Política de Privacidade e Proteção de Dados Pessoais

Elaborado por:	Verificado por:	Aprovado por:
Gerente de TI	Diretoria Estatutária e Comitê de Auditoria	Conselho de Administração

SUMÁRIO

1.0 – OBJETIVO:

A Política é utilizada para estabelecer a forma como os Dados Pessoais são coletados, armazenados e descartados pela Companhia, assegurando que são colocados em prática mecanismos que garantam que o Tratamento dos Dados Pessoais seja compatível com os princípios da Priner, bases legais, direitos dos Titulares e demais disposições previstas na LGPD, além de garantir a utilização de medidas técnicas e administrativas aptas à proteção dos Dados Pessoais.

2.0 – CONSIDERAÇÕES GERAIS:

A "Priner" ou "Companhia", em conformidade com a Lei nº 13.709/ 2018 ("Lei Geral de Proteção de Dados" ou "LGPD") e demais normas e regulamentos correlatos, elaborou a presente Política de Privacidade e Proteção de Dados Pessoais ("Política"), com intuito de reafirmar o compromisso da Companhia com as melhores práticas de proteção dos Dados Pessoais utilizados, compartilhados e/ou armazenados pela Companhia, decorrentes da relação com seus colaboradores, acionistas, prestadores de serviços, fornecedores, clientes, parceiros comerciais e terceiros. ("Titular(es)").

A Companhia entende que, nos termos da LGPD, desempenha o papel de Controladora e Operadora dos Dados Pessoais, uma vez que é responsável pelo recolhimento e tratamento dos dados obtidos, exceto nas relações contratuais.

3.0 – TERMOS E DEFINIÇÕES:

Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao Tratamento de dados pessoais.

Dados Pessoais: Toda e qualquer informação relativa a uma pessoa física singular identificada ou identificável, ou seja, que possa ser identificada, direta ou indiretamente, tal como nome, número de identificação ou elementos específicos de sua identidade física, fisiológica, genética, psíquica, econômica, cultural ou social, dentre outras.

Dados Sensíveis: Consideram-se dados pessoais sensíveis os dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, além de dados referentes à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Encarregado ou DPO (*Data Protection Officer*): 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).

LGPD (Lei Geral de Proteção de Dados): Lei Federal nº 13.709, de 14 de agosto de 2018, legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.

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

Titulares: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Neste caso, qualquer pessoa, administrador, funcionário e/ou investidor (pessoa física) que, de qualquer forma, disponibilize seus dados para a Priner.

Dependentes: Qualquer pessoa natural vinculada ao titular, podendo ser cônjuge ou filho (as), enteados (as), curatelados (as) e/ou tutelados (as), dependentes economicamente do titular, que, por qualquer razão, tenha seus Dados Pessoais disponibilizados para a Priner.

Tratamento: É toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Colaboradores: Funcionários e estagiários.

Terceiros: Qualquer pessoa física ou jurídica que possa se relacionar com a Companhia, como por exemplo: clientes, prestadores de serviço, fornecedores, parceiros comerciais, membros dos órgãos da administração.

4.0 – DIRETRIZES:

4.1 – Tratamento de dados:

4.1.1 – Tratamento dos dados pessoais:

A Companhia realizará o Tratamento dos Dados Pessoais, inclusive Dados Sensíveis dos Titulares para os fins de atendimento a todos os requerimentos legais que envolvam tais relacionamentos, bem como para os especificados abaixo:

Colaboradores ou seus dependentes:

a) Permitir a plena execução dos contratos de trabalho:

A Companhia tratará os Dados Pessoais dos seus colaboradores, inclusive dados bancários e/ou financeiros, tais como números de cadastro, números de agência e conta bancária, dentre outros, com a finalidade de viabilizar a execução do trabalho, realizar o pagamento da remuneração e amparar o colaborador em toda e qualquer situação que demande o Tratamento de seus Dados Pessoais.

b) Permitir a execução de contratos acessórios aos contratos de trabalho:

A Companhia tratará os Dados Pessoais dos colaboradores e de seus Dependentes, quando for o caso, incluindo números de cadastro, dados e informações de familiares e Dependentes, dentre outros, para permitir o gozo de benefícios por ela fornecidos, como planos de saúde, assistência

odontológica, vale refeição, vale alimentação, seguro de vida, dentre outros benefícios possivelmente oferecidos enquanto vigente o contrato de trabalho celebrado.

