

Política de Privacidade e Proteção de Dados Pessoais

Legend

,

Abril de 2024

Versão: 2.0

Elaboração: Departamento Jurídico

Aprovação: Alta Direção

Classificação do Documento: Público

Índice

1. Termos e Definições	4
2. Objetivo	5
3. Escopo de Aplicação.....	5
4. Responsáveis pela Política	5
4.1. Comitê de Privacidade	5
4.2. DPO	6
4.3. Colaboradores	7
4.4. Gestores	7
4.5. Alta Administração.....	7
5. Descrição da Política	8
5.1. Princípios da Proteção de Dados Pessoais	8
5.2. Classificação como Agente de Tratamento.....	9
5.3. Direitos dos Titulares dos Dados Pessoais.....	10
5.4. Atendimento aos Direitos dos Titulares dos Dados	11
5.5. Tipos de Dados Pessoais	11
5.6. Tratamento dos Dados Pessoais	12
5.7. Mapeamento de Dados Pessoais.....	12
5.8. Treinamentos	134
5.9. <i>Privacy by Design</i> e <i>Privacy by Default</i>	14
5.10 Retenção e Descarte	15
5.11 Incidentes de Privacidade.....	15
5.12 Fornecedores.....	15
5.13 Cooperação com Autoridades	16
6. Desvio à Política	16
7. Gestão da Política.....	16
8. Privacidade	16
8.1. Diretriz de Utilização de <i>E-mail</i>	16
8.2. Diretriz de Utilização de Telefone.....	17
8.3. Diretriz de Utilização de Internet	17

8.4. Diretriz de Utilização da Rede Interna	17
8.5. Outras Diretrizes	18
8.6. Exceções Pontuais	18
9. Considerações Finais.....	18

1. Termos e Definições

Esse item esclarece a terminologia utilizada dentro desta Política (em letras maiúsculas ou minúsculas), para facilitar seu entendimento e aplicação.

Termo	Descrição
LGPD	Lei Geral de Proteção de Dados Pessoais, nº 13.709, de 14 de agosto de 2018, que vigora desde 18/09/2020. Dispõe sobre o tratamento de dados pessoais com a finalidade de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
ANPD	Autoridade Nacional de Proteção de Dados, órgão da administração pública federal, responsável por fiscalizar o cumprimento da LGPD.
Dado Pessoal	Informação relacionada a pessoa natural identificada ou identificável.
Dado Pessoal Sensível	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.
Tratamento	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.
Titular dos Dados	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
Legend	Legend
DPO	Encarregado de Dados Pessoais – Pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, o Titular dos Dados e a ANPD, responsável por orientar o Colaboradores, Fornecedor e Operador sobre as práticas a serem tomadas em relação à proteção de dados pessoais.
Fornecedor	Pessoa ou empresa terceira contratada para exercer atividades para a Legend.
Operador	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.
Terceiros	Pessoa externa à Legend que interage com dados pessoais (Ex. Auditoria Independente).
Colaborador	Funcionário, contratado, terceirizado, trabalhador temporário, e aqueles contratados por outros para executar trabalhos nas instalações da Legend
Gestor	Responsável pelas áreas internas da Legend.
Alta Administração	Compostos por membros da administração da Legend, eleitos por meios de seus atos societários.
Informação	É todo e qualquer conteúdo ou dados que tenha valor para a Legend ou seus clientes. Ela pode ser de uso restrito ou exposta de forma pública para consultas ou manuseio.
Privacidade	É o direito à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.
Risco	Qualquer evento que possa causar danos a um processo ou tratamento, onde a probabilidade de uma ameaça seja explorada por uma vulnerabilidade, resultando impacto para operações da Legend.
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 pessoa natural.

2. Objetivo

O objetivo desta Política é dar visibilidade sobre as diretrizes aplicáveis à privacidade e proteção das informações das pessoas naturais com os quais a Legend lidará no exercício de suas atividades, bem como seus administradores, funcionários, prepostos, prestadores de serviços, enfim, terceiros em geral.

Ao longo desta leitura, em especial com as disposições trazidas pela LGPD, o que se pretende é auxiliar na forma correta de coletar, registrar, armazenar, utilizar e compartilhar os dados pessoais a que todos os envolvidos na atividade da Legend tiverem acesso.

As orientações a seguir expostas devem ser observadas pela Legend, considerando as necessidades específicas e os aspectos legais e regulamentares de cada um dos seus ramos de atuação.

Com a esta Política, a Legend pretende assegurar que está comprometida em respeitar os dados pessoais a que tiver conhecimento no exercício de suas atividades, adotando medidas eficientes de segurança e de proteção a riscos, enfim, dar visibilidade ao tratamento.

3. Escopo de Aplicação

Essa política aplica-se a todos Colaboradores, estendem-se a todos os grupos e empresas que se relacionem, em algum momento, com a Legend, e têm acesso a qualquer informação, sistema, computador, rede de computadores, telecomunicação, mensagem ou serviço de informações pertencentes à Legend, em todas as divisões, subsidiárias, filiais e parcerias onde as leis locais, estatutos e regulamentações do governo não se sobreponham a essas políticas e procedimentos.

