POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

POL-022

Versão 2.0

Classificação: Pública

HISTÓRICO DE ALTERAÇÕES / REVISÕES

NÚMERO DA VERSÃO	DATA	RESUMO DAS ALTERAÇÕES	AUTOR
1.0	17/10/2022	Documento original	Felipe Romero – Solarplex
1.1	08/12/2022	Revisão de Formatação	Max dos Santos – Vortex Security
2.0	26/01/2026	Revisão geral	Henrique Carvalho – Vortex Security

REVISÃO SEGURANÇA DA INFORMAÇÃO

NOME	CARGO	ASSINATURA
Henrique Carvalho	CTO	

APROVAÇÃO ALTA DIREÇÃO

NOME	CARGO	ASSINATURA
Vagner Aguiar	CTO	

ÍNDICE

1. OBJETIVO

Em suas operações de negócio diárias, a Vortex Security usa uma variedade de dados sobre indivíduos identificáveis, incluindo dados sobre colaboradores atuais, anteriores e futuros, clientes, usuários de seus sites e aplicativos e outras partes interessadas. O objetivo desta Política é estabelecer diretrizes para o tratamento de dados pessoais, garantindo a privacidade e a proteção destes dados.
A Vortex Security atua em dois papéis distintos:

1. **Controladora:** Responsável pelas decisões sobre o tratamento de dados de seus próprios colaboradores, candidatos e leads.
2. **Operadora:** Realiza o tratamento de dados pessoais (como usuários e identificadores técnicos em logs) em nome de seus clientes, no escopo dos serviços de SOC e resposta a incidentes.

2. APLICAÇÃO

Esta política se aplica a todos os sistemas, pessoas e processos que constituem os sistemas de informação da organização, incluindo membros do conselho, diretores, colaboradores, fornecedores e outros terceiros que tenham acesso aos sistemas da Vortex Security.

3. REFERÊNCIAS

Este documento foi elaborado de forma a atender as normas:
ISO 27001:2012
ISO 27701:2019
Lei Geral de Proteção de Dados

4. POLÍTICA

4.1. GERAL

A LGPD é uma das legislações mais significativas que afetam a forma como a Vortex Security realiza suas atividades de processamento de informações. Multas significativas são aplicáveis se uma violação for considerada como tendo ocorrido ao abrigo da LGPD, que se destina a proteger os dados pessoais dos cidadãos. É política da Vortex Security garantir que nossa conformidade com a LGPD e outras legislações relevantes seja clara e demonstrável em todos os momentos.

A Política determina os seguintes compromissos:

- Respeito à privacidade dos titulares;
- Transparência aos titulares sobre as necessidades de tratamento de seus dados pessoais, a forma, a duração e a exatidão das informações;
- O tratamento dos dados deve atender à finalidade legítima;
- Proteção aos dados pessoais dos titulares nos ambientes digitais e analógicos da organização;
- Limitação do tratamento de dados ao mínimo necessário para realização das atividades e processos da
- organização;

Impossibilidade de realização do tratamento dos dados para fins discriminatórios ilícitos ou abusivos.

É política da Vortex Security garantir que nossa conformidade com a LGPD e outras legislações seja clara e demonstrável. A organização assume compromissos de respeito à privacidade, transparência, proteção de dados em ambientes digitais e analógicos, e a limitação do tratamento ao mínimo necessário

4.2. DEFINIÇÕES

Os termos mais relevantes para esta política incluem:

