CRUZ VERMELHA PORTUGUESA

Regulamento Geral sobre a Proteção de Dados (RGPD)

Guia Prático da Cruz Vermelha Portuguesa

CRUZ VERMELHA PORTUGUESA

Conteúdo

CRUZ VERMELHA PORTUGUESA

Introdução

O Regulamento Geral sobre a Proteção de Dados ("RGPD") é o novo quadro legal que irá entrar em vigor no dia 25 de maio de 2018 na União Europeia ("UE"). Os Regulamentos da UE têm aplicação direta em todos os Estados-Membros, o que significa que o RGPD prevalece sobre quaisquer leis nacionais.

O RGPD regula a proteção de dados pessoais, ou seja, dados respeitantes às pessoas singulares. Com efeito, o RGPD constitui uma das maiores alterações de sempre respeitantes ao modo como deve ser realizado o tratamento de dados de uma pessoa singular, sendo suscetível de afetar não só as empresas, mas também qualquer pessoa singular, organização, autoridade pública, agência ou outro organismo que proceda ao tratamento de dados de pessoas singulares baseados na UE. Isto inclui fornecedores e outros terceiros a que a empresa recorra para o tratamento de dados pessoais.

Tem um âmbito de aplicabilidade surpreendentemente amplo, incluindo todos os Estados-Membros da União Europeia, bem como o Reino Unido pós-Brexit em 2019, dado que o RGPD será incorporado na legislação deste país. Contrariamente às regras de proteção de dados pessoais estabelecidas pela Diretiva 95/46/CE, o RGPD afeta também quaisquer empresas estabelecidas fora da UE que ofereçam bens ou serviços a pessoas singulares na UE ou que supervisionem o seu comportamento na UE. A título de exemplo, as empresas de alojamento de sites nos Estados Unidos da América que façam o alojamento de sites acessíveis a pessoas singulares na UE serão diretamente afetadas.

O RGPD tem um impacto enorme em todos os departamentos de inúmeras empresas em todo o mundo. A título de exemplo, algumas poderão ter de contratar ou designar um encarregado da proteção de dados. Quase todas irão necessitar de implementar práticas e salvaguardas suplementares. É altamente recomendável a realização de uma auditoria por especialistas devidamente qualificado. A aplicação de coimas que podem ir até 4% do volume de negócios global anual ou 20 milhões de Euros (o que for mais elevado), torna o conhecimento RGDP indispensável.

Este documento consiste num guia conciso e simplificado para a rede CVP. É possível encontrar mais informações junto das autoridades de controlo, tais como a Comissão Nacional de Proteção de Dados (CNPD) em Portugal e as suas publicações. Queira ler a Declaração de Isenção de Responsabilidade da Cruz Vermelha Portuguesa no fim deste guia.

Visão geral do RGPD

Noções básicas

O RGPD estipula os requisitos mínimos para o tratamento de todos os dados pessoais. Os dados pessoais podem ser definidos como qualquer informação identificativa de uma pessoa singular ou a ela respeitante nas mais diversas formas (incluindo aparência física ou até dados biométricos).

A maioria das organizações recolhe dados pessoais no preciso momento em que interage com uma pessoa singular e, em alguns casos, pode até nem se aperceber que o fez. Por exemplo, a recolha de dados pessoais poderá ser algo tão simples como o uso de cookies de monitorização de sites que identifiquem um utilizador do seu site. Pode envolver algo tão detalhado como o registo de uma pessoa singular numa base de dados de gestão da relação com os clientes ("CRM") e processos ainda mais complexos. Os dados pessoais podem ser recolhidos ou tratados para benefício exclusivo da pessoa singular, o que também recai sob a alçada do RGPD.

À semelhança da Diretiva 95/46/CE, o RGPD reafirma três conjuntos de regras básicos respeitantes aos dados pessoais: Princípios da Proteção de Dados, Tratamento Lícito e restrições às Transferências Internacionais. A maioria das organizações já deverá ter conhecimento destas regras, assim como maior parte das pessoas singulares ficarão a par das mesmas. Estes três conjuntos de regras estão descritos mais pormenorizadamente neste documento.

Recomendamos que os leia, nem que seja para relembrar conhecimentos já adquiridos. Contudo, o RGPD introduz vários e importantes requisitos novos.

Síntese do RGPD

Eis as áreas fundamentais da atuação do RGPD, com especial referência à Diretiva 95/46/CE sobre a proteção de dados.