4. Responsáveis pela Política

Cada Colaborador na Legend tem seu papel fundamental para a condução esta Política. Dessa forma, descrevemos abaixo mais detalhes para cada papel-chave na estrutura da organização.

4.1. Comitê de Privacidade

Grupo formado por integrantes de áreas estratégicas da Legend, com objetivo de deliberar e definir assuntos relacionados à privacidade e proteção de dados pessoais, tendo como principais responsabilidades:

- Apoiar o DPO na gestão desta Política, que ele esteja alinhado as regulamentações legais e estratégia da Legend;
- Garantir a comunicação adequada desta Política a todos envolvidos;
- Avaliar e aprovar as diretivas locais de proteção de dados e privacidade, regras e padrões a serem usados pelos Colaboradores;
- Sugerir e acompanhar a implantação de políticas, inclusive de boas práticas e de governança;
- Avaliar e definir todas as ações relacionados a riscos existentes nos processos de tratamento de dados pessoais e exigir a elaboração de relatórios de impacto à proteção de dados pessoais, se necessário;
- Fiscalizar e tomar decisões relacionadas às atividades de tratamentos que possam envolver risco ou dano ao titular de dados ou a Legend;
- Deliberar sobre medidas disciplinares, sanções e penalidades, quando aplicável;

- Auxiliar no processo de gestão de incidente da Legend no que tange à tomada de decisões, à avaliação de impacto e às lições aprendidas;
- Propor ações voltadas ao aperfeiçoamento contínuo desta Política, das salvaguardas e medidas de prevenção de riscos.

4.2. DPO

O encarregado dos dados pessoais indicados pela Legend tem como principais atribuições:

- Gerenciar esta Política, conforme entendimento prévio com o Comitê de Privacidade e a Alta Administração;
- Ser o ponto focal de contato com a ANPD, Operadores e os Titulares de Dado Pessoal;
- Produzir diretivas locais de proteção de dados e privacidade, regras e padrões a serem usados pelos Colaboradores. Estes padrões de proteção de dados e privacidade devem levar em conta aspectos como, necessidades dos negócios da Legend, regulamentações e leis locais etc.;
- Desenvolver e promover programas de conscientização de proteção de dados e privacidade;
- Garantir que todos os gestores estejam completamente cientes de suas próprias responsabilidades relacionadas à proteção de dados e privacidade;
- Certificar-se que o processo de gestão de pessoas leva em conta todos os aspectos de proteção de dados e privacidade, desde a contratação de novos empregados até a rescisão de contratos de trabalho;
- Monitorar periodicamente o nível de maturidade e conformidade das ações de proteção de dados e privacidade de sistemas e processos internos, emitindo avisos após estas revisões. Analisar criticamente, em intervalos periódicos, o progresso dos planos de melhoria resultantes em conjunto com os gestores envolvidos;
- Manter-se atualizado com relação à tecnologia, legislação e novas ameaças;
- Garantir a atualização do mapa de dados pessoais, sempre que houver alteração em algum processo de tratamento;
- Analisar criticamente os incidentes de segurança e privacidade mais significativos e gerenciar e/ou acompanhar as ações relacionadas à solução deles. Qualquer incidente de segurança e privacidade deve resultar em uma análise realizada sob a autoridade do DPO;
- Acompanhar o sistema de ações corretivas e preventivas desta Política;
- Elaborar sempre que necessário relatório de impacto à proteção de dados pessoais com a devida apuração dos riscos envolvidos aos tratamentos.

4.3. Colaboradores

As principais responsabilidades dos Colaboradores são:

- Conhecer, seguir todas as políticas e procedimentos pertencentes a esta Política;
- Estar cientes dos métodos, processos e parâmetros aplicados na Legend para proteção de dados e privacidade;
- Conhecer e aplicar a LGPD;

- Cuidar pela privacidade e proteção dos ativos e dados pessoais a que tiverem acesso;
- Fiscalizar o cumprimento da presente Política por parte de Terceiros que tenham acesso aos dados pessoais tratados pela Legend;
- Recomendar melhorias nesta Política;
- Identificar qualquer incidente de segurança e reportá-lo ao seu Gestor ou a área de TI da Legend.

4.4. Gestores

Cabe aos Gestores:

- Garantir a disseminação do conhecimento sobre proteção de dados e privacidade sob sua responsabilidade, para seus comandados e para a Legend, incentivando a participação em treinamentos internos ou externos;
- Comunicar ao DPO sempre que houver alguma alteração nos processos de sua responsabilidade, para manter atualizado o Mapeamento de Dados Pessoais;
- Implantar e monitorar a eficácia de procedimentos, instruções de trabalho e documentos quanto a proteção de dados pessoais e privacidade;
- Planejar a adoção de procedimentos desta Política e monitorar sua eficácia;
- Garantir a contínua eficácia dos controles implantados de proteção de dados e privacidade, para satisfazer os requisitos desta Política.