- Agentes de tratamento: o controlador e o operador de dados pessoais;
- Anonimização: utilização de meios técnicos, razoáveis e disponíveis no momento do tratamento de dados pessoais, 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 território nacional;
- Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
- Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
- 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;
- Dado anonimizado: dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
- Dado pessoal: informação relacionada à pessoa natural identificada ou identificável;
- Dado pessoal de criança e de adolescente: o Estatuto da Criança e do Adolescente (ECA) considera criança a pessoa até 12 anos de idade incompletos e adolescente aquela entre 12 e 18 anos de idade. Em especial, a LGPD determina que as informações sobre o tratamento de dados pessoais de crianças e de adolescentes deverão ser fornecidas de maneira simples, clara e acessível de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança;
- Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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;
- Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
- Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- Garantia da segurança da informação: capacidade de sistemas e organizações assegurarem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. A Política Nacional de Segurança da Informação (PNSI) dispõe sobre a governança da segurança da informação aos órgãos e às entidades da administração pública federal em seu âmbito de atuação;
- Garantia da segurança de dados: ver garantia da segurança da informação;
- Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- Relatório de impacto à proteção de dados pessoais: 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;
- 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;
- Tratamento: toda operação realizada com dados pessoais; como as que se referem a:
    - **acesso** - possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc., visando receber, fornecer, ou eliminar dados;
    - **armazenamento** - ação ou resultado de manter ou conservar em repositório um dado;

- **arquivamento** - ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotada a sua vigência;
- **avaliação** - ato ou efeito de calcular valor sobre um ou mais dados;
- **classificação** - maneira de ordenar os dados conforme algum critério estabelecido;
- **coleta** - recolhimento de dados com finalidade específica;
- **comunicação** - transmitir informações pertinentes a políticas de ação sobre os dados;
- **controle** - ação ou poder de regular, determinar ou monitorar as ações sobre o dado;
- **difusão** - ato ou efeito de divulgação, propagação, multiplicação dos dados;
- **distribuição** - ato ou efeito de dispor de dados de acordo com algum critério estabelecido;
- **eliminação** - ato ou efeito de excluir ou destruir dado do repositório;
- **extração** - ato de copiar ou retirar dados do repositório em que se encontrava;
- **modificação** - ato ou efeito de alteração do dado;
- **processamento** - ato ou efeito de processar dados;
- **produção** - criação de bens e de serviços a partir do tratamento de dados;
- **recepção** - ato de receber os dados ao final da transmissão;
- **reprodução** - cópia de dado preexistente obtido por meio de qualquer processo;
- **transferência** - mudança de dados de uma área de armazenamento para outra, ou para terceiro;
- **transmissão** - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.;
- **utilização** - ato ou efeito do aproveitamento dos dados.

- Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

4.3. PRINCÍPIOS

Para uma efetiva e adequada atividade de tratamento dos dados pessoais, é necessário respeitar os dez preceitos base de tratamento existentes na Lei nº 13.709/2018, todos previstos no artigo 6º da LGPD.

4.3.1. DA ADEQUAÇÃO

Com previsão no inciso segundo do artigo 6º da LGPD, o princípio da adequação emprega-se com o seguinte conceito "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento".

Assim temos que o tratamento de dados deverá ser condizente à destinação à qual se refere, não apresentando-se de forma contraditória à finalidade destinada. A coleta de dados deverá ser compatível com a atividade fim do tratamento, não podendo apresentar uma relação destoante entre o titular dos dados e o controlador.

4.3.2. DA NECESSIDADE

O princípio da necessidade da coleta de dados pessoais estipula dentro do contexto da Lei que a coleta de dados deve se dar de maneira restritiva, presando pelo tratamento de dados pessoais estritamente necessários ao atendimento da finalidade pretendida, dispensada a coleta excessiva.

Isso significa que ao fazer o levantamento e a varredura dos dados pessoais armazenados e suas respectivas naturezas, o empresário tem a inédita oportunidade de propor uma revisão da sua estrutura de armazenamento e segurança de informação para que essa seja adequada ao tamanho da sua operação.

4.3.3. DA TRANSPARÊNCIA

O presente princípio visa a garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, bem como formulada numa linguagem clara e simples, e que se recorra, adicionalmente, à visualização sempre que for adequado, observados os segredos comercial e industrial.

Originalmente surgiu ante o "Right to be Informed", que nos traz a ideia de que as pessoas naturais têm o direito de serem informados sobre a coleta e o uso de seu dado pessoal, incluindo: seus propósitos para processar os dados, seus períodos de retenção para esses dados pessoais e com quem serão compartilhados.