c) Zelar pela saúde:

A Companhia poderá tratar os Dados Pessoais dos colaboradores e seus Dependentes, quando for o caso, incluindo Dados Sensíveis relacionados à saúde, tais como aqueles que tiver acesso através de serviços de saúde junto a planos médico-hospitalares, campanhas de vacinação e incentivo à saúde, atendimento médico em caso de acidente ou doença ocupacional e qualquer outro procedimento vinculado à saúde. Dados esses restritos ao médico do trabalho e demais profissionais de saúde, nos termos de regulamentação específica.

d) Zelar pela segurança e incolumidade física e evitar fraudes:

A Companhia poderá tratar os Dados Pessoais dos colaboradores, incluindo Dados Sensíveis biométricos, para zelar pela segurança dos colaboradores e terceiros, incluindo para o controle de acesso às suas dependências, bem como para evitar fraudes de identidade, mediante o uso de identificação biométrica.

e) Cumprir com obrigações legais e regulatórias:

A Companhia tratará os Dados Pessoais dos colaboradores, inclusive Dados Sensíveis, tais como qualificação completa, afiliação sindical, documentos pessoais, dados relacionados à origem racial ou étnica, dados bancários e previdenciários, exames admissionais e outros, para cumprir com obrigações dispostas por lei, por regulações de órgãos governamentais, por autoridades fiscais, pelo Poder Judiciário e/ou por qualquer outra autoridade competente.

f) Exercício de direitos:

A Companhia tratará os Dados Pessoais dos colaboradores e de seus Dependentes, quando for o caso, inclusive após o término da relação contratual, para exercer os seus direitos garantidos por lei, incluindo para utilização como prova em processos judiciais e administrativos.

g) Para o cumprimento das finalidades de suas operações:

A Companhia poderá tratar e compartilhar os Dados Pessoais de seus colaboradores para finalidades legítimas envolvendo a operação e a continuidade de suas atividades, incluindo a análise e condução de relatórios internos, levantamento e análise de estatísticas, organização interna de processos e procedimentos, bem como negociações e operações societárias. Nestes casos, o Tratamento somente poderá ocorrer se estritamente necessário para o alcance dessas finalidades.

h) Excepcionalmente para outras finalidades, com consentimento:

A Companhia poderá tratar outros Dados Pessoais de seus colaboradores e de seus Dependentes, desde que estes compreendam e de forma expressa consintam, que este tratamento seja necessário, adequado e atenda a uma finalidade específica. Da mesma forma, o Titular terá a possibilidade de retirar o seu consentimento a qualquer momento, bastando comunicar à Companhia.

Acionistas, Membros do órgão da administração (Conselhos, Diretoria e Comitês), Clientes, Prestadores de Serviços, Parceiros Comerciais, Candidatos a cargos disponíveis, dentre outros terceiros:

a) Para ofertar, fornecer e executar seus serviços:

A Companhia poderá tratar Dados Pessoais que sejam necessários para ofertar, fornecer e executar seus serviços, como, por exemplo, nome, documento de identidade, telefone, endereço eletrônico de representantes legais, dentre outros.

b) Para a contratação de serviços de terceiros:

A Companhia poderá tratar Dados Pessoais que sejam necessários para a contratação de serviços de terceiros, como, por exemplo, nome, documento de identidade e telefone de representantes legais, dentre outros.

c) Para segurança das nossas sedes dependências:

Quando o Titular visita uma das nossas sedes e espaços, podemos coletar seu nome, documento de identidade, foto e imagens de câmeras de segurança.

d) Para a seleção de candidatos a cargos na Companhia:

A Companhia poderá tratar Dados Pessoais inclusos nos currículos enviados, bem como Dados Pessoais coletados durante entrevistas, como nome, telefone, e-mail, formação acadêmica, experiência profissional, idiomas, entre outros que possam ser necessários para cada processo de seleção.

4.1.2 – Coleta e Recepção dos Dados:

a) Dados coletados automaticamente:

A Companhia coleta uma série de informações de modo automático, tais como: características do dispositivo de acesso, do navegador, IP (com data e hora), origem do IP, informações sobre cliques, páginas acessadas, as páginas seguintes acessadas após a saída das páginas, ou qualquer termo de procura digitado nos sites ou em referência a estes, dentre outros. Para tal coleta, a Companhia fará uso de algumas tecnologias padrões, como *cookies*, *pixel tags*, *beacons* e *local shared objects*, que são utilizadas com o propósito de melhorar a experiência de navegação do Titular nas páginas, de acordo com seus hábitos e suas preferências.

