uma Transferência Internacional de Dados Pessoais.

Tratamento de Dados Pessoais ou Tratamento: toda operação realizada com Dados Pessoais, em meio físico ou digital, que integre o ciclo de vida do dado, desde sua coleta até seu descarte. Exemplos: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

6 REFERÊNCIAS

- Lei Geral de Proteção de Dados Pessoais – LGPD. Lei 13.709/2018.
- Regulamento Geral de Proteção de Dados da União Europeia – Regulamento 2016/679.

7. ANEXOS

7.1. Anexo A – Modelo RIPD.