MANUAL DE BOAS PRÁTICAS E PRINCIPAIS CONCEITOS SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS.

APRESENTAÇÃO DO GUIA DE BOAS PRÁTICAS DA LGPD

Implementar a Lei Federal n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) no seio corporativo da Intercore Intermediação de Negócios Ltda. é o meio de assegurar a proteção dos dados pessoais de todos os nossos clientes, parceiros, colaboradores e fornecedores de insumos.

O objetivo deste documento, portanto, é promover a tomada de decisão informada nos movimentos atinentes a proteção de dados pessoais de todas as pessoas naturais vinculadas as atividades empresariais da Intercore Intermediação de Negócios Ltda., atuando na forma recomendada para o tratamento de dados e as boas práticas em segurança da informação, mormente o compromisso com a proteção aos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Logo, a governança no compartilhamento de dados na Intercore Intermediação de Negócios Ltda. está compreendida à luz das restrições legais, dos requisitos de segurança da informação e comunicações e do disposto pela Lei Federal n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), servindo este documento para fornecer orientações de boas práticas a empresa nas suas operações de tratamento de dados pessoais, conforme previsto no artigo 50 da LGPD, observando-se a boa-fé e os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Este manual de boas práticas e de principais conceitos sobre a Lei Geral de Proteção de Dados representa um marco na cultura organizacional da Intercore Intermediação de Negócios Ltda., centrada na pessoa física, em minimizar impactos e

aumentar a segurança aplicada ao tratamento dos seus dados pessoais, encontrando-se estruturado em seis capítulos:

O Capítulo 1 contempla os conceitos basilares e as definições impostas na lei.

Já o Capítulo 2 apresenta a aplicação da LGPD para todos os efeitos de tratamentos de dados pessoais.

Na sequência o Capítulo 3 revela os princípios indicados para o tratamento de dados pessoais.

O Capítulo 4 exibe os requisitos para a efetivação do tratamento dos dados pessoais, compreendendo as condições necessárias para o tratamento de dados pessoais e dados pessoais sensíveis.

Em prosseguimento o Capítulo 5 realça a segurança da informação que deve haver em todas as fases do ciclo de vida nas operações de tratamento indicadas na LGPD.

Por fim, o Capítulo 6 estabelecem as regras de boas práticas e de governança de dados observadas pela Intercore Intermediação de Negócios Ltda.

CAPÍTULO 1 – CONCEITOS E DEFINIÇÕES IMPOSTA NA LEI

Preliminarmente, para compreender a extensão das boas práticas sobre a lei geral de proteção de dados é imprescindível compreender a extensão dos conceitos e definições das expressões empregadas pela lei. Vejamos:

1.1 Titular do dado pessoal: é toda e qualquer informação relacionada a pessoa natural identificada ou identificável.

1.2 Dado pessoal: é toda e qualquer informação relacionada a pessoa natural identificada ou identificável.

1.3 Dado pessoal sensível: é o dado pessoal 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.

1.4 Dado anonimizado: é o dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

1.5 Banco de dados: é o conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

1.6 Agentes de tratamento: são os controlador e operador.

1.7 Controlador: é o responsável, podendo ser pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

1.8 Operador: é o responsável, podendo ser pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

1.9 Encarregado: é a 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).

1.10 Tratamento de dados: 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.

1.11 Anonimização: é a 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 um indivíduo.

1.12 Consentimento de vontade para o uso dos dados: é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

1.13 Bloqueio de dados: é a suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

1.14 Eliminação de dados: é a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

1.15 Transferência internacional de dados: é a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

1.16 Uso compartilhado de dados: é a comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos 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.

1.17 Relatório de impacto à proteção de dados pessoais: é a 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.

1.18 Órgão de pesquisa: é o órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

1.19 Autoridade nacional: é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

CAPÍTULO 2 – APLICAÇÃO DA LEI PARA TODOS OS EFEITOS DE TRATAMENTOS DE DADOS PESSOAIS

A lei em comento apresenta no seu artigo 3º que os seus termos normativos alcançam qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que **(a)** a operação de tratamento seja realizada no Brasil, (**b**) tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional e (**c**) os dados pessoais objeto do tratamento, tenham sido coletados no território nacional, ou seja, quando o titular dos dados pessoais se encontre no Brasil ao tempo da coleta.

Outrossim, a LGPD também evidencia os casos de não aplicação do tratamento de dados pessoais, que ocorrem quando é **(i)** realizado por pessoa natural para fins exclusivamente particulares e não econômicos; **(ii)** para fins exclusivamente jornalístico e artísticos ou acadêmicos, aplicando-se a esta hipótese os artigos 7º e 11 da lei; **(iii)** para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; ou **(iv)** provenientes do exterior e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na Lei.