4.1.3 – Acesso e Armazenamento de Dados:

Após a sua coleta e recepção dos Dados, estes são armazenados em um servidor interno da Companhia, sempre disponível em ambiente de nuvem ("Base de Dados") e na rede da Companhia, com acesso restrito aos departamentos responsáveis pelas áreas de recursos humanos, tecnologia da informação e marketing da Companhia, conforme o caso, os quais possuem procedimentos de segurança para proteger a confidencialidade, segurança e integridade dos Dados Pessoais, a fim de prevenir a ocorrência de eventuais danos em virtude do Tratamento, como invasões, vazamentos e exclusões dos Dados Pessoais.

4.1.4 – Acesso dos Dados de Colaboradores Internos:

Além das medidas de proteção dos Dados Pessoais e do Banco de Dados descritos no item 4.3 desta Política, a Companhia confere acesso restrito e limitado a determinados funcionários para garantir o bom funcionamento, manutenção, correção e proteção dos Dados Pessoais.
Para tanto, o acesso ao Banco de Dados se dará mediante identificação por meio de um login e senha de acesso, gerados exclusivamente para determinados funcionários da Companhia, além da empresa contratada pela Companhia, responsável pelo apoio e suporte tecnológico.

Os funcionários com acesso ao Banco de Dados aderem, integralmente, aos princípios de ética e conduta da Companhia por meio da anuência ao Código de Ética e Conduta da Companhia.

4.1.5 – Compartilhamento de Dados:

Os Dados Pessoais, inclusive Dados Sensíveis, poderão ser compartilhados com pessoas jurídicas de direito público, clientes, sindicatos, órgãos de classe, na forma da lei, além de empresas prestadoras de serviços como planos de saúde, seguradoras e administradoras de benefícios e seguradoras, empresas de vale alimentação, vale transporte, dentre outros, quando aplicável e sempre observando a finalidade do Tratamento dos Dados Pessoais.

Nas hipóteses de compartilhamento de Dados Pessoais com terceiros, todos os sujeitos receptores da informação deverão utilizar os Dados Pessoais partilhados de maneira consistente e de acordo com os propósitos para os quais foram coletados (ou com os quais os Titulares consentiram previamente) e de acordo com o que foi determinado por esta Política, tendo, os terceiros, o dever de observar as limitações de autorização concedidas pelos Titulares dos Dados, não sendo responsabilidade da Companhia quaisquer infrações cometidas por terceiros ou desvio de finalidade na utilização dos Dados cometido por estes.

Importante lembrar que a Priner não vende ou aluga informações sobre Usuários para ninguém, apenas cede o acesso aos mesmos, gratuitamente, a seus parceiros efetivos ou potenciais, os quais, dessa forma, não adquirem qualquer propriedade sobre tais dados. Mesmo em relação a dados divulgados gratuitamente, a seus parceiros, o Usuário sempre terá tido a opção de não permitir a transferência quando da manifestação de aceitação ou não dos cookies. Se o Usuário desejar que seus dados não sejam compartilhados, poderá optar por não usar um determinado serviço.

4.1.6 – Descarte de Dados Pessoais:

A Companhia realizará o descarte dos Dados Pessoais coletados sempre que solicitado pelo Titular ou após o seu desligamento ou término da relação contratual com a Companhia, da seguinte forma:

Descarte do Dados Pessoais recebidos de colaboradores internos (funcionários, administradores e investidores):

É realizado por meio de uma empresa terceirizada especializada. A Companhia poderá manter armazenados os Dados Pessoais recebidos de colaboradores internos, pelo máximo período permitido em lei, a contar do rompimento da ligação do Titular com a Companhia.