4.5. Alta Administração

A Alta Administração é responsável por:

- Garantir o atendimento dos requisitos das políticas e dos objetivos desta Política;
- Designar o DPO;
- Aprovar as iniciativas para a melhoria contínua do sistema;
- Prover recursos para a gestão, operação e monitoramento adequado das atividades desta Política;
- Suportar perante toda a organização as iniciativas das áreas críticas envolvidas no tratamento de dados pessoais;
- Garantir a contínua manutenção desta Política e desdobramento dos respectivos objetivos;
- Garantir a contínua análise e realimentação dos resultados de gestão de riscos a esta Política;
- Faz parte do comprometimento da Alta Administração com relação a esta Política, a destinação de orçamento para a aquisição de recursos para a melhoria do sistema de Governança de Dados Pessoais e para o alcance dos objetivos desta Política.

5. Descrição da Política

Com essa política, A Legend busca orientar seus Colaboradores sobre o correto tratamento de dados pessoais focando na proteção dessas informações e na privacidade de seus titulares. O Titular do Dado é o ponto focal dessas orientações, sempre respeitando seus direitos baseados nas regulamentações vigentes e aplicáveis.

Esta Política orienta a todos sobre o correto comportamento voltado para os requisitos legais apresentados na LGPD, bem como as melhores práticas nacionais e internacionais, sempre considerando as limitações legais e as estratégias de negócios da Legend.

Para o cumprimento dos objetivos desta Política, das estratégias e dos tempos acordados, seguem abaixo premissas a serem consideradas nas operações de tratamento de dados pessoais:

5.1. Princípios da Proteção de Dados Pessoais

As atividades de tratamento de dados pessoais deverão se basear na boa-fé e, também, nos princípios dispostos na LGPD. Portanto, as atividades de tratamento de dados pessoais realizadas pela Legend se orientarão pelos princípios na tabela abaixo, a fim de demonstrar, de forma clara e transparente, a adoção de medidas eficazes e capazes de comprovar o cumprimento das normas de privacidade e proteção de dados pessoais.

Princípio	Detalhes
Finalidade	O princípio da finalidade é uma garantia para os titulares de dados pessoais de que as informações tratadas, seguem aos propósitos legítimos, específicos, explícitos e informados ao titular da informação. A Legend deve sempre tratar as informações com o propósito definido antes da coleta da informação. Tratamentos secundários relacionados aos dados pessoais coletados para um propósito específico poderão ocorrer sempre que existir uma base legal que comprove e registre a legalidade do tratamento da informação pessoal.
Adequação	O princípio da adequação assegura ao titular da informação pessoal tratada pela Legend que os dados coletados e tratados têm compatibilidade com o contexto das atividades desenvolvidas pela empresa e informadas ao titular. Portanto, a Legend assegura que os dados pessoais tratados no contexto das suas atividades estarão relacionados com os propósitos específicos informados ao titular da informação.
Necessidade	O princípio da necessidade é complementar aos princípios da finalidade e da adequação e, portanto, a Legend também garante ao titular que os dados pessoais coletados e tratados pela empresa, além de ter um propósito específico e compatível com as finalidades do tratamento, serão sempre limitados ao mínimo necessário para o desenvolvimento das atividades. Logo, os dados coletados pela Legend não serão excessivos, mas sim proporcionais às finalidades e compatíveis com o desenvolvimento das atividades de tratamento de dados pessoais. Dados pessoais que não são mais necessários, após a expiração de períodos legais ou de processos de negócio, deverão ser excluídos. A Legend, entretanto, poderá manter os dados pessoais tratados – ainda que não mais necessários para as atividades desenvolvidas pela empresa, caso os dados sejam anonimizados.
Livre Acesso	É assegurado ao titular dos dados pessoais um procedimento gratuito e fácil sobre as informações dos tratamentos de dados pessoais realizados pela Legend acerca de seus dados pessoais. As informações sobre o tratamento, disponibilizadas pela Legend, deverão dispor sobre: <ul style="list-style-type: none"> • A finalidade específica; • A forma e duração; • A identificação do controlador; • O contato do controlador; • O uso compartilhado de informações e a respectiva finalidade; • As responsabilidades de cada parte que realiza o tratamento de dados pessoais; • Os direitos do titular.
Qualidade dos Dados	As atividades de tratamento devem se estruturar para que as informações que compõem os dados pessoais sejam exatas e claras. Portanto, a atualização de dados é fundamental para que a finalidade do tratamento se cumpra. É garantido ao Titular dos Dados os meios adequados para corrigir e atualizar suas informações pessoais, assegurando que os dados pessoais tratados sejam relevantes e necessários à persecução das atividades da organização e da finalidade previamente acordada.