4.3.4. DO LIVRE ACESSO

Como exposto, o princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. E, consequentemente, o titular dos dados tem o livre acesso para consultar, de forma facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

A disposição poderá ser entregue de forma física ou eletrônica, mediante requisição do titular. O formato da entrega porá ser de forma simplificada e imediato ou por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, no prazo de até 15 (quinze) dias, contado da data do requerimento do titular (Artigo 19 LGPD), formato este que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

4.3.5. DA QUALIDADE DOS DADOS

No mesmo sentido dos princípios da transparência e do livre acesso, o princípio da qualidade dos dados garante aos titulares exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Conforme vemos na própria Lei Geral de Proteção de Dados, o titular dos dados tem o direito de correção de dados incompletos, inexatos ou desatualizados e, ainda, informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados e sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

4.3.6. DA SEGURANÇA

A segurança compreende nas 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. Atua junto ao princípio da prevenção, vez que se realiza a contratação de mecanismos de segurança exatamente para mitigar e poder prevenir de eventuais incidentes.

Os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas.

4.3.7. DA PREVENÇÃO

A prevenção vem dos pilares da Segurança da Informação, onde é necessário se precaver de eventuais eventualidades que possam ocorrer, adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Para garantir que a informação esteja protegida e ter uma Segurança da Informação efetiva, além de investir em tecnologia, é essencial também trabalhar com alinhamento de processos e conscientização de pessoas de toda a organização.

4.3.8. DA RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS

O princípio da responsabilização e da prestação de contas dispõe que o agente tratador dos dados pessoais (controlador ou operador), deverá demonstrar todas as medidas eficazes e capazes de comprovar o cumprimento da LGPD e, ainda, a eficácia das medidas aplicadas.

Em outras palavras, é dizer que o controlador ou operador tem o dever de prestar contas, ante a sua responsabilização, de demonstrar a autoridade delegante que os objetivos propostos foram cumpridos, sejam elas técnicas e/ou preventivas, e que esses processos guardaram adequação (conformidade) com as regras e princípios estabelecidos, que comprovem a efetividade e a observância da proteção aos dados pessoais.

4.3.9. DA NÃO DISCRIMINAÇÃO

O presente princípio por seu nome já diz sua finalidade. O tratamento de dados não pode ser realizado para fins discriminatórios ilícitos ou abusivos. Não se pode ter exclusão de titulares de dados pessoais no momento de seu tratamento de dados por determinadas características, sejam elas de origem racial ou étnica, opinião política, religião ou convicções, geolocalização, filiação sindical, estado genético ou de saúde ou orientação sexual.

Não é dizer que nunca poderá ter uma setorização de tratamento de dados, porém somente poderá ocorrer tal restrição em condições específicas e previstas em lei, como por exemplo um tratamento de dados de alunos optantes por cotas, perante a Lei de Cotas 12.711/2012.

4.3.10. DA FINALIDADE

Com previsão no inciso primeiro do artigo 6º da LGPD, o princípio da finalidade emprega-se com o seguinte conceito "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades", em outras palavras, todo dado coletado deverá ter, no momento de seu colhimento, a indicação clara e completa que justifique sua coleta.

A LGPD obriga que as empresas tenham propósitos bem determinados ao tratar dados pessoais. Mas não apenas isto. Elas precisam também deixar claras as suas intenções para o titular dos dados, justificando e apontando o uso dos dados pessoais.

Ou seja, ao coletar um endereço de e-mail com a finalidade exclusiva de enviar um boleto bancário ou uma fatura para o cliente, por exemplo, a empresa não pode utilizar o e-mail para enviar ofertas e promoções.

