POLÍTICA INTERNA DE PROTEÇÃO DE DADOS

1. Definições

Para fins de cumprimento do Regulamento Geral de Proteção de Dados (RGPD), de acordo com o Capítulo 1, art. 4° "Definições" especifica as principais informações determinantes:

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

Dados genéticos: dados pessoais relativos às características genéticas herdadas ou adquiridas de uma pessoa singular, que fornecem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resultam, em particular, de uma análise de uma amostra biológica proveniente do organismo natural pessoa em questão.

Dados biométricos: os dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitem ou confirmam a identificação única dessa pessoa singular, tais como imagens faciais ou dados dactiloscópicos.

Dados relativos à saúde: os dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de cuidados de saúde, que revelem informações sobre o seu estado de saúde.

Titular: uma pessoa singular identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador online ou a um ou mais fatores específicos da natureza física, fisiológica, identidade genética, mental, económica, cultural ou social dessa pessoa singular.

Consentimento: manifestação livre, específica e inequívoca dos desejos do titular dos dados, por uma declaração ou por uma ação afirmativa clara, expressa acordo com o tratamento de dados pessoais que lhe digam respeito.

Responsável pelo tratamento: a pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que, isoladamente ou em conjunto com outros, determina as finalidades e os meios de tratamento de dados pessoais.

Subcontratante: uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que processa dados pessoais em nome do responsável pelo tratamento.

Tratamento: toda operação ou conjunto de operação realizada com dados pessoais, por meios automatizados ou não, tais como recolha, registo, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização de outra forma, alinhamento ou combinação, restrição, apagamento ou destruição.

Restrição do tratamento: a marcação dos dados pessoais armazenados com o objetivo de limitar o seu tratamento no futuro.

Definição de perfis: qualquer forma de tratamento automatizado de dados pessoais que consiste na utilização de dados pessoais para avaliar determinados aspectos pessoais relativos a uma pessoa singular, em particular para analisar ou prever aspectos relativos ao desempenho dessa pessoa singular no trabalho, situação económica, saúde, preferências pessoais, interesses, confiabilidade, comportamento, localização ou movimentos.

Pseudonimização: o tratamento de dados pessoais de tal forma que os dados pessoais já não possam ser atribuídos a um titular de dados específico sem a utilização de informações adicionais, desde que essas informações adicionais sejam mantidas separadamente e estejam sujeitas a medidas técnicas e organizacionais assegurar que os dados pessoais não são atribuídos a uma pessoa singular identificada ou identificável.

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 o Regulamento Geral de Proteção de Dados (RGPD).

3. Contexto da GDPR

O Regulamento Geral sobre a Proteção de Dados da União Europeia entrou em vigor em maio de 2018, sendo adotada como padrão e como base para o desenvolvimento de legislações aplicáveis em países da América.

Começou a ser idealizado em 2012, sendo aprovado em 2016, substituindo assim a Diretiva 95/46 CE, de 1995, a qual mesmo com atualizações, já não correspondia aos avanços tecnológicos e comerciais.

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 GDPR

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.

Legalidade: atenção aos limites de tratamento dos dados conforme a legislação específica, nos termos do art. 6° do Regulamento Geral de Proteção de Dados.

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.

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 Responsável pelo tratamento, para que não sejam perdidos, alterados, destruídos ou acessados indevidamente.

Prevenção: cabe ao Responsável pelo tratamento 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 responsáveis pelo tratamento e subcontratantes, sendo fundamental a cooperação de todos para que a organização esteja sempre em conformidade com a lei, oferecendo segurança a todos os titulares de dados pessoais sob seu controle.

Nos termos do art. 26 da GDPR, sempre que dois ou mais responsáveis pelo tratamento determinarem conjuntamente as finalidades e os meios de tratamento, serão responsáveis conjuntos pelo tratamento.

Os responsáveis poderão acordar quanto as respetivas responsabilidades, bem como quanto o cumprimento das obrigações decorrentes da GDPR. O acordo deve refletir devidamente as respetivas funções e relações dos responsáveis conjuntos pelo tratamento relativamente aos titulares dos dados.

A essência do acordo será disponibilizada ao titular dos dados.

Em caso de violação de dados pessoais, o responsável pelo tratamento deve, sem demora injustificada e, sempre que possível, o mais tardar 72 horas após ter tomado conhecimento dela, notificar a violação de dados pessoais à autoridade de controle competente

Caso a notificação à autoridade de controle não seja feita no prazo de 72 horas, deve ser acompanhada dos motivos do atraso.

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 organização 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 responsabilização do responsável pelo tratamento ou subcontratante, de forma material e imaterial, em consequência do descumprimento do regulamento.

7. Critérios de coleta dos dados pessoais.

As informações referentes a pessoas singulares identificada ou identificável 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 de forma específica, informada e inequívoca dos desejos do titular dos dados, pela qual ele ou ela, por uma declaração ou por uma ação afirmativa clara, expressa acordo com o tratamento de dados pessoais que lhe digam respeito.

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, como atestados médicos, exames e outros, só podem ser compartilhados dentro da organização com pessoas responsáveis pelo tratamento dessas informações. 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 organização 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 responsáveis pelo tratamento e os subcontratados 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 subcontratantes deverão informar ao Responsável da Proteção de Dados Pessoais sobre a solicitação e então prestar as informações solicitadas ao titular.

13. O Responsável da Proteção de Dados Pessoais.

O Responsável pela Proteção de Dados, é um indivíduo, pessoa física, que pode desempenhar outras funções dentro da organização, além da função de Responsável pela Proteção de Dados. Sendo que, não pode haver conflito de interesses entre as outras tarefas e os deveres do referido indivíduo.

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

Quaisquer questionamentos que surgirem no dia a dia da organização 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.

O responsável pelo tratamento e o subcontratante devem garantir que o responsável pela proteção de dados é envolvido, de forma adequada e atempada, em todas as questões relacionadas com a proteção de dados pessoais.

Os titulares dos dados podem contactar o responsável pela proteção de dados sobre todas as questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos seus direitos ao abrigo do presente regulamento.

14. Relatório de Impacto à Proteção de Dados Pessoais.

O Responsável 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 Responsável de dados ficará responsável por informar os riscos e procedimentos necessários quando ocorre o vazamento de dados.