Comissão Europeia

Sete passos para as empresas

se prepararem para o Regulamento Geral sobre a Proteção de Dados

Justiça e Consumidores

A quem se destina este guia?

Este guia visa ajudar as empresas que não gerem os dados pessoais como uma atividade empresarial principal, como as PME, e que lidam essencialmente com os dados pessoais dos seus funcionários ou de listas de clientes. Trata-se, por exemplo, de comerciantes ou lojas, como as padarias ou talhos, ou de prestadores de serviços, como os arquitetos. Este guia destaca os passos que têm de ser dados para estar preparado para o RGPD.

Os dados pessoais são quaisquer informações que digam respeito a um indivíduo vivo real (não entidades jurídicas). Podem incluir, por exemplo: nome, apelido, morada, endereço de correio eletrónico ou dados de localização do mapa no seu telemóvel. No geral, serão os dados que detenha sobre os seus funcionários, clientes ou fornecedores.

Quanto menos riscos as suas atividades colocarem aos dados pessoais, menos terá de fazer

Apply key principles:

- **recolha dados pessoais com um objetivo claramente definido e não os utilize para outros fins** (se diz aos seus clientes para fornecerem o seu correio eletrónico para que possam receber novas ofertas ou promoções, não pode utilizar esse correio eletrónico 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 uma morada 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 controlo.

PASSO 1 — VERIFIQUE OS DADOS PESSOAIS QUE RECOLHE E TRATA, O OBJETIVO COM QUE O FAZ E COM QUE FUNDAMENTO JURÍDICO

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/segurança social).

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 as pessoas esperam que os seus dados sejam objeto de tratamento. Por exemplo, como vendedor de pizas pode tratar os dados da morada 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.

Se gerir uma lista de **fornecedores** ou **clientes empresariais**, então fá-lo com base nos contratos que tem com os mesmos. Os contratos não são necessariamente escritos.

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

Os indivíduos devem saber que os seus dados pessoais são objeto de tratamento e para que finalidade.

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.

Tem também de informar os indivíduos sobre os dados pessoais que possui sobre os mesmos e fornecer-lhes acesso a esses dados, caso o solicitem. Mantenha os seus dados organizados. Desta forma, quando um funcionário pretende, por exemplo, saber que tipo de dados pessoais possui sobre ele pode facilmente fornecê-los sem grande inconveniente.

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

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

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).

Elimine os dados quando deixarem de ser necessários para os fins que foram recolhidos.

PASSO 4 — MANTENHA SEGUROS OS DADOS QUE SUJEITA A TRATAMENTO

Se armazenar estes dados num **sistema informático**, limite o acesso aos ficheiros com os dados, por exemplo, através de palavra-passe. Atualize regularmente as definições de segurança do seu sistema.

(Nota: o RGPD não recomenda a utilização de um sistema informático específico)

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

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 sua autoridade nacional de proteção de dados, quando solicitado.

Esta documentação deverá incluir as informações referidas abaixo.

INFORMAÇÃO	EXEMPLOS
A finalidade do tratamento de dados	Alertar os clientes sobre ofertas especiais/fazer entregas ao domicílio; pagar a fornecedores; pagamento de salários e da segurança social dos funcionários
Os tipos de dados pessoais	Dados de contacto dos clientes, dados de contacto de fornecedores; dados dos funcionários
As categorias dos titulares dos dados em causa	Funcionários; clientes; fornecedores
As categorias dos destinatários	Autoridades competentes em matéria laboral; autoridade tributária
Os períodos de armazenamento	Dados pessoais dos funcionários até ao fim do contrato de trabalho (e obrigações legais pertinentes); dados pessoais de clientes até ao fim da relação com o cliente/contratual
As medidas de segurança técnica e organizacionais para proteger os dados pessoais	Soluções do sistema informático atualizadas com regularidade; armário com chave/cofre
Se os dados pessoais são transferidos para destinatários fora da UE	Utilização de um processador fora da UE (p. ex. para armazenamento na nuvem)

PASSO 6 — CERTIFIQUE-SE DE QUE AS ENTIDADES QUE SUBCONTRATA RESPEITAM AS REGRAS

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 do RGPD (por exemplo, as medidas de segurança). Antes de assinar um contrato, verifique se já procederam às alterações e adaptações ao RGPD. Mencione isto no contrato.

