INFORMAÇÃO SOBRE O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS PESSOAIS

O Regulamento Geral sobre a Proteção de Dados define requisitos pormenorizados em matéria de recolha, armazenamento e gestão de dados pessoais, aplicáveis tanto a empresas e organizações europeias que tratam dados pessoais na UE como a empresas e organizações estabelecidas fora do território da UE que tratam dados pessoais de pessoas de vivem na UE.

(fonte: https://europa.eu/)

Conteúdo

Em que casos é aplicável o Regulamento Geral sobre a Proteção de Dados (RGPD)? 3

O que se entende por dados pessoais ? 4

Categorias especiais de dados 4

Quem trata os dados pessoais? 5

Quem controla o modo como os dados pessoais são tratados por uma empresa? 5

Quando é necessário designar um encarregado da proteção? 5

Tratamento de dados em nome de outra empresa 6

Transferências de dados para fora da UE 6

Quando é autorizado o tratamento de dados? 7

Autorizar o tratamento de dados – consentimento 8

Dar informações transparentes (direito à informação) 8

Regras específicas aplicáveis às crianças 9

Direito de acesso e direito à portabilidade dos dados 9

Direito a corrigir os dados e direito de oposição 10

Direito ao apagamento dos dados (direito a ser esquecido) 11

Decisão e definição de perfis automatizadas 11

Notificação das violações de dados 12

Resposta a pedidos de titulares 13

Avaliação de impacto 13

Manutenção de registos 14

Proteção de dados desde a conceção e por defeito 15

Incumprimento das regras e sanções 15

«Cookies» (testemunhos de conexão) 16

«Cookies» que não exigem consentimento 16

«Cookies» que exigem consentimento 16

Retirada do consentimento 17

Em que casos é aplicável o Regulamento Geral sobre a Proteção de Dados (RGPD)?

O **RGPD é aplicável** se:

- a sua empresa trata dados pessoais e está estabelecida na UE, independentemente do local onde é realizado o tratamento de dados
- a sua empresa está estabelecida fora da UE mas trata dados pessoais em relação com oferta de bens ou serviços a pessoas na UE ou segue o comportamento de pessoas na UE
- As empresas estabelecidas fora do território da UE que tratam dados de cidadãos da UE devem nomear um representante na UE.

Em que casos não é aplicável o Regulamento Geral sobre a Proteção de Dados (RGPD)?

O **RGPD não é aplicável** se:

- o titular dos dados tiver falecido
- o titular dos dados for uma pessoa coletiva
- o tratamento for efetuado por uma pessoa singular no exercício de atividades sem qualquer ligação com uma atividade comercial ou profissional

As regras de proteção de dados aplicam-se aos dados relativos a empresas? (fonte: https://ec.europa.eu/)

> Não, **as regras aplicam-se apenas a dados pessoais relativos a pessoas singulares**. Não dizem respeito a dados relativos a empresas nem a outras entidades jurídicas. **No entanto**, as informações respeitantes a **empresas unipessoais** podem constituir dados pessoais caso permitam a identificação de uma pessoa singular. As **regras também se aplicam a todos os dados pessoais relacionados com pessoas singulares no âmbito de uma atividade profissional**, como os trabalhadores de uma

empresa/organização, incluindo endereços de correio eletrónico profissionais como «nome.apelido@empresa.eu» ou os números de telefone profissionais dos trabalhadores.

O que se entende por dados pessoais ?

Dados pessoais são quaisquer informações sobre uma determinada pessoa, **identificada ou identificável**, denominada titular dos dados. Exemplos de dados pessoais:

- nome
- morada
- número do documento de identificação/passaporte
- rendimento
- perfil cultural
- endereço IP (protocolo internet)
- dados na posse de um hospital ou médico (que identifiquem de forma inequívoca uma pessoa para fins relacionados com a saúde)

Categorias especiais de dados

Não pode tratar os dados pessoais sobre:

- origem racial ou étnica
- orientação sexual
- opiniões políticas
- convicções religiosas ou filosóficas
- filiação sindical
- dados genéticos, biométricos (dados resultantes de um tratamento técnico específico relativo a características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoas singular, nomeadamente **imagens faciais ou dados dactiloscópicos**) e relativos à saúde, **exceto em casos específicos** (por exemplo, se tiver recebido consentimento explícito ou o tratamento for

(fonte: https://europa.eu/)

necessário por motivos de interesse público importante, com base no direito europeu ou nacional)

- dados pessoais relacionados com condenações penais e infrações, salvo se tal for autorizado pelo direito europeu ou nacional

Quem trata os dados pessoais?