Descarte do Dados Pessoais recebidos de terceiros (clientes, prestadores de serviço, fornecedores e parceiros comerciais):

A Companhia realizará o descarte dos Dados Pessoais dos Titulares na forma e no prazo da lei.
A Companhia poderá manter armazenados os Dados Pessoais obtidos de colaboradores externos, pelo máximo período permitido em lei.
Os Titulares ficam cientes que a eliminação dos Dados não ocorrerá quando sua manutenção for necessária para:

a) cumprimento de obrigação legal ou regulatória pelo Controlador;
b) exercício regular de direitos em processo judicial, administrativo ou arbitral; ou
c) uso exclusivo do Controlador, vedado seu acesso por terceiro e, desde que anonimizados os dados.

4.2 – Direitos do titular:

Enquanto a Companhia for detentora do Tratamento dos Dados Pessoais, o Titular poderá exercer todos os direitos garantidos pela LGPD a qualquer momento, inclusive os especificados a seguir:

i. Direito de acessar as informações correspondentes a si, em formato estruturado, acessível e facilitado, como também a liberalidade de solicitar cópia das informações que a Companhia possui sobre seus Dados, tendo como garantia o processamento desses de forma lícita, leal e transparente.

ii. Direito de corrigir os Dados que considere imprecisos, incompletos ou desatualizados.

iii. Direito de requisitar que os Dados correspondentes a si, sejam apagados de todos os registros da Companhia, como também a anonimização e o bloqueio deles, desde que sua manutenção e armazenamento não esteja prevista em lei ou em desacordo com os contratos firmados com terceiros.

iv. A certeza de que os Dados Pessoais serão coletados de forma adequada, pertinente e limitada às necessidades do objetivo para os quais eles são processados, de forma que esses sejam exatos e atualizados sempre que necessário.

v. Direito de obter informações sobre as entidades públicas ou privadas com as quais a Companhia compartilhou seus Dados.

4.3 – Ferramenta de proteção dos dados e segurança da informação:

A Companhia adota medidas de segurança técnicas e administrativas aptas a proteger os Dados Pessoais dos Titulares de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de Tratamento de Dados inadequado ou ilícito.

Essa análise de risco visa possibilitar a identificação, avaliação, tratamento, monitoramento e comunicação de riscos operacionais, tecnológicos e de imagem, além de possibilitar a aplicação de medidas que afastam a vulnerabilidade e ameaças à quebra de segurança da rede e do sistema utilizado pela Companhia.

É estipulado junto aos colaboradores da Companhia o uso de um login de acesso único, pessoal e intransferível, não sendo autorizada a manutenção das senhas em registro virtual, como arquivos Word e Excel;

Para maiores esclarecimentos sobre as medidas aplicadas aos colaboradores da Companhia, verificar a Política de Segurança de Informação e o Código de Ética e Conduta da Companhia.

4.4 – Relatório de impacto à proteção de dados pessoais

A Companhia elaborará, quando aplicável, relatório de impacto à proteção de Dados Pessoais, que será apresentado sempre que solicitado pela Autoridade Nacional de Proteção de Dados ou mediante obrigatoriedade prevista em legislação específica.

No relatório serão descritos detalhadamente os processos de Tratamento de Dados Pessoais que podem gerar riscos às liberdades e aos direitos dos Titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco adotados pela Companhia.

4.5 – Plano de contingência:

A Companhia estabelece uma série de procedimentos para comunicação de incidentes sobre segurança da informação e vazamento dos Dados armazenados em prazo razoável, bem como para imediata contenção dos possíveis danos que um vazamento pode representar para os Titulares.

Na eventualidade de ocorrência de qualquer evento de vazamento de informação de Dados e/ou uso fora da finalidade para o qual foi contratada, a Companhia se compromete a adotar as seguintes medidas:

i. Coletar evidências do ocorrido, de acordo com os requisitos normativos e regulamentares.

ii. Notificar imediatamente o Titular e qualquer outra parte interessada em caso de real ou suspeita de quebra de segurança, acesso não autorizado, perda, dano ou outro tipo de corrupção de segurança, confidencialidade ou integridade dos Dados Pessoais processados pela Companhia.

iii. Realizar avaliação formal da segurança da informação ou incidente de proteção de Dados para que os procedimentos e medidas de controle possam ser aprimorados, com base nas lições aprendidas

com o incidente, gerando comunicação à gerência e especialistas externos, quando necessário, para validação e aprovação de novas ações e procedimentos.

iv. Atuar com todos os esforços e no menor tempo possível para prevenir qualquer futura quebra de segurança da Companhia.