Transparência	A Legend garante ao Titular dos Dados informações claras e precisas sobre os tratamentos de dados pessoais realizados e, além disso, confere a observância dos respectivos aos agentes de tratamento com os quais se relaciona.
Segurança	Os dados pessoais tratados pela Legend estão estruturados por meio de um Sistema de Gerenciamento de Segurança da Informação e Privacidade. A Legend entende que as boas práticas de segurança da informação e privacidade devem estar sempre alinhadas às boas práticas de mercado; por isso, a Legend aplica políticas e procedimentos que buscam minimizar ou eliminar risco ou vulnerabilidade que possa, de alguma forma, comprometer a confidencialidade, integridade e disponibilidade dos dados pessoais.
Prevenção	As práticas operacionais da Legend garantem a adoção de medidas que visam prevenir e proteger as informações pessoais de eventuais danos que possam vir a ocorrer, em virtude do tratamento a eles conferido. Portanto, o Sistema de Gestão de Segurança da Informação e Privacidade da Legend, voltado para minimizar os riscos dos ativos de informação, tem por outro objetivo também a prevenção. A gestão dos riscos está em constante evolução, sendo um processo cíclico e dinâmico que requer participação de todos, inclusive daqueles que tratam dados pessoais.
Não Discriminação	A Legend entende que é fundamental para as suas atividades o tratamento de informações pessoais, sejam elas de seus Colaboradores, clientes ou parceiros. Nesse sentido, a Legend realizar o tratamento de dados pessoais com respeito à dignidade da pessoa humana, desprovido de cunho discriminatório ou ilícito. Dessa forma, a Legend entende a importância de respeitar os direitos humanos, a dignidade e o exercício da cidadania de todas as pessoas naturais.
Responsabilidade e Prestação de Contas (<i>accountability</i>)	A Legend tem como compromisso o desenvolvimento e a criação de evidências documentais e organizacionais para que se comprove a adoção de medidas eficazes e capazes de demonstrar a observância e o cumprimento das normas de proteção de dados pessoais. O processo de prestação de contas é contínuo e a Legend sempre buscará evidenciar a legalidade da atividade que se relaciona com o tratamento de dados pessoais, mitigando riscos e adotando medidas eficazes e capazes de cumprir com a norma de proteção de dados pessoais.

5.2. Classificação como Agente de Tratamento

A Legend, no âmbito dos tratamentos de dados pessoais que realiza, a depender da situação, poderá ser considerada como **Controladora** ou **Operadora** de informações pessoais. Portanto, somente será considerada como **Controladora** de dados pessoais quando tomar decisões referentes às atividades de tratamento. Em outras palavras, quando a Legend coletar dados pessoais dos titulares e identificar as finalidades, os propósitos e os meios para o tratamento deles será considerada **Controladora**.

Por outro lado, a Legend poderá ser considerada como **Operadora** de dados pessoais quando seguir instruções de uma outra parte sobre as atividades de tratamento de dados pessoais ou quando receber dados pessoais de um terceiro que a coletou e determinou as finalidades do tratamento.

ATIVIDADES DO CONTROLADOR	ATIVIDADES DO OPERADOR
Determinar as finalidades e as decisões referentes ao tratamento de dados pessoais.	Realizar o tratamento segundo instruções do Controlador.
Indicar DPO.	
Obter o consentimento válido, quando este for a base legal para o tratamento de dados pessoais.	
Informar ao Titular dos Dados alteração em relação à mudança da finalidade, forma e duração do tratamento,	

identificação do Controlador ou sobre o uso compartilhado dos dados pessoais.	
Realizar o <i>Legitimate Interest Assessment</i> para garantir, de forma transparente, que o tratamento de dados pessoais é realizado com base nas disposições legais	
Garantir o direito dos Titulares dos Dados.	
Comprovar perante o Titular dos Dados o cumprimento das normas legais pertinentes à proteção de dados quando estes forem transferidos para terceiros.	
Manter registro das operações e atividades que envolvem dados pessoais.	
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	
Comunicar, em prazo razoável, à Autoridade Nacional e ao Titular dos Dados a ocorrência de incidente de segurança que possa lhe acarretar risco ou dano relevante.	Comunicar o Controlador, em prazo razoável, sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos Titulares dos Dados

5.3. Direitos dos Titulares dos Dados Pessoais

A Legend, tem como valor garantir ao Titular de Dados pessoais a preservação dos seus direitos, elencados na GPD.

O Titular de Dados pessoais poderá requerer, expressamente e sem custo, os seguintes direitos:

- **Confirmação da existência do tratamento** - Confirmar se a Legend trata ou não os dados pessoais;
- **Acesso aos dados** - Se confirmado o tratamento, ele pode solicitar acesso aos dados pessoais;
- **Correção dos dados incompletos, inexatos ou desatualizados** - Respeitando as limitações por exigência legal, os dados poderão ser corrigidos;
- **Anonimização, bloqueio ou eliminação dos dados desnecessários, excessivos ou tratados ilicitamente:**
 - **Anonimização** – Descaracterização da informação de forma que garanta a não identificação do titular;
 - **Bloqueio** – Solicitar o bloqueio da empresa aos dados tratados desde que não haja limitação legal;
 - **Eliminação dos dados desnecessários ou tratados ilicitamente** - Quando existirem dados desnecessários à finalidade original do tratamento ou tratados de forma ilícita (obtidos sem a autorização ou conhecimento do respectivo titular), o Titular dos Dados mesmo pode solicitar sua eliminação desde que não haja limitação legal.
- **Portabilidade dos dados a outro fornecedor de serviço ou produto** – Ainda depende de regulamentação da ANPD acerca de como executar a portabilidade;
- **Eliminação dos dados pessoais tratados com o consentimento do Titular dos Dados** – desde que não haja limitação legal;

- **Informação das entidades com as quais o Controlador compartilhou seus dados pessoais** – Ser informado quando existir o compartilhamento dos dados pessoais com terceiros;
- **Não Consentimento** – Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- **Revogação do consentimento** – O Titular dos Dados pode informar a qualquer momento o não consentimento anteriormente dado ao tratamento.