Durante o tratamento, os dados pessoais podem passar por várias empresas ou organizações. No âmbito do ciclo de tratamento de dados pessoais, são de realçar dois perfis principais:

- o **responsável pelo tratamento**, que determina a finalidade e os meios do tratamento de dados
- o **subcontratante**, que armazena e trata dados por conta do responsável pelo tratamento

Quem controla o modo como os dados pessoais são tratados por uma empresa?

O **encarregado da proteção**, que tenha sido designado pela empresa, é responsável por controlar o modo como os dados pessoais são tratados e por informar e aconselhar os trabalhadores que tratam dados pessoais sobre as suas obrigações. O encarregado da proteção coopera igualmente com a autoridade de proteção de dados, funcionando como ponto de contacto entre esta e as pessoas singulares.

Quando é necessário designar um encarregado da proteção?

A empresa tem a obrigação de designar um encarregado da proteção quando:

- É uma **autoridade ou um organismo público**;

- fizer um acompanhamento regular ou sistemático de pessoas singulares ou tratar categorias especiais de dados
- o tratamento dos dados for uma atividade comercial principal
- tratar dados a grande escala

O encarregado da proteção pode ser um elemento do pessoal da sua organização ou pode ser contratado externamente, através de num contrato de prestação de serviços, podendo ser um indivíduo ou fazer parte de uma organização.

Tratamento de dados em nome de outra empresa

O responsável pelo tratamento apenas pode recorrer a um subcontratante que ofereça garantias suficientes, que devem ser estabelecidas num contrato escrito entre as partes envolvidas. O contrato deve também conter uma série de cláusulas obrigatórias, por exemplo, uma cláusula que preveja que o subcontratante só pode proceder ao tratamento de dados pessoais quando receber instruções para o efeito do responsável pelo tratamento.

Transferências de dados para fora da UE

O RGPD será aplicável no Espaço Económico Europeu (EEE), que inclui todos os países da UE, a Islândia, o Listenstaine e a Noruega. Quando os dados pessoais forem transferidos para fora do EEE, a proteção proporcionada pelo RGPD deve acompanhar os dados. Isto significa que, se exportar dados para o estrangeiro, a sua empresa

(fonte: https://europa.eu/)

deve assegurar-se de que é respeitada, pelo menos, uma das seguintes condições:

- a proteção assegurada no país terceiro é considerada adequada pela UE.
- a empresa tomou as medidas necessárias para prever as salvaguardas adequadas, por exemplo, incluindo cláusulas específicas no contrato celebrado com o importador de dados pessoais
- a empresa invocou motivos específicos para a transferência (derrogações), tais como o consentimento da pessoa em causa

Quando é autorizado o tratamento de dados?

Ao abrigo das regras da UE em matéria de proteção de dados, deve tratar os dados de uma forma lícita e equitativa, para fins específicos e legítimos e apenas na medida em que tal for necessário para esses fins. Para poder tratar dados pessoais, deve certificar-se de que preenche uma das seguintes condições:

- obteve o **consentimento** do titular dos dados (condição não aplicável aos colaboradores da empresa)
- o tratamento é necessário para executar um **contrato** no qual o titular dos dados é parte
- o tratamento é necessário para cumprir uma **obrigação legal**
- o tratamento é necessário para defender os **interesses vitais** do titular ou de outra pessoa
- o tratamento é necessário para **exercer funções de interesse público**
- o tratamento é necessário no **interesse legítimo** da sua empresa, desde que os direitos e liberdades fundamentais dos titulares dos mesmos não sejam afetados de forma significativa. Se os direitos dos titulares prevalecerem sobre os interesses da sua empresa, então não pode tratar os dados pessoais.

(fonte: https://europa.eu/)

Autorizar o tratamento de dados – consentimento

O RGPD prevê **regras rigorosas em matéria de tratamento de dados com base no consentimento dos titulares**. O objetivo destas regras é assegurar que o titular dos dados percebe para que é que está a dar consentimento. Isto significa que o consentimento deve ser dado de forma livre, específica, informada e inequívoca, por meio de um pedido apresentado numa linguagem simples e clara. O consentimento do titular dos dados deve ser dado através de um ato positivo, por exemplo assinalando uma casa ou assinando um formulário.

Sempre que um titular dê consentimento para o tratamento dos seus dados pessoais, só pode tratar esses dados para as finalidades para as quais o consentimento foi dado. O titular tem de ter possibilidade de retirar o consentimento.