Os direitos das pessoas singulares e sua sensibilização

A legislação em vigor na UE sobre a proteção de dados (Diretiva 95/46/CE) confere às pessoas singulares direitos sobre os seus dados pessoais e descreve quais as informações que têm de lhes ser facultadas pelas empresas, designadamente acerca da finalidade a que esses dados

pessoais se destinam. É frequente estas informações serem facultadas através de declarações ou notificações de privacidade disponibilizadas num site.

O RGPD expande significativamente o seu âmbito de aplicabilidade, estabelecendo direitos adicionais que têm de ser novamente comunicados às pessoas singulares. Em especial, as pessoas singulares têm de ser informadas de que têm os seguintes direitos (lista meramente indicativa):

1. Apresentar uma queixa junto das autoridades de controlo, como a CNPD em Portugal;

2. Retirar o consentimento para o tratamento dos respetivos dados pessoais (ver abaixo);

3. Aceder aos respetivos dados pessoais, bem como solicitar a sua retificação ou eliminação (o "direito a ser esquecido") às empresas ou a quaisquer terceiros que a eles tenham tido acesso;

4. Ser informado da existência de qualquer tratamento automatizado de dados pessoais (incluindo a criação de perfis);

5. Opor-se a certos tipos de tratamento, como marketing direto e decisões baseadas apenas no tratamento automatizado;

6. Ser informado sobre o período de retenção dos dados pessoais;

7. Ser informado sobre a identidade e contactos de qualquer Encarregado de Proteção de Dados (ver abaixo).

Além disso, as pessoas singulares têm o direito de recorrer a organizações sem fins lucrativos para fazerem valer os seus direitos e interporem ações judiciais em seu nome, semelhantes às ações coletivas nos Estados Unidos.

Consentimento

Caso esteja a recolher dados com base no consentimento das pessoas singulares, ainda que a legislação da UE em sede de proteção de dados tenha sempre exigido que esse consentimento fosse livre, específico e informado, com o RGPD este consentimento tem de ser confirmado por uma declaração ou qualquer outro ato positivo claro. Dito de outro modo, as opções pré-selecionadas nos sites, ou o silêncio/omissão por parte da pessoa singular após a leitura da declaração de privacidade, não constituem um consentimento.

Além disso, o consentimento não pode ser universal, na medida em que uma empresa não pode usar um único consentimento da pessoa singular numa fase da sua transação como consentimento para outros tipos de tratamento de dados pessoais.

São necessários consentimentos separados para operações diferentes de tratamento de dados pessoais. Por fim, as pessoas singulares têm não só de ser informadas de que podem retirar o consentimento a qualquer momento, mas também de que o consentimento é tão fácil de retirar quanto de dar.

Os consentimentos existentes concedidos pelas pessoas singulares têm de ser revistos para assegurar a conformidade com os requisitos do RGPD. Se existirem conflitos ou ambiguidades, as empresas terão de criar uma nova base lícita para o tratamento de dados (por exemplo, se for necessário para o cumprimento de um contrato), obter novo consentimento ou cessar o tratamento dos dados pessoais.

Direito de circulação ou transferência de dados pessoais (portabilidade dos dados)

As pessoas singulares têm agora o direito à circulação, cópia ou transferência dos seus dados pessoais de um local para outro ou até mesmo para uma empresa concorrente. Por exemplo, o utilizador de um serviço de música que criou uma lista de reprodução pode levar esta lista consigo caso decida mudar de fornecedor de serviço. Deste modo, os dados pessoais têm de estar num formato estruturado, de uso corrente e de leitura automática para que possam ser facilmente utilizados e partilhados. A exigência de tornar os dados verdadeiramente portáteis e fáceis de utilizar por outros irá muito provavelmente implicar ajustamentos significativos ao nível das TI e, portando, ao nível dos custos.

Âmbito de aplicabilidade alargado

Muito simplesmente, o RGPD torna responsáveis pelas violações de dados não só a empresa que recolhe os dados pessoais, mas também qualquer terceiro que faça o tratamento de dados em nome dessa empresa, seja esse terceiro uma outra empresa, organização ou pessoa singular. No entanto, isto não significa que uma empresa possa simplesmente transferir os dados pessoais para um terceiro e exonerar-se de qualquer responsabilidade. A empresa tem de assegurar que o terceiro prestador do serviço também está em conformidade com o RGPD.

Acresce ainda que o eventual âmbito geográfico é ampliado para além da UE, passando a abranger qualquer empresa — ou, novamente, qualquer terceiro que faça o tratamento de dados em nome da mesma — que ofereça bens ou serviços a pessoas singulares na UE, ou que supervisionem o comportamento de pessoas singulares na UE. É de notar que não é relevante se há ou não pagamento desses bens ou serviços, pelo que as instituições de caridade e as ONG estão abrangidas pelo âmbito de aplicabilidade do RGPD.