5.4. Atendimento aos Direitos dos Titulares dos Dados

O DPO será responsável pelo atendimento que se referem aos direitos assegurados na lei e nesta Política. Sendo assim, os Titulares dos Dados devem comunicar ao DPO por escrito, as dúvidas ou solicitações.

Essa comunicação pode ser feita ao e-mail dpo@legendcapital.com.br ou, por correio, ao endereço:

À Legend

A/C: DPO

Av. Brig. Faria Lima, 3900 - 6º Andar – Cj. 602

Itaim Bibi - São Paulo - SP

CEP 04538-132

5.5. Tipos de Dados Pessoais

De acordo com os requisitos da LGPD, todo dado pessoal deve ser tratado de forma adequada à finalidade para o qual foi coletado, dessa forma, se faz, necessário que todos os Colaboradores saibam identificar os dados pessoais e determinar sua classificação e importância para os negócios da empresa. Segue abaixo uma explicação sobre os tipos de dados relacionados na LGPD:

TIPO DE DADOS	DEFINIÇÃO
Pessoal	Informação relacionada a pessoa natural identificada ou identificável
Pessoal Sensível	Informação 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
Criança e Adolescente	Dado pessoal ou pessoal sensível relacionados a criança de até doze anos de idade incompletos, e adolescente entre doze e dezoito anos de idade, conforme lei nº 8069, de 13 de Julho de 1990, Art. 2º.

De uma maneira geral, a Legend não realiza tratamento de dados sensíveis, exceto para fins de gestão dos sistemas de acesso físico que se baseia no tratamento das digitais das pessoas cujo acesso às dependências da Legend é autorizado.

Em nossos processos de departamento pessoal, eventualmente tratamos informações de crianças e adolescentes. Os dados coletados devem se limitar tão somente àqueles necessários para a finalidade de fornecer aos filhos de colaboradores benefícios de seguro saúde.

Para efetuar a coleta de informações relacionadas à criança e adolescente, sempre devemos obter a autorização formal de pelo menos um dos pais ou responsável legal através do consentimento informado e documentado.

No âmbito da Legend, dados de crianças e adolescentes também podem ser tratados para fins de assessoria a nossos clientes e, da mesma forma, este tratamento de dados pessoais deverá observar o princípio da minimização através do qual os dados coletados devem se restringir ao mínimo necessário para a finalidade específica para o qual foi coletado.

Fora dessas finalidades estes dados pessoais não devem ser tratados em nossa empresa.

Caso exista a necessidade de tratamento desses dados pessoais para uma nova finalidade a mesma deve ser consultada e aprovada pelo DPO, que providenciará sua descrição nessa política.

5.6. Tratamento dos Dados Pessoais

A Legend tem o compromisso de coletar os Dados Pessoais por meios éticos e legais e armazená-los em ambiente seguro e controlado, pelo prazo exigido pela LGPD. Para tanto, serão tomadas todas as medidas cabíveis para manter o absoluto sigilo e a estrita confidencialidade de todos os Dados Pessoais aos quais a Legend e todos os envolvidos na prestação de serviços da Legend venham a conhecer.

Especialmente no que tange à segurança, a Legend informa que tem à sua disposição processos de segurança técnicas e administrativas que permitem tratar os Dados Pessoais com a sensibilidade que lhes é pertinente. A eficiência desses processos será periodicamente avaliada e a Legend se compromete a promover sempre melhorias tecnológicas para assegurar o bom tratamento dos Dados Pessoais.

Todas as tecnologias utilizadas atenderão aos requisitos de segurança e de transparência estabelecidos pelos padrões de boas práticas e governança, respeitando sempre a legislação vigente.

5.7. Mapeamento de Dados Pessoais

A Legend, mantém uma lista de registro sobre todos os tipos de dados pessoais tratados pela empresa, contendo as seguintes informações:

- **Área de Empresa** – Área onde é executado o tratamento;
- **Processo** – Nome do processo da área;
- **Subprocesso** – Processo secundário ao Processo;
- **Descrição do Processo** – Descrever com detalhes o processo e subprocesso;
- **Tipo de Dado** – Identificar se é Dado Pessoal ou Sensível, e, ainda, se é pertinente à criança ou adolescente;
- **Categoria de Dados Pessoais** – Descrição dos tipos de dados, p. ex.: nome, CPF, endereço;
- **Finalidade do Tratamento** – Por qual motivo é feito o tratamento;
- **Ações de Tratamento** – Descrever a ação praticada, p. ex.: coleta, armazenamento etc.;
- **Meio** – Identificar se o dado é digital, físico ou híbrido;
- **Estado do Dado** – Descrever o estado do dado, p. ex. Anonimizado, Criptografado, Arquivo em texto claro, Sem Criptografia, indefinido ou não aplicável.
- **Sistemas envolvidos** – Descrever os sistemas são utilizados no tratamento;