CAPÍTULO 3 – PRINCÍPIOS A SEREM OBSERVADOS NO TRATAMENTO DE DADOS PESSOAIS

A LGPD estabeleceu em sua estrutura legal uma ordem principiológica que garante maior segurança de direitos aos titulares de dados pessoais, que devem ser observadas pelos controladores de dados durante toda a existência do tratamento dos dados pessoais do titular realizado pelo órgão ou entidade. Os princípios estabelecidos pela lei são:

3.1 Princípio da finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (artigo 6º, inciso I).

3.2 Princípio da adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento (artigo 6º, inciso II).

3.3 Princípio da necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (artigo 6º, inciso III).

3.4 Princípio do livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (artigo 6º, inciso IV).

3.5 Princípio da qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (artigo 6º, inciso V).

3.6 Princípio da transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (artigo 6º, inciso VI).

3.7 Princípio da segurança: utilização de 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 (artigo 6º, inciso VII).

3.8 Princípio da prevenção: adoção de medidas adequadas para a prevenção de danos, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (artigo 6º, inciso VIII).

3.9 Princípio da não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos (artigo 6º, inciso IX).

3.10 Princípio da responsabilização e prestação de contas: demonstração, pelo agente de tratamento, 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 (artigo 6º, inciso X).

CAPÍTULO 4: REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados Pessoais apresenta os requisitos para a efetivação do tratamento dos dados pessoais, compreendendo como condições necessárias àquelas enumeradas no artigo 7º e para as hipóteses autorizativas o tratamento de informações pessoais sensíveis serão regulados segundo disposto no artigo 11, ficando assim definidos:

HIPÓTESE DE TRATAMENTO	DISPOSITIVO LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS	DISPOSITIVO LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS
Mediante consentimento do titular	LGPD, art. 7º, inc. I	LGPD, art. 11, inc. I
Para o cumprimento de obrigação legal ou regulatória	LGPD, art. 7º, inc. II	LGPD, art. 11, inc. II, alínea *a*
Para a execução de políticas públicas	LGPD, art. 7º, inc. III	LGPD, art. 11, inc. II, alínea *b*
Para a realização de estudos e pesquisas	LGPD, art. 7º, inc. IV	LGPD, art. 11, inc. II, alínea *c*
Para a execução ou preparação de contrato	LGPD, art. 7º, inc. V	Não se aplica
Para o exercício de direitos em processo judicial, administrativo ou arbitral	LGPD, art. 7º, inc. V	LGPD, art. 11, inc. II, alínea *d*
Para a proteção da vida ou da incolumidade física do titular ou de terceiro	LGPD, art. 7º, inc. VII	LGPD, art. 11, inc. II, alínea *e*
Para a tutela da saúde do titular	LGPD, art. 7º, inc. VIII	LGPD, art. 11, inc. II, alínea *f*
Para atender interesses legítimos do controlador ou de terceiro	LGPD, art. 7º, inc. IX	Não se aplica
Para proteção do crédito	LGPD, art. 7º, inc. X	Não se aplica
Para a garantia da prevenção à fraude e à segurança do titular	Não se aplica	LGPD, art. 11, inc. II, alínea *g*

CAPÍTULO 5: SEGURANÇA DA INFORMAÇÃO

Na Intercore Intermediação de Negócios Ltda. a segurança da informação sobre os dados pessoais tem valor primordial no desenvolvimento das suas atividades corporativas, sendo empenhados recursos técnicos quantos bastem para elevar o nível de proteção para os seus titulares de direito, evitando-se assim prejuízos de todas as naturezas, em cada fase do ciclo de vida dos dados pessoais, que tem início com a coleta do dado e se encerra com a eliminação ou descarte.

Acerca das fases do ciclo de vida, estas são definidas nas operações de tratamento indicadas na LGPD, iniciando com a **(i)** fase coleta refere-se à coleta, produção e recepção de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, sistema de informação etc.); tendo também a **(ii)** fase da retenção corresponde ao arquivamento ou armazenamento de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, banco de dados, arquivo de aço etc.); a do **(iii)** processamento que é qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação e extração e modificação de dados pessoais retidos pelo controlador; a do **(iv)** compartilhamento que, por sua vez, envolve qualquer operação de transmissão, distribuição, comunicação, transferência, difusão e uso compartilhamento de dados pessoais; e por fim, a da **(v)** eliminação é qualquer operação que visa excluir um dado ou conjunto de dados pessoais armazenados em banco de dados, em virtude do tratamento da LGPD.

Coleta → Retenção → Processamento → Compartilhamento → Eliminação.

As operações de tratamento de dados pessoais se cruzam com os procedimentos e as operações da gestão de documentos, nas fases do ciclo de vida do documento das pessoas naturais, sendo que quando se tratarem de dados pessoais

integrados a documentos arquivísticos, os procedimentos e as operações da gestão de documentos precisam ser efetivados conjuntamente, como por exemplo, produção, recebimento, tramitação, arquivamento, classificação, indexação, atribuição de restrição de acesso, avaliação, transferência, acesso e eliminação.

