AEVO TECNOLOGIA DA INFORMAÇÃO S/A

RELATÓRIO DE IMPACTO

À PROTEÇÃO DE DADOS PESSOAIS

Vitória, 28 de Março de 2023

AEVO TECNOLOGIA DA INFORMAÇÃO S/A

Histórico de Revisões

Data	Versão	Descrição	Autor
11/11/2021	1.0	Conclusão da primeira versão do relatório	Alef Souza
12/04/2022	1.1	Adição do Item 3.1.4	Alef Souza
28/03/2023	1.2	Revisões Gerais	Pedro Henrique Moura

AEVO TECNOLOGIA DA INFORMAÇÃO S/A

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

OBJETIVO
O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os 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. **Referência:** Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador	
Operador	
AEVO TECNOLOGIA DA INFORMAÇÃO S.A	
Encarregado	
Marcelo Côgo	
E-mail Encarregado	**Telefone Encarregado**
<Marcelo.cogo@aevo.com.br>	(27) 99737-1764

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

Os serviços oferecidos pela AEVO, através do software AEVO, realizará o tratamento de dados pessoais de colaboradores e outros que sejam compartilhados pela controladora para a execução de contrato entre as partes. A elaboração do relatório tem como base o interesse legítimo da Controladora (LGPD, art. 10, § 3º) em relação aos processos de tratamento de dados que serão realizados pela Operadora durante o período de vigência do contrato estabelecido entre as partes.

Durante a execução do contrato e prestação, a Operadora realizará o tratamento de dados cuja natureza, em caso de vazamento ou incidente de segurança, pode resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados (LGPD, art. 42).

3 – DESCRIÇÃO DO TRATAMENTO

3.1 – NATUREZA DO TRATAMENTO

3.1.1 Os dados pessoais são coletados nos seguintes cenários:

1. Compartilhamento, resultando em leitura dos dados a partir de um Provedor de Identidade onde os dados dos colaboradores que receberão acesso ao sistema estão armazenados.
2. Preenchimento e Importação de Planilha Eletrônica com os dados de acesso a ser importada na plataforma da AEVO.
3. Cadastro de usuário por meio do uso da API do AEVO em formato JSON.
4. Preenchimento de formulário eletrônico no portal da plataforma AEVO.

Após receber os dados do usuário, esses dados são armazenados em um banco relacional SQL Server no Microsoft Azure, onde serão armazenados durante toda a vigência do contrato. Os dados serão processados posteriormente para autorização de usuários na plataforma e sua exibição na plataforma, com o intuito de identificar o usuário logado e criar uma associação entre o usuário e suas atividades no sistema.

A Controladora pode solicitar a qualquer momento, através da plataforma de suporte ou do portal administrativo, ou pelos canais de comunicação oficiais com o DPO, alterações, correções e, ou, exclusão de dados da plataforma.

3.1.2 A fonte de dados é a Controladora, mediante esta ter coletado de seus colaboradores e demais indivíduos participantes no serviço o consentimento inequívoco para o compartilhamento de dados pessoais coletados desses, de acordo com o estabelecido na Lei Geral de Proteção de Dados.

3.1.3 São compartilhados com a Microsoft, fornecedora de Cloud, todos os dados adquiridos na etapa de coleta.

3.1.4 Poderão ser compartilhados com a Amazon Web Services, fornecedora de Cloud, através do processo de armazenamento de dados, todos os dados de identificação armazenados no banco de dados da aplicação, com o objetivo de fornecer serviços de BI ao cliente, caso tenha o serviço adquirido em seu contrato.

3.1.5 A Microsoft, através de seus serviços, realiza o enriquecimento de dados e coleta e armazena dados de navegação do usuário como tipo do dispositivo, IP do dispositivo, cidade, estado, e país de origem do IP, navegador e a versão utilizada. Esse processo é realizado de forma automática e acontece durante a interação do usuário com o serviço de SaaS fornecido pela AEVO. Esses dados serão utilizados exclusivamente para fins de monitoramento, correlação de eventos para análise de erros e análise do uso da aplicação.

3.1.6 A exclusão definitiva dos dados acontecerá mediante encerramento da vigência de contrato ou distrato entre as partes no prazo de 15 dias úteis. A exclusão refere-se à eliminação completa do recurso de banco de dados onde os dados estavam armazenados até o momento. Backups poderão ser providenciados e os dados poderão ser exportados também estarão a disponibilidade da Controladora mediante solicitação.

