GESTÃO INTEGRADA DE DOCUMENTOS

Dúvidas? Contate o DPO:
https://www.gid.net.br
2020/2021

7 passos para adequação

Lei Geral de Proteção de Dados

A quem se destina este guia?

Este guia visa ajudar as empresas que lidam essencialmente com os dados pessoais de clientes, funcionários e demais fontes que contenham dados pessoais. Trata-se, por exemplo, de comerciantes, lojas, prestadores de serviços e demais.

Este guia, portanto, destaca os passos para que você, controlador, se adeque à LGPD (Lei 13.709/2018).

Os dados pessoais são quaisquer informações que digam respeito a um indivíduo (pessoa física), denominado "Titular". Podem incluir, por exemplo: nome, apelido, data de nascimento, e-mail ou seus dados de localização do mapa no seu celular. No geral, serão os dados que você detém sobre os seus funcionários, clientes ou fornecedores.

Quanto menos riscos as suas atividades colocarem aos dados pessoais, menos você precisará fazer!

Direitos dos titulares de dados pessoais

- ✓ *confirmação da existência de tratamento;*
- ✓ *acesso aos dados;*
- ✓ *correção de dados incompletos/inexatos/desatualizados;*
- ✓ *anonimização;*
- ✓ *portabilidade;*
- ✓ *eliminação;*
- ✓ *inf. a respeito do compartilhamento de dados;*
- ✓ *inf. sobre não fornecer o consentimento e as consequências;*
- ✓ *revogação do consentimento.*

Dica!

- **recolha dados pessoais com um objetivo claramente definido e não os utilize para outros fins** (se diz aos seus clientes para fornecerem o seu e-mail para que possam receber novas ofertas ou promoções, não pode utilizar esse mesmo dado para outros fins ou vendê-lo a outras empresas).
- **não recolha mais dados do que aqueles de que precisa** (se faz entregas ao domicílio, necessita, por exemplo, de um endereço e do nome do destinatário, mas não tem de saber se essa pessoa é casada ou solteira) — basicamente, esteja atento aos dados pessoais sob o seu controle.

PASSO 1 — VERIFIQUE OS DADOS PESSOAIS QUE VOCÊ RECOLHE E TRATA, A FINALIDADE E O FUNDAMENTO JURÍDICO PARA TAL PROCESSO

Se tem **funcionários**, os seus dados pessoais são objeto de tratamento com base no contrato de trabalho e nas obrigações legais (por ex., comunicações à autoridade tributária/previdência social).

Se estiver trabalhando com **fornecedores** ou **clientes empresariais**, então faça com base em contratos, sempre considerando as cláusulas de tratamento de dados claramente propostas e direcionadas.

Pode gerir uma lista de **clientes individuais**, por exemplo, para enviar notícias sobre ofertas especiais/publicidade caso tenha obtido o consentimento desses clientes.

Mas nem sempre necessita do consentimento. Existem casos em que as pessoas esperam que os seus dados sejam objeto de tratamento. Por exemplo, como tele entregas que podem tratar os dados de endereço de entrega para publicitar um dos seus novos produtos. Isto chama-se interesse legítimo. Se o titular dos dados o solicitar, tem de o informar sobre a utilização pretendida e deixar de efetuar o tratamento dos seus dados.

- ✓ ***A base legal do tratamento de dados pessoais é o ponto chave!***
- ✓ ***Envolva a alta direção para suportar a implantação do projeto!***

PASSO 2 — INFORME OS SEUS CLIENTES, FUNCIONÁRIOS E OUTROS INDIVÍDUOS QUANDO RECOLHE OS SEUS DADOS PESSOAIS

Os titulares devem saber se os seus dados pessoais são objeto de tratamento, quais as finalidades e se há compartilhamento. No entanto, não é necessário informar os indivíduos quando estes já estão informados sobre como vai utilizar os seus dados, por exemplo, quando um cliente lhe pede para fazer uma entrega em casa.

Informe os indivíduos sobre os dados pessoais que possui deles e forneca-lhes acesso a esses dados, caso o solicitem. Mantenha os seus dados organizados. Desta forma, quando um cliente necessitar saber que tipo de dados pessoais possui sobre ele, você pode facilmente fornecê-los sem grandes inconvenientes.

- ✓ ***Implemente um Aviso de Privacidade e torne-o público!***
- ✓ ***Informe e Implemente os Direitos dos Titulares!***

PASSO 3 — GUARDE OS DADOS PESSOAIS APENAS DURANTE O TEMPO NECESSÁRIO

Dados sobre os seus clientes: durante o tempo de duração da relação com o cliente e em conformidade com as obrigações legais pertinentes (por exemplo, para fins fiscais).

Dados sobre os seus funcionários: durante a relação laboral e em conformidade com as obrigações legais pertinentes.