A Companhia disponibilizará ainda o modelo de formulário para relatório de vazamentos de Dados que deverá ser preenchido com as informações pormenorizadas em relação a quebra de segurança da Companhia e encaminhado a qualquer interessado.

4.6 – Encarregado de proteção de dados:

Tendo em vista a importância da proteção dos Dados Pessoais, a Companhia nomeou o Sr. Wladimir Gomes como DPO (*Data Protection Officer*), que é responsável e Encarregado pela implementação e monitoramento desta Política, bem como aos demais dispositivos relacionados à Lei Geral de Proteção de Dados.

Para garantir o cumprimento dessa Política e da LGPD, o Encarregado implementará as seguintes medidas:

i. Realizará, anualmente, treinamento para todos os Colaboradores da Priner em todas as unidades de negócio da Companhia, sobre essa Política e a LGPD, que poderá ser presencial, por videoconferência ou outro meio não presencial, como por exemplo, via web.

ii. Poderá aplicar questionário anual sobre Política e a LGPD a ser respondido por todos os seus colaboradores e administradores.

iii. Realizará auditoria externa anual para avaliar os riscos expostos e as medidas que podem ser tomadas para mitigar os riscos ou solucioná-los. Esta auditoria será realizada em todo sistema da Companhia - na documentação, *hosting,* políticas de segurança, acesso interno e servidores.

iv. Coordenará a atualização dessa Política.

4.7 – Contato:

Para reportar assuntos que considere convenientes no âmbito desta Política, os Titulares podem remeter qualquer pedido relativamente aos mesmos, por escrito, no seguinte endereço de e-mail: lgpd@priner.com.br**.**

4.8 – Alterações à Política de Privacidade e Proteção de Dados Pessoais:

Esta Política está sujeita a alterações para melhor adequação à Lei Geral de Proteção de Dados e às normativas da Agência Nacional de Proteção de Dados.

A Companhia pode alterar a presente Política a qualquer momento, quando considerado necessário.

5.0 – REFERÊNCIAS:

- Código de Ética e Conduta da Priner
- Política de Segurança da Informação
- Política de Segurança do Site
- Lei n° 13.709/2018 – Lei Geral de Proteção de Dados

6.0 – PAPÉIS E RESPONSABILIDADES:

6.1 – DEPARTAMENTO DE TI:

a) Salvaguardar as informações.

b) Garantir o acesso apenas de pessoas autorizadas.

c) Realizar backup de informações.

6.2 – DPO (*DATA PROTECTION OFFICER*):

a) Responsável pelo contato com o órgão regulador de processamento de dados.

6.3 – GENTE E GESTÃO:

a) Manter as informações dos colaboradores seguras e atualizadas.

b) Realizar exclusão das informações de colaboradores e candidatos de processos seletivos quando solicitado.

6.4 – USUÁRIOS:

a) Seguir as diretrizes da presente política.

b) Garantir a confidencialidade das informações a que ele tem acesso.

c) Garantir a veracidade das informações fornecidas para a Companhia.

6.5 – CONTROLES INTERNOS:

a) Realizar a avaliação crítica da política quanto as regras internas e externas.

b) Acompanhar e/ou realizar auditorias internas.

c) Revisar a política em conjunto com a área responsável, quando tiver alteração nos processos e/ou no final do prazo de vigência do documento.

6.6 – CONSELHO DE ADMINISTRAÇÃO:

a) Aprovar as alterações na presente política.

7.0 – ANEXOS:

Não aplicável.

8.0 – APROVAÇÃO E VIGÊNCIA:

Compete exclusivamente ao Conselho de Administração da Priner Serviços Industriais S.A. aprovar quaisquer alterações à presente política.

Esta política entrará em vigor a partir da data de sua aprovação pelo Conselho de Administração e permanecerá em vigor por prazo indeterminado.

9.0 – CONTROLE DE REVISÕES:

REVISÃO	DATA	DESCRIÇÃO DA ALTERAÇÃO
0	27/01/2021	1. Versão Inicial – Elaboração da política
1	03/11/2022	1. Alteração para o novo modelo da política. 2. Inclusão da definição de DPO. 3. Inclusão da classificação do documento. 4. Inclusão dos documentos de referência.
2	07/12/2023	1. Inclusão dos papéis e responsabilidades de Controles Internos e do Conselho de Administração. 2. Inclusão da vigência da política.