3.1.7 Backups automáticos mantidos pelo Azure, de acordo com a última janela de operação,

poderão estar disponíveis por até 35 dias. Esses serão completamente eliminados após o encerramento do prazo de armazenamento dado a inexistência do recurso para realizar a operação. Os Backups disponíveis serão armazenados pela provedora de forma criptografada com uma chave de criptografia AES-256(https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview?tabs=azure-portal#service-managed-transparent-data-encryption).Backups com longo prazo de retenção (até 5 anos), em caso da contratação dos mesmos, também serão armazenados internamente pela provedora de nuvem seguindo os mesmos princípios de segurança aplicados aos backups padrão.

3.1.8 Os dados coletados através dos serviços do Microsoft Azure serão armazenados diretamente em serviço de dados também da Microsoft, localizado no Brasil, especializado no processamento de logs, cuja finalidade é validar o fornecimento constante do serviço, garantindo a execução contratual, e a melhoria constante dos serviços oferecidos.

3.2 – ESCOPO DO TRATAMENTO

3.2.1 Os dados pessoais tratados pela plataforma AEVO abrangem:

1. Informação de identificação pessoal - Obrigatórios: Nome ou nome de usuário, e-mail, departamento do usuário.
2. Dados de identificação eletrônica (Coletados automaticamente): Endereço IP do dispositivo eletrônico, Cidade, Estado e País do IP do dispositivo. Browser e Sistema Operacional e suas respectivas versões.
3. Vídeo e imagem: Foto do usuário.
4. Outros dados não obrigatórios: Localização, matrícula ou número de identificação funcional, cargo e subdivisão.

3.2.2 A quantidade de dados pessoais tratados são 16 dados pessoais e 0 dados sensíveis. A frequência de tratamento é 24x7(24 horas dia, 7 dias na semana) para acesso e utilização da plataforma.

3.2.3 Os dados pessoais tratados serão armazenados durante toda a vigência do contrato estabelecido entre as partes.

3.2.4 O número de titulares afetados pelo tratamento será definido de acordo com o número de usuários contratos pela Controladora e os dados que serão efetivamente compartilhados pelas partes.

3.2.5 A abrangência do tratamento de dados pessoais é nacional. Todos as etapas relacionadas ao tratamento serão realizadas em serviços localizados no Brasil.

3.3 – CONTEXTO DO TRATAMENTO

3.3.1 A natureza do relacionamento dos usuários (colaboradores da Contratante) do AEVO com a

AEVO é baseada no acesso a plataforma, através de sua identificação no momento de autenticação na plataforma, na autorização (permissões de ações na plataforma atribuídas ao usuário acessando) e na vinculação e identificação de um usuário a uma atividade dentro da plataforma.

3.3.2 Qualquer atualização, compartilhamento dos dados pessoais ou acessos suspeitos à AEVO serão avisados à Controladora. O usuário poderá solicitar alterações de seus dados, entretanto, as solicitações serão comunicadas à Controladora e somente serão realizados após o aceite da Controladora para a realização da operação.

3.3.3 Dados de crianças e adolescentes não fazem parte do escopo de dados que serão tratados.

3.3.4 O tratamento de dados é realizado de acordo com a expectativa da Controladora.

3.3.5 A AEVO detém boa experiência em tratamento de dados pessoais e tem estabelecido ações para implementação (conformidade) do previsto pela LGPD.

3.3.6 A AEVO utiliza recursos de segurança robustos (SaaS + PaaS + Cloud) e está investindo ainda mais através certificações em segurança da informação, ISO 27001, e em processos robustos de detecção em tempo real de ameaças.

3.4 – FINALIDADE DO TRATAMENTO

3.4.1 Garantir que a execução do contrato de prestação de serviços firmado entre a partes possa ser realizado de acordo com o legítimo interesse da Controladora com o objetivo de apoiar e promover as atividades do Controlador.

3.4.2 Os resultados pretendidos para os titulares de dados pessoais são: Permitir que os usuários possam acessar e utilizar o sistema de acordo com os módulos contratados e as funcionalidades relacionadas aos módulos. Permitir que os administradores possam segmentar e controlar adequadamente o nível de acesso a tarefas administrativas dentro do sistema e o nível de acesso às diferentes centrais, caso mais de uma tenha sido contratado.