- **Infraestrutura**– Identificar o local de armazenamento físico e digital dos dados;
- **Pessoa responsável pelo processo** – Identificação do responsável pelo processo;
- **Compartilhamento com áreas ou pessoas internas** – Identificação das pessoas ou área com as quais os dados são compartilhados;
- **Compartilhamento externo (outro controlador)** – Identificar a entidade externa com a qual é compartilhado os dados pessoais;
- **Agente de tratamento** – Identificar se o tratamento é realizado pelo Controlador ou Operador;
- **Base Legal** – Informar a base legal usada para o tratamento;
- **Detalhe da Base Legal** – Motivar a escolha da base legal;
- **Categoria do Titular** – Qual tipo de titular no processo, p. ex. Colaborador, cliente etc.;
- **Período de Retenção** – Informar o período recomendado para a retenção dos dados pessoais;
- **Justificativa da Retenção** – O porquê do período de retenção;
- **Recomendações** – Qualquer recomendação focando a melhoria ou eliminação de qualquer risco identificado sobre o tratamento.

Esse documento deverá ser mantido atualizado, com todos os tratamentos de dados pessoais, bem como, deve refletir qualquer alteração nos processos internos que tratam dados pessoais da empresa, na busca de garantir o atendimento aos requisitos legais da LGPD.

É responsabilidade de todos na empresa adequar esse mapa aos processos atualizados sobre cada tratamento executado, visando ao fornecimento de uma gestão completa de todos os riscos atribuídos a esses tratamentos.

5.8. Treinamentos

A Legend determina que todos os Colaboradores sejam periodicamente treinados e capacitados para conhecer o Programa de Privacidade e Proteção de Dados Pessoais, alinhados as boas práticas de segurança da informação e privacidade.

Faz-se necessário que todos tenham conhecimento sobre as regras e controles definidos e aplicados para garantir a privacidade e proteção de dados pessoais, mas especificamente, e no mínimo, sobre:

- Conceitos gerais de Privacidade e Proteção de Dados
- A apresentação desta política e de materiais de estudo prático sobre os princípios da LGPD;
- Conceitos específicos de Privacidade e Proteção de Dados, aplicados às atividades de cada área.

O Processo de integração de novos Colaboradores deve garantir que eles recebam o treinamento necessário sobre os itens acima descritos para exercer suas funções na empresa.

5.9. Privacy by Design e Privacy by Default

Todos os sistemas da Legend devem ter como premissa a privacidade como requisito obrigatório; dessa forma, todo o processo de aquisição dos sistemas e produtos deve determinar e adotar controles e medidas para prevenir a ocorrência de danos aos Titulares dos Dados e deve estar focado na proteção dos dados pessoais e nos seus tratamentos que lhe são conferidos.

É mandatório que todos os projetos de novos sistemas e produtos na sua concepção até o momento da entrega deles, têm que considerar e assegurar a privacidade e proteção dos dados pessoais. A seguir, a Legend informa os princípios relacionados a *Privacy by Design* que deverão ser considerados:

- **Proativo, e não reativo e não corretivo** – Deve antecipar e prevenir situações que comprometam a privacidade antes que ela aconteça e nunca depois do ocorrido;
- **Privacidade como padrão** – Todas as iniciativas devem utilizar o nível mais alto de proteção à privacidade como princípio padrão;
- **Privacidade incorporada ao design** – Deve ser incorporado na arquitetura de sistemas de TI, práticas de negócio e produtos e serviços, fazendo parte dos projetos como disciplina a ser avaliada e aprovados por todos;
- **Funcionalidade total** – Garantia da privacidade dos dados pessoais, sem comprometer as funcionalidades ou objetivos do produto ou serviço;
- **Segurança de ponta a ponta** – Proteção durante todo o ciclo de vida dos dados pessoais;
- **Visibilidade e transparência** – Garantia de transparência nos tratamentos de dados pessoais, com geração de avisos adequados à finalidade dos tratamentos;
- **Respeito pela privacidade do usuário** – Foco nos interesses dos Titulares dos Dados, visando a garantia da privacidade dos dados pessoais.

Estas práticas envolvem, mas não se limitam, as seguintes medidas:

- Realizar a uma Análise de Impacto de Privacidade;
- Assegurar as práticas de Segurança da Informação, em especial em escopos que incluam dados pessoais;
- Empreender os melhores esforços para adequar seus processos para proteção de dados pessoais;
- Alertar sobre situações de riscos em produtos e serviços que possam propiciar incidentes de violação de dados;
- Considerar adoção de indicadores, métricas e demais recursos para monitoramento;
- Implementar registros de processamento de dados pessoais, como trilhas de auditoria, em especial para os casos de: inclusão, alteração e exclusão destes dados, para fins de fiscalização ou apuração de responsabilidades em investigações sobre violação de dados pessoais;
- Adotar práticas de desenvolvimento seguro e análises de vulnerabilidades, quando se tratar de sistemas e demais soluções tecnológicas.

5.10. Retenção e Descarte

Todos os responsáveis pelos processos que envolvam tratamentos de dados pessoais devem mantê-los armazenados pelo menor período possível necessário, isto é, a guarda deve acontecer somente pelo período necessário ao tratamento de acordo com suas finalidades estipuladas.

A Legend por meio do mapa de dados - item **5.7. Mapeamento de Dados Pessoais** desse documento, apresenta para cada processo e subprocesso as recomendações acerca do período legal, conforme descrito no campo “**Período de retenção**”.