4.4. DIRETRIZES

No atendimento ao que é requerido pela legislação e pelos compromissos assumidos nesta política, a Vortex Security seguirá, em seus processos, as seguintes diretrizes:

- Os dados pessoais do titular serão processados de forma lícita, leal e transparente;
- Os dados pessoais do titular serão coletados apenas para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de forma incompatível com essas finalidades (limitação das finalidades);
- Os dados pessoais do titular serão coletados de forma adequada, pertinente e limitada às necessidades do objetivo para os quais eles são processados (minimização dos dados);
- Os dados pessoais do titular serão exatos e atualizados sempre que necessário, de maneira que os dados inexatos sejam apagados ou retificados quando possível (exatidão);

- Os dados pessoais do titular serão conservados de forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados, (limitação da conservação, anonimização);
- Os dados pessoais do titular serão tratados de forma segura, protegidos do tratamento não autorizado ou ilícito e contra sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas (integridade e confidencialidade);
- É garantido ao titular dos dados a consulta gratuita sobre a forma e a duração do tratamento, bem como sobre a integridade de seus dados pessoais (transparência); (Art. 6º - IV e VI da Lei Federal n. 13.709);
- 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 (Art. 6º - X da Lei Federal n. 13.709);
- Assegurar que o tratamento de dados pessoais somente será realizado nas seguintes hipóteses:
    - Mediante o fornecimento de consentimento pelo titular quando assina o contrato de adesão aos serviços prestados pela organização;
    - Para o cumprimento de obrigação legal ou regulatória pelo controlador;
    - 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;
    - Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
    - 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;
    - 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);
    - Para a proteção da vida ou da incolumidade física do titular ou de terceiros;
    - Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
    - Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
    - Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
- Reconhecer que o tratamento de dados pessoais sensíveis representa riscos mais altos ao titular de dados pessoais e por esta razão a organização deve assumir o compromisso de resguardo e cuidados especiais frente ao tratamento de dados pessoais sensíveis.
- Os dados pessoais de crianças e adolescentes serão tratados com o mesmo nível de cuidado exigido e oferecido aos dados pessoais sensíveis, mas também estarão sujeitos às disposições próprias estabelecidas no Capítulo II, Seção III, da LGPD, e outras normas específicas aplicáveis.
- A realização de operações de tratamento de dados pessoais sensíveis pela Vortex Security somente poderá ser realizada:
    - Quando o titular de dados pessoais ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
    - Sem fornecimento de consentimento do titular de dados pessoais, nos casos em que o tratamento for indispensável para:
        - O cumprimento de obrigação legal ou regulatória pela Vortex Security;
        - A realização de estudos quando a Vortex Security estiver na posição de Órgão de Pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

- O exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
- Proteção da vida ou da incolumidade física do titular de dados pessoais ou de terceiros;
- Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
- Garantia da prevenção à fraude e à segurança do titular de dados pessoais, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

- Minimização e Finalidade: Os dados serão coletados apenas para finalidades legítimas e limitadas ao necessário.
- Segurança e Confidencialidade: Proteção contra tratamento não autorizado, perda ou destruição.
- Privacy by Design: A proteção de dados é integrada desde a fase de concepção de novos produtos, serviços ou processos internos, realizando análise previa.
- Registros de Tratamento: A organização manterá um registro atualizado de todas as atividades de tratamento de dados pessoais sob sua responsabilidade.
- Relatório de Impacto (DPIA): Realizar avaliações de impacto à proteção de dados para tratamentos que possam gerar riscos às liberdades civis.
- Atuação como Operadora (SOC): Nos serviços, a Vortex processará dados pessoais estritamente conforme as instruções documentadas do Cliente (Controlador), não utilizando tais dados para fins próprios.
- Apoio ao Controlador: A Vortex compromete-se a auxiliar seus clientes (Controladores) no atendimento aos direitos dos titulares e em eventuais consultas da ANPD.
- Subprocessadores: Qualquer contratação de terceiros (sub-operadores) que possam ter acesso a dados dos clientes do SOC deve ser informada e autorizada pelo Controlador original. Utilizamos ambientes cloud e ferramentas de terceiros, sempre garantindo que haja proteção em contrato.

4.5. DIREITOS DOS TITULARES DE DADOS PESSOAIS

O direito mais elementar da pessoa física em termos de proteção de dados é o de titularidade de seus dados pessoais.

Significa que, ao permitir o tratamento de seus dados pessoais, de modo algum e em nenhuma circunstância, a pessoa transfere a outrem a condição de dono de seus próprios dados pessoais.