4 – PARTES INTERESSADAS CONSULTADAS

4.1 Assistente em Segurança da informação, Analista de DevOps e DPO da Operadora, que desempenhou o papel de conduzir o levantamento dos dados coletados e tratados pela AEVO e apreciar as informações técnicas, administrativas e legais e de risco referentes aos processos da Operadora.

5 – NECESSIDADE E PROPORCIONALIDADE

5.1 – FUNDAMENTAÇÃO LEGAL

5.1.1 A hipótese legal para o tratamento de dados pessoais é o art. 7º, V - 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(...) e, IX - 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(...)

5.2 – QUALIDADE E MINIMIZAÇÃO DE DADOS

5.2.1 A escolha dos dados coletados, obrigatórios, segue o princípio do mínimo necessário para garantir o acesso aos serviços básicos oferecidos pela Operadora. Os dados opcionais têm como objetivo incrementar as funcionalidades básicas da aplicação com o intuito de oferecer maior controle para os gestores da aplicação em relação à gestão de permissões e acessos dos usuários as funcionalidades oferecidas. Os dados opcionais apenas serão coletados caso a Controladora manifeste interesse em utilizar tais funcionalidades.

5.2.2 Está previsto para o ano de 2023 a implementação da ISO 27001 na Operadora, trazendo ainda mais mecanismos e procedimentos para melhorar o processo de análise de dados e trazer garantias para a qualidade de dados.

5.3 – MEDIDAS PARA ASSEGURAR DIREITOS DO TITULAR DOS DADOS

5.3.1 A AEVO disponibiliza para a Controladora a plataforma Movidesk no https://aevo.movidesk.com para contato e solicitações referentes a uso da plataforma, para que a Controladora possa demandar as solicitações previstas pelo art. 18º da LGPD. A Política de Privacidade informa sobre o direito que o titular dos dados pessoais tem de realizar qualquer uma das referidas solicitações. A Política de Privacidade pode ser encontrada no sítio da AEVO no link https://aevo.com.br/politica-de-privacidade nas Políticas de Privacidade do AEVO. Caso o usuário identifique alguma falha ou vulnerabilidade de segurança no sistema, é possível reportá-la também pela Movidesk.

5.4 – SALVAGUARDAS PARA AS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS

5.4.1 A AEVO não realiza qualquer tipo de transferência internacional de dados.

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de

				Risco (P x I)
R01	Acesso não autorizado.	5	10	50
R02	Modificação não autorizada.	10	5	50
R03	Perda.	5	5	25
R04	Roubo.	5	15	75
R05	Remoção não autorizada.	5	10	50
R06	Coleção excessiva.	10	10	100
R07	Informação insuficiente sobre a finalidade do tratamento.	5	15	75
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	5	15	75
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	75
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	10	100
R11	Retenção prolongada de dados pessoais sem necessidade.	5	5	25
R12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	10	50
R13	Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada, etc.).	5	10	50
R14	Reidentificação de dados pseudonimizados.	5	5	25

Legenda: P – Probabilidade; I – Impacto.

[1] Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

[2] Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

[3] Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

AEVO TECNOLOGIA DA INFORMAÇÃO S/A

7 – MEDIDAS PARA TRATAR OS RISCOS

<Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46.).>

<Importante reforçar que as medidas para tratar os riscos podem ser: de segurança; técnicas ou administrativas.

<A coluna "Medida(s)" pode ser preenchida com uma medida de segurança ou controle específico adotado para tratamento do risco identificado na seção 6 deste Relatório.>

<A instituição nem sempre precisa eliminar todos os riscos. Nesse sentido, pode-se decidir que alguns riscos são aceitáveis - até um risco de nível alto-, devidos aos benefícios do processamento dos dados pessoais e as dificuldades de mitigação. **No entanto, se houver um risco residual de nível alto, é recomendável consultar a ANPD antes de prosseguir com as operações de tratamento dos dados pessoais**.>

Risco	Medida(s)	Efeito sobre o Risco[1]	Risco Residual[2]			Medida(s)[3] Aprovada(s)
			P	I	Nível (P x I)	
R06 - Coleção excessiva.	1. Limitação da coleta de acordo com o estabelecido na Política de Dados e Privacidade.	Reduzir	5	10	50	Sim
R10 - Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	1. Controle de Acesso Lógico a nível de Banco de dados. 2. Política estabelecendo procedimentos para validação de compartilhamento de dados.	Reduzir	5	10	50	Sim

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6.

[1] Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.

[2] Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratar o risco.

[3] Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.