Uma vez que a UE é um parceiro comercial da maioria dos países, o âmbito de aplicabilidade mais alargado do RGPD significa que este tem repercussões em várias empresas em todo o mundo e irá realmente exigir que estas estejam em conformidade caso desejem operar em Estados-Membros da UE, quer diretamente, quer como terceiro de outrem.

Prova de conformidade

Não basta cumprir o RGPD. As empresas têm de provar a implementação à luz do requisito de "responsabilidade" do RGPD. Tal implica assegurar a conformidade com alguns requisitos bastante onerosos de retenção de registos. Em especial, têm de ser mantidos registos que detalhem as atividades* de tratamento, os pedidos de acesso pelo titular, violações de dados, como são obtidos os consentimentos e Avaliações de Impacto da Privacidade (ver abaixo).

Mais uma vez, este requisito afeta também terceiros responsáveis pelo tratamento de dados pessoais em nome de uma empresa, embora os requisitos não sejam tão detalhados. *

Aplicável a empresas que empreguem mais de 250 trabalhadores ou empresas que empreguem menos trabalhadores, mas em que o tratamento de dados seja suscetível de implicar um risco para os direitos e liberdades das pessoas singulares, não seja ocasional ou abranja categorias especiais de dados, tais como dados relativos à saúde, religião ou orientação sexual.

Privacidade do princípio ao fim

As medidas técnicas e organizacionais têm de ser postas em prática durante toda a vida útil dos dados pessoais a fim de corresponderem às expectativas de privacidade da pessoa singular — desde o início, durante a execução e até à cessação dessa atividade. Este é o princípio de "privacidade desde a conceção", o que significa que as considerações relativas à privacidade têm de ser incorporadas em todos os aspetos deste tratamento desde a conceção.

Além disso, apenas é possível efetuar o tratamento dos dados pessoais estritamente necessários para uma dada finalidade — algo designado de minimização de dados ou "Privacidade por Defeito".

De facto, a implementação da Privacidade desde a Conceção e da Privacidade por Defeito irá implicar formação constante, auditorias regulares, minimização dos dados recolhidos, restrição do acesso aos dados pessoais com base na "necessidade de conhecimento", assim como a implementação de medidas técnicas e organizacionais de segurança como a pseudonimização e a cifragem.

Notificação obrigatória de violação de dados

Em caso de violação do RGPD, as empresas responsáveis pela recolha de dados pessoais têm de notificar as autoridades de controlo — como a CNPD em Portugal - até 72 horas após terem tomado conhecimento dessa violação. Os terceiros responsáveis pelo tratamento de dados pessoais em nome dessas empresas têm de as notificar sem demora injustificada.

Quando a violação de dados for suscetível de implicar um elevado risco para as pessoas singulares envolvidas, as empresas têm também de notificá-las sem demora injustificada.

Encarregado da Proteção de Dados (DPO)

Nos termos do RGPD, as empresas e quaisquer terceiros responsáveis pelo tratamento de dados pessoais em nome dessas empresas têm de designar um Encarregado da Proteção de Dados ("DPO") se: (i) forem um organismo público; (ii) as atividades principais da empresa ou do terceiro exigirem um controlo das pessoas em grande escala; ou se as atividades principais consistirem em operações de tratamento em grande escala de categorias especiais de dados pessoais, como dados relacionados com condenações penais e infrações. O DPO tem de ter conhecimentos especializados no domínio do direito da proteção de dados, embora não tenha necessariamente de ser um funcionário, podendo, em vez disso, ser contratado para prestar esse serviço. Os dados do DPO têm de ser comunicados à autoridade de controlo, como a CNPD em Portugal.

Coimas

As coimas pelo incumprimento do RGPD são duras e podem ir até 4% do volume de negócios global anual, ou 20 milhões de euros, o que for mais elevado. Poderá ser aplicada uma coima mesmo que não haja perda de dados. Algo a ter em conta é que não há exclusões ou exceções para pequenas empresas. Além disso, as pessoas singulares têm o direito de interpor uma ação coletiva a solicitar uma investigação regulamentar formal sempre que uma empresa não cumpra o RGPD.