O titular dos dados pessoais tem o direito de requisitar do controlador, a qualquer momento:

4.5.1. CONFIRMAÇÃO DA EXISTÊNCIA DE TRATAMENTO

O tratamento de dados é qualquer atividade relacionada a dados pessoais, como coleta, armazenamento, uso e classificação. Por lei, o titular dos dados tem o direito de confirmar se uma empresa realiza o tratamento de seus dados pessoais.

A LGPD estabelece ainda que a resposta pode ser feita de forma imediata e de maneira simplificada, ou por meio de declaração “clara e completa”, que indique a origem dos dados, os critérios usados e a finalidade do tratamento.

O prazo para a resposta no formato completo é de até 15 dias contado a partir da data do requerimento.

4.5.2. ACESSO AOS DADOS

Além de saber se a empresa trata seus dados pessoais, o titular também pode pedir acesso aos dados. Ou seja, é possível obter uma cópia dos dados pessoais que a empresa possui em seus arquivos.

Da mesma forma que a confirmação de tratamento, o acesso também pode ser respondido de forma imediata e simplificada ou por meio de declaração completa no prazo de até 15 dias contado da data do requerimento.

4.5.3. CORREÇÃO DOS DADOS

Outro direito do titular de dados é solicitar à empresa a correção de dados pessoais incompletos, inexatos ou desatualizados.

É o caso, por exemplo, de uma atualização de endereço, número de telefone ou estado civil.

4.5.4. ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO DE DADOS

Caso queira, o titular de dados também tem o direito de solicitar a anonimização (processo que torna um dado impossível de ser vinculado a um indivíduo), bloqueio ou eliminação de dados quando eles forem “desnecessários, excessivos ou tratados em desconformidade” com a lei.

Por exemplo, se a empresa trata dados que não são necessários para alcançar a finalidade do tratamento ou se o tratamento não é enquadrado em nenhuma das bases legais previstas na lei.

4.5.5. PORTABILIDADE DOS DADOS

A LGPD prevê ainda que o titular de dados pode solicitar a portabilidade dos dados, ou seja, a transferência das suas informações pessoais a outro fornecedor de serviço ou produto.

Neste caso, é preciso uma requisição expressa, seguindo uma regulamentação que deverá ser feita pela ANPD (Autoridade Nacional de Proteção de Dados), que ainda não está em operação.

Além disso, a portabilidade não inclui dados que já tenham sido anonimizados pelo controlador – dados anonimizados, aliás, ficam de fora do escopo da LGPD.

4.5.6. ELIMINAÇÃO DOS DADOS TRATADOS COM CONSENTIMENTO

Se o titular dos dados consentiu com o tratamento, mas mudou de ideia e não quer mais que a empresa trate seus dados pessoais, ele pode solicitar a eliminação desses dados.

4.5.7. INFORMAÇÕES SOBRE O COMPARTILHAMENTO DE DADOS

A LGPD preza, neste e em outros pontos, pela transparência, que é um dos princípios da lei que devem ser respeitados pelas empresas.

Desta forma, é direito do titular saber exatamente com quem o controlador está compartilhando seus dados. Isto inclui entidades públicas e privadas, que devem ser expressamente nomeadas, e não mencionadas apenas de forma genérica.

4.5.8. INFORMAÇÃO SOBRE A POSSIBILIDADE DE NÃO FORNECER CONSENTIMENTO

A premissa do consentimento é que ele seja pedido e concedido de forma clara, transparente e totalmente livre. Para isso, o titular de dados tem o direito de ser informado sobre a possibilidade de não fornecer o consentimento e de quais as consequências caso o consentimento seja negado.

É o caso, por exemplo, de um usuário que é convidado a consentir ou não com o uso de cookies em um site. Se o não consentimento for prejudicar a experiência de navegação ou impedir o acesso a algumas ferramentas, o usuário deve ser informado disso.

4.5.9. REVOGAÇÃO DO CONSENTIMENTO

Por fim, qualquer consentimento dado para o tratamento de dados pessoais pode ser revogado. Este é um direito do titular de dados, que pode fazer uma solicitação revogando o consentimento.