Quando do vencimento do período de retenção, a recomendação da empresa é efetuar o descarte no período definido, sendo certo que haverá situações de exceção, por exemplo, devido a legislações específicas a serem validadas no decorrer do processo.

5.11. Incidentes de Privacidade

Todo ou qualquer evento que possa estar em desacordo com os pontos apresentados nesta política pode ser considerado incidente de privacidade. Esses incidentes podem causar danos aos Titulares dos Dados ou violação da privacidade.

Todas as ações necessárias para a condução do tratamento desses incidentes estão descritas no documento “Plano de Resposta e Tratamento de Incidentes” de forma organizada, com indicações das ações necessárias para minimizar os impactos e danos desses incidentes.

De qualquer forma, qualquer falha identificada por nossos Colaboradores, devem ser imediatamente comunicadas ao DPO por meio do e-mail dpo@legendcapital.com.br, relatando a ocorrência com o máximo possível de informações, permitindo que o plano seja ativado e os responsáveis pelo tratamento do incidente sejam acionados imediatamente e ações de comunicação sejam feitas de acordo com as definições do plano.

5.12. Fornecedores

Para garantir boas práticas na gestão da privacidade e proteção de dados, os Fornecedores também necessitam executar todos os requisitos apresentados nesta política.

Nenhum serviço oferecido à Legend pode ser iniciado sem que os contratos sejam assinados, devendo estes conterem as cláusulas de proteção de dados e privacidade.

No processo de avaliação dos fornecedores é recomendado que sejam apresentadas evidências sobre quais ações foram tomadas pelos Fornecedores para se adequarem aos requisitos exigidos pela LGPD.

Deve existir um processo de validação contínua dos Fornecedores que irão operar dados pessoais em nome da Legend, para garantir que todos os requisitos de proteção de dados e privacidade descritos nesta política estejam adequados aos serviços ou produtos contratados.

A Legend exige de todos os terceiros com quem se relaciona que mantenham a confidencialidade dos Dados Pessoais com eles compartilhados, ou que tenham acesso em virtude do exercício das suas atividades, sendo expressamente vedada a cessão, bem como a utilização das informações para os fins que não os expressamente permitidos. No entanto, a Legend não se responsabilizará pelo uso indevido de tais informações pelos terceiros, em virtude do descumprimento desta Política e das obrigações contratuais por eles assumidas em instrumentos próprios.

5.13. Cooperação com Autoridades

A Legend declara que, quando a divulgação dos Dados Pessoais se fizer necessária, seja em razão de cumprimento de lei, determinação judicial ou de órgão competente fiscalizador das suas atividades, a respectiva revelação se dará nos estritos termos e nos limites requeridos para a sua divulgação, sendo que os titulares dos Dados Pessoais, se possível, serão notificados sobre tal divulgação, para que tomem as medidas protetivas ou reparadoras apropriadas.

6. Desvio à Política

Os funcionários, prepostos, prestadores de serviços, enfim, terceiros em geral que observarem quaisquer desvios ao disposto nesta Política poderão relatar o fato à Área de Compliance e/ou ao Canal de Denúncia, podendo ou não se identificar.

No âmbito interno da Legend, o descumprimento das orientações desta Política ensejará na aplicação de medidas de responsabilização de quem as descumprirem.

7. Gestão da Política

A Legend, seus administradores, funcionários, prepostos, prestadores de serviços e terceiros em geral que se envolverem em suas atividades deverão observar e zelar pelo cumprimento desta Política e, quando se fizer necessário, acionar a Área de Compliance para consulta sobre situações que envolvam conflito com esta Política.

A Legend se compromete a manter esta Política atualizada, de forma a garantir que serão observadas todas as disposições legais a ela atinentes.

À Área de Compliance caberá aceitar reclamações e comunicações dos titulares dos Dados Pessoais e tomar as providências cabíveis e fazer o relacionamento com a Autoridade Nacional de Proteção de Dados, recebendo as comunicações e adotando eventuais providências.

8. Privacidade

8.1. Diretriz de Utilização de *E-mail*

A Legend possui servidores de *e-mail* configurados com camadas de proteção de segurança para prevenir vírus ou a execução de códigos maliciosos. Os usuários serão frequentemente orientados a utilizar o serviço de *e-mail* de forma segura. Seguem diretrizes para utilização de e-mail na Legend.

- As contas de *e-mail* pessoal serão bloqueadas na rede da Legend.
- O *e-mail* corporativo deverá estar ativo sempre que o usuário estiver trabalhando no computador.
- Não utilizar contas de *e-mail* pessoal para enviar qualquer tipo de informação confidencial ou interna.
- Ao receber *e-mails* com *links*, verificar se este corresponde ao endereço que aparece na tela. Para tanto, posicionar o ponteiro do *mouse* sobre o *link* (não clicar).
- Não abrir, em hipótese alguma, caso não tenha certeza da procedência do envio e da legitimidade do *e-mail*.