Princípios básicos do RGPD

Além dos novos requisitos explicados anteriormente, e como acontece com a Diretiva 95/46/CE, o RGPD reafirma os três conjuntos de regras básicos respeitantes aos dados pessoais. Podem muito simplesmente ser resumidos do seguinte modo:

• Princípios da Proteção de Dados: o tratamento dos dados pessoais tem de ser lícito, leal e transparente para as pessoas singulares a quem dizem respeito. Têm de ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma incompatível com essas finalidades. Os dados pessoais têm de ser adequados, pertinentes e limitados ao que é necessário. Têm de ser exatos e atualizados, e têm de ser tomadas todas as medidas adequadas para que os dados pessoais inexatos sejam apagados ou retificados sem demora. Têm de ser conservados de uma forma que permita a identificação da pessoa singular apenas durante o período necessário e têm de ser tratados de uma forma que garanta a sua segurança — incluindo a proteção contra a sua perda, destruição ou danificação, e o acesso não autorizado ou ilícito.

• Tratamento Lícito: o tratamento de dados pessoais só é lícito caso se verifique pelo menos uma das seguintes situações: a pessoa singular tiver dado consentimento para uma ou mais finalidades específicas; seja necessário para um contrato do qual a pessoa singular seja ou vá em breve ser parte; seja necessário para o cumprimento de uma obrigação legal (por exemplo, a entrega das declarações de impostos por uma empresa); exista uma missão de interesse público ou levada a cabo no interesse de uma autoridade pública; seja necessário para prosseguir interesses legítimos da empresa (ou de um terceiro), salvo quando prevaleçam os interesses, direitos fundamentais e liberdades da pessoa singular.

• Transferências Internacionais: o RGPD perpetua a proibição geral de enviar dados pessoais para um país fora do Espaço Económico Europeu que não garanta a proteção adequada. Até ao momento da redação deste documento, os países que a Comissão Europeia entende que garantem proteção “adequada” são: empresas norte-americanas que se enquadrem na autocertificação do Escudo de Privacidade EU-EUA (tome nota: isto não significa que os Estados Unidos, como país, sejam considerados um país que garanta proteção adequada), Andorra, Argentina, Canadá (limitado ao PIPEDA), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Jersey, Nova Zelândia, Suíça e Uruguai. Onde não haja uma decisão de adequação, as transferências podem apenas ser feitas em casos limitados, como quando haja consentimento, sejam utilizadas cláusulas contratuaistipo publicadas pela Comissão Europeia ou, no caso de transferências entre empresas, a utilização de Regras Vinculativas Aplicáveis às Empresas.

Medidas que pode tomar já

• Para saber mais, visite o site da CNPD, onde poderá encontrar legislação e informação de caráter geral. Em particular, consulte a publicação da CNPD, "10 medidas para preparar a aplicação do Regulamento Europeu de Proteção de Dados" que foi disponibilizado com o formulário para caracterização geral da vossa entidade.

• Revejam os vossos sistemas de recolha e tratamento de dados pessoais a fim de se assegurar que cumprem os requisitos do RGPD. Quem recolhe? Onde ficam guardados? Quem pode aceder? É do vosso interesse promover uma auditoria de conformidade com o RGPD, quer do ponto de vista jurídico, quer do ponto de vista tecnológico, entre outros, de uma forma simples e prática por forma a conseguirmos enquadrar todas as valências e definir processos que assegurem o RGPD.

• Assegure-se de que os seus colaboradores/voluntários e parceiros conhecem o RGPD promovendo uma ação de formação para os preparar/sensibilizar. Lembre-se de que o RGPD o torna também responsável pelos terceiros que lhe prestem serviços de tratamento de dados pessoais.

• Preenchendo com o maior detalhe possível o documento que foi disponibilizado para enquadramento geral da vossa entidade. Posteriormente irá ser disponibilizado um aconselhamento/enquadramento jurídico para compreender melhor o impacto do RGPD nas entidades da Cruz Vermelha Portuguesa.

Declaração de Isenção de Responsabilidade da Cruz Vermelha Portuguesa

A informação contida neste guia tem uma finalidade meramente informativa. Não é nem deve ser entendida como aconselhamento jurídico. Não queremos deixar de reforçar que nada substitui as diligências de averiguação aprofundada e da caracterização dos processos associados a todas as valências que existem nas entidades da Rede CVP, e caso não estejam seguros das implicações que o RGPD, tentaremos prestar o máximo apoio.

As informações remetidas pretendem sensibilizar e elucidar para a necessidade de cumprimento do novo Regulamento Geral de Proteção de Dados e que toda a Rede CVP deverá ser responsável pelo efetivo cumprimento do mesmo.