- ✓ ***Implemente uma Política de Retenção de Dados!***

PASSO 4 — MANTENHA SEGUROS OS DADOS QUE ESTÃO SUJEITOS AO TRATAMENTO

Se armazenar estes dados num **software/app**, limite o acesso aos registros, pastas, e demais, por exemplo, através de senhas ou utilizando autenticação de duplo fator. Atualize regularmente as definições de segurança do seu sistema.

Se armazenar documentos físicos com dados pessoais, certifique-se de que estão inacessíveis a pessoas não autorizadas; feche-os num cofre ou armário.

- ✓ ***Implemente uma Política de Proteção de Dados!***
- ✓ ***Implemente uma Política de Controle de Acesso!***

PASSO 5 — DOCUMENTE AS SUAS ATIVIDADES DE TRATAMENTO DE DADOS

Elabore um documento resumido no qual explica que dados pessoais detém e quais os motivos. Poderá ter de disponibilizar a documentação à autoridade nacional de proteção de dados (ANPD), quando solicitado.

Esta documentação deverá incluir, no mínimo, as informações referidas abaixo.

- ✓ ***Implemente o Mapeamento do Fluxo de Dados!***

INFORMAÇÃO	EXEMPLOS
A função de négocio/processo relacionada	Gestão de Clientes; Gestão de RH; Administrativo; Marketing.
A finalidade do tratamento de dados	Alertar os clientes sobre ofertas especiais/fazer entregas ao domicílio; pagar a fornecedores; pagamento de salários e da previdência social dos funcionários.
Os tipos de dados pessoais	Dados de contato dos clientes, dados de contato de fornecedores; dados dos funcionários; dados profissionais.
As categorias dos titulares dos dados em causa	Funcionários; clientes; fornecedores.
As categorias dos destinatários	Autoridades competentes do trabalho; autoridade tributária; autoridade fiscal.
Os períodos de armazenamento	Dados pessoais de funcionários até ao fim do contrato de trabalho (e obrigações legais pertinentes); dp de clientes até ao fim da relação com o cliente/contratual.
As medidas de segurança técnica e organizacionais para proteger os dados pessoais	Soluções dos sistema de informação atualizadas com regularidade; criptografia; armário com chave/cofre.
Se os dados pessoais são transferidos para destinatários fora do Brasil	Utilização de um operador fora do Brasil (ex.: armazenamento cloud nos EUA).

PASSO 6 — CERTIFIQUE-SE DE QUE OS PARCEIROS SUBCONTRATADOS RESPEITAM AS LEIS

Se subcontratar o tratamento dos dados pessoais a outra empresa, utilize apenas um fornecedor de serviços que garanta o tratamento em conformidade com os requisitos da LGPD (por exemplo, as medidas de segurança). Antes de assinar um contrato, verifique se já procederam às alterações e adaptações à LGPD, mencionando isto no contrato e tornando todas as operações sempre transparêntes e auditáveis.

- ✓ ***Implemente um Acordo de Processamento de DP (DPA)!***
- ✓ ***Implemente uma Política de Due Diligence!***

PASSO 7 — VERIFIQUE SE ESTÁ CUMPRINDO AS DISPOSIÇÕES ABAIXO

> DPO - para protegerem melhor os dados pessoais e os processos envonvidos, as organizações devem ter um encarregado da proteção de dados (DPO) nomeado (consultor / DPOaaS / ou empresa)

> RPID - a autoridade nacional poderá determinar que se elabore um relatório de impacto à proteção de dados pessoais, que descreve o processamento, avalia a necessidade e a proporcionalidade do tratamento e ajudar a gerir os riscos.

> Treinamento – a conscientização da importância da privacidade e proteção de dados pessoais é de extrema importância junto a todos os colaboradores e envolvidos.

> Gestão – você deve incorporar a gestão da privacidade e proteção junto à sua organização. Utilize um SGPD em conjunto com normas de segurança da informação, gerenciamento de riscos e continuidade dos negócios.

Sanções e Multas

A ANPD está autorizada a aplicar sanções de acordo com o Art. 52º "Os agentes de tratamento de dados, em razão das infrações ometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional". Veja as sanções abaixo:

- ➢ Advertência – com indicação de prazo para regularizar as medidas cabíveis;
- ➢ Multa Simples - até 2% do faturamento do último exercício, no total de R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- ➢ Multa Diária – aplicada continuamente, mas limitada ao valor máximo de cinquenta milhões de reais;
- ➢ Publicização da Infração após devidamente apurada e confirmada a sua ocorrência;
- ➢ Bloqueio/Eliminação dos Dados Pessoais a que se refere a infração até a sua regularização.

Enfim, seja sniper na gestão da privacidade!

Proteção Privacidade Precisão Proatividade