POLÍTICA INTERNA DE PROTEÇÃO DE DADOS

1. Definições

Para fins de cumprimento da Lei Geral de Proteção de Dados nº 13.709/18, de acordo com o Capítulo 1 “Disposições Preliminares”, o art. 5° especifica as principais informações determinantes:

Dado pessoal: qualquer informação relacionada a uma pessoa natural identificada ou identificável.

Dado pessoal sensível: qualquer dado pessoal que contenha informação sobre:

- Origem racial ou étnica.
- Convicção religiosa.
- Opinião política.
- Filiação a sindicato ou organização de caráter religioso, filosófico ou político.
- Saúde.
- Vida sexual.
- Genética ou biometria.

Titular: Pessoa natural (física) a quem se referem os dados. Tratamento: qualquer operação com os dados pessoais, incluindo armazenamento.

Consentimento: manifestação livre e inequívoca pela qual o titular concorda com o tratamento dos seus dados pessoais para uma finalidade específica.

Operador: pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais em nome do controlador. São operadores os empregados, prestadores de serviço e demais parceiros que participam do tratamento de dados pessoais dentro da empresa.

Controlador: pessoa física ou jurídica, de direito público ou privado, que administra e toma decisões sobre o tratamento de dados pessoais.

Agentes de tratamento: o controlador e o operador.

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;

Encarregado de Dados (DPO): pessoa indicada pelo controlador para ser responsável pela comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANDP).

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

2. Objetivo da política interna de proteção de dados

A organização deve orientar a todos os membros acerca das boas práticas em proteção de dados pessoais, visando conformidade com a Lei nº 13.709 de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais.

3. Contexto da LGPD

A Lei Geral de Proteção de Dados foi aprovada em 2018, com o objetivo de trazer ao ordenamento jurídico brasileiro uma preocupação que já tem lugar em todos os países desenvolvidos: a proteção de dados pessoais. No mundo todo, a legislação de proteção a dados de pessoas naturais é um instrumento necessário para garantir maior segurança jurídica e o respeito aos direitos humanos fundamentais. Assim sendo, a conformidade com tais leis tem sido um fator importante internamente.

4. Princípios da LGPD

São os princípios norteadores da Lei Geral de Proteção de Dados e, também, os desta política interna:

Adequação: o tratamento dos dados tem que ser compatível com a finalidade informada ao titular.

Necessidade: o tratamento deve ser limitado ao mínimo necessário para atingir a finalidade proposta.

Livre acesso: os titulares têm o direito de acessar a qualquer tempo as informações referentes ao tratamento que seus dados recebem.

Qualidade dos dados: o tratamento dos dados deve mantê-los exatos, claros, relevantes e atualizados, sem discrepâncias ou distorções.

Transparência: o tratamento dos dados deve ser explicado aos titulares de maneira transparente e acessível, observado o segredo comercial e industrial necessário.

Segurança: os dados pessoais devem ser protegidos pelo controlador, para que não sejam perdidos, alterados, destruídos ou acessados indevidamente.

Prevenção: cabe ao controlador tomar medidas para prevenir danos provenientes do tratamento de dados pessoais.

Não discriminação: o tratamento de dados pessoais não deve ser realizado com finalidades discriminatórias, ilícitas ou abusivas.

Responsabilização e prestação de contas: demonstração, aos titulares, das medidas utilizadas para garantir conformidade com a Lei Geral de Proteção de Dados Pessoais.

5. Responsabilidade compartilhada

A responsabilidade pelo correto tratamento dos dados pessoais é compartilhada entre todos que atuam como controladores e operadores, sendo fundamental a cooperação de todos para que a empresa esteja sempre em conformidade com a lei, oferecendo segurança a todos os titulares de dados pessoais sob seu controle.

Nos termos dos art. 42 e seguintes da Lei Geral de Proteção de Dados nº 13.709/18, o operador de dados pessoais que descumprir as diretrizes lícitas de proteção de dados do controlador responderá como se também fosse controlador dos dados em questão, estando assim sujeito à responsabilidade civil, administrativa e criminal sobre o tratamento inadequado dos dados.

Segundo art. 23 da mesma Lei, a violação de segredos da organização, concepção que inclui dados pessoais sob seu controle, poderá a critério exclusivo da Direção ser motivo para embasar a

demissão por justa causa de colaboradores ou a rescisão de contrato de prestadores de serviços envolvidos na violação, sem prejuízo das ações de regresso cabíveis judicialmente.

6. Tratamento dos dados pessoais

O tratamento de dados deve seguir os princípios definidos nesta política, devendo ser estritamente voltado às finalidades às quais as coletas dos dados se destinam, respeitando os princípios desta política e os critérios de compartilhamento e de segurança das informações.

Os dados pessoais devem ser manipulados apenas por pessoas que precisem lidar com eles. Assim, reduzem-se os riscos de falhas humanas propiciando um vazamento ou uso inadequado da informação. Para garantia, é necessário dividir os dados por setores e por responsabilidades específicas dentro de cada setor. Assim se saberá em cada situação quem são os operadores dos dados e os riscos de um incidente na segurança da informação diminuem.