No entanto, vale lembrar que para que os dados tratados até então sejam de fato eliminados é preciso fazer uma requisição específica, conforme mencionamos no item 2.4.6.

4.5.10. OUTROS DIREITOS

Além dos 9 direitos principais dos titulares de dados previstos em seu artigo 18, a LGPD menciona outros, como, por exemplo:

- O direito do titular de dados de se manifestar contra o controlador na ANPD e nos órgãos de defesa do consumidor;
- O direito de opor-se ao tratamento realizado com dispensa de consentimento, caso não esteja em conformidade com a lei.

É importante ressaltar, no entanto, que nenhum direito é absoluto e que há situações em que as empresas podem não conseguir atender aos requerimentos do titular, devendo indicar os motivos -como, por exemplo, o cumprimento de obrigações legais ou regulatórias.

4.6. DEVERES PARA USO ADEQUADO DE DADOS PESSOAIS

Os deveres de cuidado, atenção e uso adequado de dados pessoais se estendem a todos os destinatários desta Política no desenvolvimento de seus trabalhos e atividades na Vortex Security, comprometendo-se a auxiliar a organização a cumprir suas obrigações na implementação de sua estratégia de privacidade e proteção de dados pessoais.

Todos devem reportar suspeitas de violações ao Encarregado (DPO). Em caso de incidentes envolvendo dados de clientes (SOC), a Vortex notificará o Cliente imediatamente para que este cumpra seu papel de Controlador

4.6.1. DEVERES ESPECÍFICOS DOS TITULARES DE DADOS PESSOAIS

Incumbe aos titulares de dados pessoais comunicar à Vortex Security sobre quaisquer modificações em seus dados pessoais na sua relação com a organização (e.g. mudança de endereço), notificando-a preferencialmente na seguinte ordem:

- Por meio da plataforma disponibilizada pela Vortex Security com a qual o titular se relaciona;
- Por e-mail endereçado ao responsável da Vortex Security com o qual o titular se relaciona;
- Por e-mail endereçado diretamente ao DPO da Vortex Security; e
- Por meio físico (e.g. carta) endereçado diretamente ao DPO da Vortex Security.
- Comunicar modificações em seus dados.

4.6.2. DEVERES ESPECÍFICOS DOS COLABORADORES E TERCEIROS

O compartilhamento de dados pessoais de titulares de dados pessoais entre os setores da Vortex Security é permitido, desde que respeitada a sua finalidade e base legal, observado o princípio da necessidade, ficando o tratamento de dados pessoais sempre restrito ao desenvolvimento de atividades autorizadas pela organização. Além disso, são deveres dos colaboradores e terceiros:

- Não disponibilizar nem garantir acesso aos dados pessoais mantidos pela Vortex Security para quaisquer pessoas não autorizadas ou competentes de acordo com as normas da organização;

- Obter a autorização necessária para o tratamento de dados e ter os documentos necessários que demonstrem a designação de sua competência para a realização da operação de tratamento de dados lícita, nos termos do arcabouço normativo da Vortex Security que será elaborado;
- Cumprir as normas, recomendações, orientações de segurança da informação, classificação de dados e prevenção de incidentes de segurança da informação publicadas pela organização.
- Respeitar a finalidade e base legal, não garantir acesso a pessoas não autorizadas e cumprir normas de segurança.

4.6.3. DEVERES DE TODOS OS DESTINATÁRIOS DESTA POLÍTICA

Todos os destinatários desta Política têm o dever de contatar o Encarregado da Vortex Security, quando da suspeita ou da ocorrência efetiva das seguintes ações:

- Operação de tratamento de dados pessoais realizada sem base legal que a justifique;
- Tratamento de dados pessoais sem a autorização por parte da Vortex Security no escopo das atividades que desenvolve;
- Operação de tratamento de dados pessoais que seja realizada em desconformidade com a Política de segurança da Informação da Vortex Security;
- Eliminação ou destruição não autorizada pela Vortex Security de dados pessoais de plataformas digitais ou acervos físicos em todas as instalações da Instituição ou por ela utilizadas;
- Qualquer outra violação desta Política ou de qualquer um dos princípios de proteção de dados.

