ÍNDICE DE REVISÕES

REVISÃO	STATUS	DESCRIÇÃO
0	AP	Elaboração inicial do documento.

PA - PARA APROVAÇÃO	CA - CANCELADO	PR - PRELIMINAR
PI - PARA INFORMAÇÃO	AP - APROVADO	LI - LIBERADO

REVISÃO	REV. 0	REV. A	REV. B	REV. C	REV. D	REV. E	REV. F	REV. G
DATA	05/05/2022							
ELABORAÇÃO	CARLOS C.							
ANÁLISE CRÍTICA	ADRIANA S.							
PADRONIZAÇÃO	ADRIANA S.							
APROVAÇÃO	PAULO M.							

Sumário

1. ATA DE APROVAÇÃO

A ata de aprovação desta política encontra-se devidamente assinada e arquivada na plataforma UniVoce, no Curso Treinamentos Corporativos – Normas e Políticas Internas, acessível a todos os públicos.

URL de Acesso: https://univoce.com.br/enrol/index.php?id=46

2. ABRANGÊNCIA

Abrangência interna e externa, para todos os colaboradores, clientes, fornecedores, parceiros e demais utentes que queiram conhecer esta Política.

3. POLÍTICA

3.1 Obrigação de uso de recursos em versões seguras e atualizadas

A empresa e seus desenvolvedores procurarão, dentro das possibilidades existentes, utilizar recursos de segurança da informação e de tecnologia da informação de qualidade, eficiência e eficácia reconhecidas e em versões comprovadamente seguras e atualizadas, de forma a reduzir o nível de risco ao qual o objeto do contrato e/ou a contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela contratante.

3.2 Reportar Incidentes

Quando tomar conhecimento de ocorrência de algum Incidente de segurança, os envolvidos da empresa deverão reportar o ocorrido ao Contratante, nos termos do que for estabelecido no Procedimento de Suporte a Incidentes Críticos Plano de Comunicação de Incidentes de Segurança .

3.3 Assinatura de Termos de Compromisso de Confidencialidade

Todos os colaboradores que estiverem envolvidos na execução de contratos da empresa deverão assinar o Termo de Compromisso de Confidencialidade sobre as informações do Contratante e das pessoas que têm dados tratados nos sistemas da empresa.

3.4 Descarte seguro de dados

3.4.1 O descarte de dados nos sistemas desenvolvidos pela empresa é uma decisão do Contratante (Controlador de Dados), embora a empresa possa emitir recomendações quanto aos critérios para realização desse tipo de descarte;

3.4.2 Após o encerramento de um Contrato, os responsáveis, dentro da empresa deverão realizar a transferência da base de dados para o Contratante;

3.4.3 Essa base deverá ser excluída dos bancos da empresa, salvo em caso de concordância expressa do Controlador quanto à manutenção desses dados nos sistemas da empresa.

3.5 Contratação de suboperadores

3.5.1 Caso a empresa precise contratar terceiros para auxiliar na execução dos contratos (exemplo: contratação de serviço de armazenamento em nuvem), estes serão considerados como suboperadores de dados.

3.5.2 A contratação de suboperador de dados deverá ocorrer por meio de anuência da contratante.

3.6 Adoção de controles de segurança da informação

A empresa se compromete a adotar sistemas de controles de segurança da Informação que deverão sempre ser aperfeiçoados objetivando reduzir os riscos de segurança da informação presentes em suas operações.

3.7 Apresentação de documentação à Contratante

3.7.1 A empresa deverá manter documentação atualizada comprovando o cumprimento de requisitos para adequação à Lei Geral de Proteção de Dados;

3.7.2 Serão considerados como parâmetros para que a empresa possa se considerar adequada (previstos no Artigo 50, §2º, II da LGPD):

- demonstrar o comprometimento em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
- correção de processos relacionados a todo o conjunto de dados pessoais que esteja sob seu controle, independentemente do modo como se realizou sua coleta;
- existência de programa adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
- estabelecimento de políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- estabelecimento de relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
- integração do programa de privacidade com a estrutura geral de governança da empresa, estabelecendo e aplicando mecanismos de supervisão internos e externos;
- elaboração de planos de resposta e remediação a incidentes;
- atualização constante do Programa de Adequação a Lei Geral de Proteção de Dados.

3.7.3 A empresa permitirá que as contratadas realizem auditorias para verificação de cumprimento dos critérios de adequação previstos na Lei 13;907/2018.

3.8 Tratamento de Incidentes de Segurança da Informação e Privacidade

A empresa se compromete a, em conjunto aos seus contratantes, realizar ações de tratamentos de incidente visando minimizar os prejuízos a privacidade dos titulares que tem dados tratados em seus sistemas;

3.9 Revisões

Esta política será revisada com periodicidade anual.

3.10 Gestão da Política

3.10.1 A Política de Diretrizes para Atuação como Operador de Dados Pessoais é aprovada pela Diretoria da empresa, devendo ser revisada anualmente pelo Comitê Gestor de Proteção de Dados Pessoais ou

conforme solicitação de revisão pontual expressa por qualquer pessoa, por meio de abertura de chamados no sistema Meu HelpDesk (www.meuhelpdesk.com.br), ou ainda identificação de mudança na legislação atual que impacte o conteúdo abordado nessa Política.

3.10.2 Essa Política precisa estar atualizada em sua última versão na plataforma UniVoce, no Curso Treinamentos Corporativos – Normas e Políticas Internas conforme acesso anteriormente citado.

4. DIRETRIZES

4.1 Objetivo

4.1.1 Segundo definido na Lei 13.709/2018 (Lei Geral de Proteção de Dados), o Controlador é ‘’pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais’’ (Artigo 5º, VI, da LGPD). **Dessa forma, quem tem o poder de decidir sobre os tratamentos a serem realizados é o controlador.**

4.1.2 Segundo definido na Lei 13.709/2018 (Lei Geral de Proteção de Dados), o operador é ‘’pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador’’ (Artigo 5º, VII, da LGPD). **Dessa forma, o operador deve realizar o tratamento de dados de acordo com as orientações emanadas pelo controlador.**

4.2 Atribuições e Responsabilidades

4.2.1 Fica estabelecido que a empresa, em sua atuação como desenvolvedora de sistemas, será classificada como Operadora de Dados Pessoais.

4.2.2 Dentro de sua condição de Operadora de Dados Pessoais, deverá:

- Procurar seguir as orientações emanadas pelo cliente (Controlador de Dados), desde que estejam de acordo com o ordenamento jurídico brasileiro e não violem o Direito Fundamental à Proteção de Dados Pessoais dos titulares que têm dados tratados nos sistemas da empresa;
- Quando uma ordem emanada pelo controlador for aparentemente ilegal, deverá o responsável consultar o Setor Jurídico (ou Consultoria). Em caso de parecer jurídico negativo, é recomendável o encaminhamento de ofício ao município arrazoando a ilegalidade da ordem;
- Enquanto operador, a responsabilidade pelos recursos usados nos sistemas e sobre os controles de segurança utilizados cabem à empresa. Por isso, o cuidado da empresa com a existência de controles de segurança da informação no software deve ser constante.