8.2. Diretriz de Utilização de Telefone

- Número do telefone do usuário: A Legend disponibilizará telefones para utilização do usuário no desempenho de suas funções profissionais.
- Propriedades do número do telefone: O telefone disponibilizado para o usuário e as conversas associadas a esse número serão de propriedade da Legend e, portanto, poderão ser gravadas. Não deverá ser mantida, portanto, expectativa de privacidade pessoal.
- Responsabilidades e forma de uso: O usuário que utilizar um telefone será responsável por todo conteúdo da conversa e só deverá utilizar o telefone para o seu desempenho profissional na empresa. Será proibido utilizar o telefone para conversas que:
 - Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
 - Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;
 - Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
 - Defendam ou possibilitem a realização de atividades ilegais;
 - Possam prejudicar a imagem da Legend; ou
 - Sejam incoerentes com o Código de Ética da Legend.

8.3. Diretriz de Utilização de Internet

A Área de TI deverá manter os acessos à internet configurados conforme uma política de bloqueios a ser estabelecida pela Área de *Compliance*.

A Área de TI deverá manter bloqueados os *cloud services* (como *Dropbox*, *OneDrive* e *Google Drive*), por não ser permitido o uso desse tipo de serviço pelos Colaboradores. O compartilhamento de documentos por meio de *cloud services*, quando necessário, deverá ser realizado pela Área de TI, com anuência da Área de *Compliance*.

- A instalação de *softwares* será de responsabilidade da Área de TI e bloqueada por senha;
- É proibido fazer *upload* ou *download* de *softwares* ou dados ilegais (pirataria);
- Não será permitido enviar ou fazer *download* de músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais;
- Não será permitido o uso de compartilhadores de informações como redes *Peer-to-Peer*, também conhecidas como redes P2P dentro da Legend, que serão bloqueadas pelos serviços de *firewall*;
- A internet disponibilizada aos visitantes será acessível somente por uma rede de visitantes. Essa rede será totalmente segregada da rede interna da Legend e não terá acesso aos servidores da Empresa;
- No caso de perda ou roubo de dispositivos móveis que contenham acesso ao e-mail corporativo, a Área de TI juntamente com a Área de *Compliance* deverão ser comunicadas imediatamente para fins de bloqueio.

8.4. Diretriz de Utilização da Rede Interna

A Legend possui segregação de pastas na rede interna. Cada área possui um perfil de acesso, e todos os perfis terão dois níveis de segurança - leitura e edição.

É proibido armazenar na rede arquivos de música, vídeos e fotos que não sejam de propriedade da empresa.

Dispositivos externos, como *pendrives* e HD externos não são permitidos devido ao bloqueio das portas USB dos computadores. Em caso de necessidade, a Área de *Compliance* deverá aprovar a exceção mediante solicitação do responsável da área do Colaborador solicitante.

O usuário não deve obter ou tentar obter acesso não autorizado a outros sistemas ou redes de computadores conectados à rede interna.

Computadores particulares, de Colaboradores da Legend ou de visitantes, não podendo ser conectados à rede interna da empresa, salvo em situações com prévia autorização da Área de *Compliance*.

8.5. Outras Diretrizes

Não deixar papéis ou mídias removíveis da empresa contendo informações confidenciais sem o devido armazenamento (política de mesa limpa). Essas informações precisam estar guardadas em armários/gavetas com chave.

Informações confidenciais, quando impressas, devem ser imediatamente retiradas da impressora.

Os Dados Pessoais dos clientes da Legend devem ser tratados com o devido sigilo e cuidado, devendo ser observado o disposto LGPD. Em hipótese alguma esses dados serão fornecidos a terceiros, sem consentimento do cliente ou previsão legal.

8.6. Exceções Pontuais

Em caráter excepcional, e em função de suas atividades, alguns Colaboradores poderão ter acessos especiais concedidos. Nessas hipóteses, o Colaborador deverá fundamentar por *e-mail* as razões pela qual entende ser necessário o referido acesso especial, encaminhar a solicitação para a Área de *Compliance* e para o respectivo responsável pela área do colaborador. Nesses casos, ao assinar esta Política, o Colaborador se comprometerá de antemão a manter todas as informações que tiver acesso sob sigilo e se responsabiliza no caso de eventual vazamento.

A Área de *Compliance*, depois de verificar as informações, e eventualmente consultar o responsável pela área, poderá solicitar o desbloqueio das ferramentas solicitadas junto a Área de TI ou poderá, alternativamente, escalar o assunto para decisão final da Alta Direção.

9. Considerações Finais

O desconhecimento em relação a qualquer uma das obrigações e compromissos decorrentes deste documento não justifica eventuais desvios, portanto, em caso de dúvidas ou necessidade de esclarecimentos adicionais sobre seu conteúdo, favor consultar a Área de Compliance.

O descumprimento dos preceitos deste documento ou de outros relacionados pode acarretar medidas disciplinares, medidas administrativas ou judiciais cabíveis, podendo levar à demissão, exclusão societária, reporte às autoridades competentes ou outras sanções, inclusive decorrentes da legislação, autorregulação ou regulamentação aplicável.

Todos os documentos e informações exigidos serão mantidos pelo prazo previsto na regulamentação vigente ou por prazo superior por determinação expressa dos órgãos reguladores e autorreguladores.

Este documento está disponibilizado ao público em geral na página da Legend na rede mundial de computadores.