PASSO 7 — VERIFIQUE SE ESTÁ ABRANGIDO PELAS DISPOSIÇÕES ABAIXO

> Para protegerem melhor os dados pessoais, as organizações poderão ter de nomear um encarregado da proteção de dados (EPD). **Contudo, não tem de nomear um encarregado da proteção de dados** se o tratamento de dados pessoais não for uma componente essencial do seu negócio, não se tratar de um tratamento que apresente riscos ou se a sua atividade não for em grande escala.

Por exemplo, se a sua empresa apenas recolhe dados sobre os seus clientes para entregas ao domicílio, não tem de nomear um EPD.

Mesmo que precise de um EPD, este pode ser um dos seus funcionários atuais, que fica responsável por esta função para além das suas tarefas habituais. Ou pode ser um consultor externo, como os contabilistas externos utilizados por muitas empresas.

> **De uma forma geral, não tem de realizar uma avaliação de impacto sobre a proteção de dados**

Esta avaliação de impacto é reservada às empresas que apresentam mais riscos para os dados pessoais, como as que fazem monitorização em grande escala de uma zona acessível ao público (por ex., videovigilância).

Se é uma pequena empresa que apenas gere os salários dos funcionários e uma lista de clientes, não tem de executar uma avaliação de impacto sobre a proteção de dados para essas operações de tratamento.

Coimas

As autoridades de controlo competentes em matéria de proteção de dados estão autorizadas a sancionar as infrações às regras de proteção de dados. Podem adotar medidas corretivas (como uma ordem ou suspensão temporária do tratamento) e/ou impor uma coima.

A sua decisão em impor uma coima deve ser proporcional e baseada numa avaliação de todas as circunstâncias do caso individual.

Se foi decidida a imposição de uma coima, a quantia da mesma também dependerá das circunstâncias do caso, incluindo a gravidade da infração ou se esta foi intencional ou negligente. A sua atitude e intenções também serão tidas em consideração.

Se desejar obter mais informações:

1. **Visite as orientações em linha da Comissão Europeia sobre a reforma da proteção de dados — disponível em todas as línguas da UE:**

   europa.eu/dataprotection/pt

2. **Contacte a sua autoridade nacional de proteção de dados:**

   edpb.europa.eu/about-edpb/board/members_pt

AVISO IMPORTANTE

As informações contidas neste guia visam contribuir para uma melhor compreensão das regras de proteção de dados da UE.

Trata-se de um mero instrumento de orientação — apenas o Regulamento Geral sobre a Proteção de Dados (RGPD) tem valor jurídico. Por conseguinte, apenas o RGPD pode criar direitos e obrigações para os indivíduos. Estas orientações não criam direitos nem expectativas executórios.

A interpretação vinculativa da legislação da UE é da competência exclusiva do Tribunal de Justiça da União Europeia. Os pontos de vista manifestados nestas orientações não prejudicam a posição adotada pela Comissão perante o Tribunal de Justiça.

Nem a Comissão Europeia nem ninguém em nome da Comissão Europeia é responsável pela possível utilização das informações que se seguem.

Uma vez que este documento reflete o estado da arte no momento da sua elaboração, deve ser considerado como um «instrumento evolutivo» aberto a melhorias, e o seu conteúdo poderá ser modificado sem aviso prévio.

Serviço das Publicações

Luxemburgo: Serviço das Publicações da União Europeia, 2018

Print	PDF
ISBN 978-92-79-85409-5	ISBN 978-92-79-85386-9
doi:10.2838/249516	doi:10.2838/083842
DS-02-18-544-PT-C	DS-02-18-544-PT-N