CAPÍTULO 6: REGRAS DE BOAS PRÁTICAS E DE GOVERNANÇA DE DADOS

Este capítulo derradeiro funda-se na apreensão do conceito normativo apresentado no artigo 50 da LGPD, apresentando as regras de boas práticas e de governança de dados aplicadas no âmbito do desenvolvimento das atividades empresariais da Intercore Intermediação de Negócios Ltda., que levam em consideração as condições organizacionais, o regime de funcionamento e os seus procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Executando-se a governança, as tecnologias e a conformidade documental em:

a) Definição de encarregado para a segurança dos dados: o DPO tem a sua identidade e contato divulgados publicamente no *site* da empresa, cabendo-lhe aceitar reclamações e comunicações dos titulares dos dados, prestar esclarecimentos e adotar providências junto a Autoridade Nacional (ANPD), orientar os funcionários e os contratados da empresa sobre as práticas a serem tomadas em relação à proteção dos dados pessoais, executar demais funções, a fim de a segurança imposta pela lei seja alcançada.

b) Revisão contínua das políticas de segurança de informação: o DPO conjuntamente ao departamento de proteção de dados, se incumbe de analisar periodicamente todas as medidas adotadas pela organização para detectar e corrigir possíveis problemas quanto à proteção dos dados pessoais, atuando com diretrizes direcionadas a processos, pessoas e tecnologia. Prima-se por uma padronização das regras e dos processos de tratamento de dados, que em constante movimento e atualização privilegiam uma política de segurança da informação planejada para o alcance dos princípios básicos da segurança da informação: integridade, confidencialidade e disponibilidade das informações.

c) Adoção de soluções de *cloud computing*: é utilizada computação em nuvem, porquanto tratar-se de uma solução que cumpre vários requisitos de segurança, ajudando no armazenamento seguro dos dados e nos *backups* periódicos. Além de se despontar como uma solução mais ágil e que se adapta rapidamente às mudanças e às adequações necessárias para a conformidade.

d) Atenção aos dispositivos móveis dos colaboradores: sem invasão de privacidade e/ou cerceamento de quaisquer outros direitos, portanto, com toda cautela cabível, existe um cuidado sobre o uso de dispositivos particulares dos colaboradores no ambiente de trabalho analisado com cautela. Havendo uma dissipação de informações para todos sobre as políticas de segurança de dados da empresa, porquanto a necessidade de cientificar das responsabilidades no manuseio dos dados que circulam na empresa; reforçando a segurança dos *softwares* utilizados nos dispositivos, a fim de que seja evitado vazamentos e invasões (intencionais ou não).

e) Adoção de formas de consentimento para a coleta e o tratamento de dados: o consentimento, por escrito ou por meio virtual, dos usuários serve como o controle maior sobre o tratamento e o processamento de dados pessoais, cuidando de condição vital para que se realize a coleta, a utilização e o armazenamento pela empresa manifestação de vontade do usuário, garantindo à eles o ampla acesso ao poder de revogar o seu consentimento a qualquer tempo, através de manifestação expressa

f) Monitoramento do ambiente de TI em tempo real: evitando situações graves, como vazamentos e sequestro de dados, há um monitoramento perene sobre a infraestrutura de TI em tempo real da empresa, com uma equipe especializada, com capacidade resolutiva no processo de tratamento de dados pessoais.

g) Reavaliação dos dados pessoais coletados: nos casos dos titulares não terem consentido com a coleta e o uso de seus dados pessoais, é feito contato com estes, a fim de que oferecido aos usuários a oportunidade de ler os novos termos de uso e a política de privacidade, fornecendo um novo consentimento, caso estejam de acordo.

h) Revisão dos contratos com os fornecedores: também é importante rever os contratos com todos os fornecedores da empresa, de forma direta ou indireta. Para que se necessário for, seja estabelecido um novo contrato prevendo a conformidade legal no tratamento dos dados pessoais, sob a pena de responsabilização solidária. objetiva informá-lo sobre a forma como Você deverá tratar os dados pessoais recebidos ou aos quais tenha tido acesso em razão dos serviços prestados, essencialmente, para que todos os fornecedores/parceiros estejam em conformidade com a LGPD.

i) Treinamento destinados para os colaboradores sobre o alcance da LGPD: promoção de ciclos de palestras e de debates com os colaboradores para que eles tenham conhecimento sobre a Lei Geral de Proteção de Dados e nos impactos para a rotina dos trabalhos da empresa.

j) Atenção a possíveis mudanças na LGPD: evitando-se episódios abruptos, empenha-se zelo sobre as eventuais mudanças legais como novas alterações, medidas provisórias e novos requisitos de adequação da Lei Federal n. 13.709/2018, sobre os dados pessoais.

CONSIDERAÇÕES FINAIS

Existe por parte da Intercore Intermediação de Negócios Ltda. uma responsabilidade e uma consciência no desenvolvimento do trabalho sobre o tratamento de dados pessoais dos seus clientes, parceiros, colaboradores e fornecedores de insumos, tudo desenvolvido com o objetivo de validar as ações de medidas de segurança, técnicas e administrativas sobre o mapeamento e a análise dos seus processos organizacionais para todas as fases do ciclo de vida do tratamento de dados pessoais.

Existe um compromisso empresarial ético e impoluto para com a sociedade de garantir a todos os interessados que, independentemente da prática ou tecnologia envolvida, as operações corporativas funcionem de acordo com as premissas e objetivos declarados, designados para autenticar a visibilidade, a transparência e a privacidade dos direitos dos titulares dos dados pessoais.