4.7. RESPONSABILIDADES

- Conselho de Administração:
  - Aprovar a Política de Proteção de Dados Pessoais e Privacidade;
  - Deliberar sobre temas afetos às suas atribuições.
- Diretoria Executiva:
  - Promover o processo de atendimento às diretrizes aprovadas e garantir que estejam alinhados às boas práticas de gestão, inclusive ao planejamento estratégico da organização;
  - Deliberar sobre os procedimentos que sejam encaminhados pelo Encarregado no caso de ocorrências;
  - Encaminhar ao Conselho de Administração, para aprovação, os casos específicos que impliquem em decisões estratégicas;
  - Assegurar o alinhamento das ações de planejamento, promovendo as adequações necessárias por meio de padrões de funcionamento normatizados em suas respectivas diretorias;
  - Apoiar os líderes de segurança de dados pessoais e privacidade para o atendimento à lei.
- Controlador:
  - Tomar decisão referente ao tratamento de dados pessoais;
  - Delegar as ações necessárias para operacionalizar a Política da Proteção de Dados Pessoais e Privacidade dentro da estrutura da organização;
  - Exigir das pessoas físicas e das pessoas jurídicas, de Direito Público ou Privado, com quem se relaciona, o cumprimento dessa política quando aquelas estiverem tratando dados pessoais originários da Vortex Security.
- Comitê de Segurança de Dados Pessoais e Privacidade
  - Foro de discussão e proposição de melhorias na Política de Proteção de Dados Pessoais e Privacidade;

- Deve sugerir, acompanhar e reavaliar a implementação do Programa de Proteção de Dados Pessoais;
- Dar apoio ao Encarregado na execução das ações relativas à Política e ao Programa de Proteção de Dados Pessoais.

- Encarregado (DPO ou Data Protection Officer)
  - Receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
  - Receber comunicações da autoridade nacional e adotar providências;
  - Orientar os empregados e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
  - Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares; e
  - Coordenar as ações que visam implantar a Política de Proteção de Dados Pessoais e Privacidade.
- Líderes de Segurança e Dados Pessoais e Privacidade
  - Identificar os processos que possuem tratamento de dados pessoais;
  - Disseminar a Política de Proteção de Dados Pessoais e Privacidade;
  - Comunicar ao Encarregado (DPO) situações em desconformidade com a Política.
- Agentes Internos de Tratamento de Dados (Operadores Internos)
  - Realizar o tratamento de dados conforme as instruções fornecidas pelo Controlador – formalizadas através de Política e Normativos sobre tal matéria;
  - Identificar e relatar ao Líder e ao Encarregado situações-problema que possam pôr em risco a segurança da informação e privacidade.

4.8. TRANSFERÊNCIA INTERNACIONAL DE DADOS

A transferência internacional de dados na LGPD é um fator de grande impacto entre países que possuem e os que ainda não regulamentaram o tratamento de dados, isso porque leis como a GDPR e até a própria LGPD possuem regras mais rígidas no processo de tratamento de dados nesses casos.

Os requisitos e as hipóteses para a transferência internacional de dados estão previstos no Capítulo V, art. 33 e seguintes da LGPD. Conforme art. 33 da LGPD, a transferência internacional de dados só é permitida em nove hipóteses:

- Para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
- Quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
  - cláusulas contratuais específicas para determinada transferência;
  - cláusulas-padrão contratuais;
  - normas corporativas globais;
  - selos, certificados e códigos de conduta regularmente emitidos;
- Quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
- Quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros;
- Quando a autoridade nacional autorizar a transferência;

- Quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
- Quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
- Quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente essa de outras finalidades; ou
- Quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

5. NOMEAÇÃO DO ENCARREGADO

O encarregado de dados pessoais nomeado é:
HENRIQUE CARVALHO

O encarregado substituto nomeado é:
REGINALDO SARRAF.