Para garantir este tratamento setorizado dos dados, cada acesso ao banco de dados da empresa é individual e intransferível. Assim, somente pessoas autorizadas poderão ter acesso.

O mero acesso e/ou a utilização indevida de quaisquer dados pessoais armazenados ou processados pela empresa são terminantemente proibidos, sob pena de demissão por justa causa (ou rescisão do contrato de prestação de serviços e/ou fornecimento), sem prejuízo da responsabilização cível e criminal cabível em âmbito judiciário do infrator.

7. Critérios de coleta dos dados pessoais.

As informações referentes a pessoas físicas somente devem ser coletadas na medida da necessidade para a prestação de serviços e/ou fornecimento. Em todas as hipóteses é devido o consentimento para o tratamento dos dados, que deverá ser obtido em conformidade com a Lei Geral de Proteção de Dados nº 13.709/18.

O consentimento é requerido ao solicitar os dados aos titulares, quando necessário, através do aceite no campo apropriado do sistema ou mediante e-mail resposta à solicitação.

8. Critérios de armazenagem dos dados pessoais.

Quanto à armazenagem, devem seguir as seguintes diretrizes:

Quando armazenados fisicamente: os dados devem ficar em local protegido, fora do alcance de outras pessoas que não são expressamente autorizadas a acessá-los.

Quando armazenados digitalmente: devem ficar em pasta protegida por criptografia e restrição de acesso por senha pessoal.

Eventuais cópias de dados pessoais somente devem ser feitas em caso de necessidade para cumprimento da finalidade proposta ao tratamento, todas as cópias devem ser administradas internamente e protegidas para que não ocorra vazamento de dados.

9. Critérios de compartilhamento interno de dados pessoais.

Os dados pessoais somente podem ser compartilhados com pessoas cuja função dentro da empresa exija que elas tenham acesso. Por exemplo: dados referentes a saúde ocupacional, como atestados médicos, exames admissionais e outros, só podem ser compartilhados dentro da empresa com pessoas responsáveis pelo tratamento dessas informações, como o responsável pelo RH. Não podendo ser compartilhados com alguém da área técnica que não precise ter acesso a esses dados para o cumprimento de suas funções.

10. Critérios de compartilhamento externo de dados pessoais.

O compartilhamento de dados pessoais com pessoas ou entidades externas à empresa deve ser restrito ao mínimo necessário para a execução dos contratos e prestações de serviços e/ou fornecimentos, que os titulares estão envolvidos, incluindo o cumprimento de obrigações legais. Mesmo quando o tratamento envolver diretamente a prestação de serviços e/ou o fornecimento, o consentimento para este tratamento e compartilhamento deverá ter sido previamente obtido.

11. Critérios de eliminação dos dados pessoais.

Quando atingida a finalidade do tratamento dos dados pessoais e o armazenamento, para satisfazer quaisquer exigências legais, for desnecessário, estes deverão ser devidamente eliminados física e digitalmente. O titular deve ser comunicado desta eliminação nos casos em que ela se dê de maneira diversa à prevista no termo de consentimento aplicável.

12. Prestação de informações e transparência.

Os operadores de dados pessoais deverão prover todas as informações requeridas pelos titulares acerca do tratamento de seus dados pessoais, respeitando o direito da empresa de manter sigilo comercial quando cabível. A finalidade do tratamento deve ser sempre evidenciada e transparente.

Quando houver solicitação da prestação de informações sobre os dados pessoais pelo titular destes, os operadores deverão informar ao Encarregado da Proteção de Dados Pessoais sobre a solicitação e então prestar as informações solicitadas ao titular.

13. Encarregado da Proteção de Dados Pessoais (DPO).

O encarregado da proteção de dados pessoais DPO é a pessoa responsável, nos termos da Lei Geral de Proteção Dados nº 13.709/18, pela comunicação com os titulares.

São atribuições do encarregado: verificar os riscos existentes, apontar as medidas corretivas e avaliar periodicamente a segurança de dados pessoais dentro da empresa, devendo também realizar eventuais comunicações necessárias com os titulares ou com o poder público.

Quaisquer questionamentos que surgirem no dia a dia da empresa acerca da proteção de dados pessoais devem ser levados ao encarregado para que este possa orientar de imediato o operador ou buscar junto às entidades especializadas uma orientação adequada ao questionamento levantado.

14. Relatório de Impacto à Proteção de Dados Pessoais.

O Encarregado da Proteção de Dados Pessoais manterá relatório de avaliação de riscos e impactos à proteção de dados pessoais, por meio dele, as medidas necessárias à segurança da informação de dados pessoais poderão ser estruturadas, implementadas e avaliadas.

Quando necessário é realizada a elaboração de um relatório de impacto e o encarregado de dados ficará responsável por informar os riscos e procedimentos necessários quando ocorre o vazamento de dados.