Dar informações transparentes (direito à informação)

Deve fornecer informações claras aos titulares sobre quem está a tratar os respetivos dados pessoais e o motivo desse tratamento, incluindo, **no mínimo**, os seguintes elementos:

- a sua identificação
- por que razão trata os dados pessoais
- qual a base jurídica para o fazer
- a quem se destinam os dados (se aplicável)

Em alguns casos, deve igualmente indicar:

- os contactos do encarregado da proteção de dados, se for caso disso

(fonte: https://europa.eu/)

- o interesse legítimo da empresa, sempre que invocar este fundamento jurídico para o tratamento
- as medidas aplicadas para transferir os dados para um país fora da UE
- por quanto tempo serão conservados os dados
- os direitos de proteção dos dados dos titulares (ou seja, o direito de acesso, retificação, apagamento, limitação, oposição, portabilidade, etc.)
- a forma como o consentimento pode ser retirado (sempre que o consentimento for o fundamento jurídico para o tratamento)
- se existe ou não uma obrigação legal ou contratual de fornecer os dados
- no caso de decisões automatizadas, informações acerca da lógica, o alcance e as consequências da decisão

Deve apresentar estas **informações numa linguagem e simples e clara**.

Regras específicas aplicáveis às crianças

Se recolher dados pessoais de crianças com base no consentimento, por exemplo, para criar uma conta de rede social ou descarregar conteúdos, deve começar por **obter o consentimento parental**, por exemplo através do envio de uma notificação a um progenitor/tutor. A idade até à qual um utilizador é considerado criança varia de país para país, oscilando entre os 13 e os 16 anos.

Direito de acesso e direito à portabilidade dos dados

Os titulares dos dados têm **direito a aceder aos respetivos dados pessoais de forma gratuita**. Se um titular lhe pedir para aceder aos seus próprios dados pessoais, deve:

- informá-lo de se os dados pessoais em questão estão a ser tratados

- dar-lhe informações sobre o tratamento (finalidade do tratamento, categorias de dados pessoais tratados, destinatários dos dados, etc.)
- fornecer-lhe uma cópia dos dados pessoais que estão a ser tratados (num formato acessível)

Sempre que o tratamento tiver por base o consentimento ou um contrato, o titular pode também solicitar-lhe que lhe devolva os seus dados pessoais ou os transmita a outra empresa. Trata-se do **direito à portabilidade dos dados**. Os dados devem ser apresentados num formato de uso corrente que permita a leitura automática.

Direito a corrigir os dados e direito de oposição

Se o titular dos dados considerar que os seus dados pessoais estão incorretos, incompletos ou inexatos, tem o **direito de os retificar** ou completar, sem demoras injustificadas.

Se isto acontecer, deve informar todos os destinatários com quem partilha os dados em questão de que estes foram alterados ou apagados. Se os dados pessoais que tiver partilhado estiverem incorretos, poderá igualmente ter de informar desse facto qualquer pessoa que os tenha consultado (exceto se tal for considerado um esforço desproporcionado).

O titular dos dados pode também **opor-se a qualquer momento ao tratamento dos respetivos dados pessoais para um uso específico**, se a sua empresa tratar esses dados com base no seu próprio interesse legítimo ou no exercício de funções de interesse público. A menos que o interesse legítimo da empresa prevaleça sobre o interesse do titular dos dados, esta deve cessar o tratamento dos dados pessoais.

(fonte: https://europa.eu/)

Do mesmo modo, um titular de dados pode pedir a **limitação do tratamento dos seus dados pessoais** enquanto se determina se o interesse prevalecente é o seu próprio interesse ou o interesse legítimo da empresa. No entanto, no caso da comercialização direta, a empresa é obrigada a pôr termo ao tratamento dos dados pessoais sempre que o titular o solicite.

Direito ao apagamento dos dados (direito a ser esquecido)

Em determinadas circunstâncias, o titular dos dados pode **solicitar ao responsável pelo tratamento que apague os seus dados pessoais**, caso os mesmos deixem de ser necessários para cumprir a finalidade do tratamento. No entanto, a empresa não é obrigada a apagar os dados, se:

- o seu tratamento for necessário para respeitar a liberdade de expressão e de informação
- tiver de conservar os dados pessoais para cumprir uma obrigação legal
- existirem outras razões de interesse público para conservar os dados pessoais, tais como motivos relacionados com a saúde pública ou a investigação científica e histórica
- a conservação dos dados pessoais for necessária no âmbito de um processo judicial

Decisão e definição de perfis automatizadas

Os titulares dos dados **têm o direito de não ficarem sujeitos a nenhuma decisão tomada exclusivamente com base no tratamento automatizado**. No entanto, há algumas exceções a

esta regra, como no caso em que os titulares dão o seu consentimento explícito para o recurso a decisões automatizadas. Salvo se a decisão automatizada for autorizada por lei, a sua empresa deve:

- informar o titular acerca das decisões automatizadas
- dar-lhe o direito de solicitar a revisão da decisão automatizada por uma pessoa
- dar-lhe o direito de contestar a decisão automatizada

Por exemplo, se um banco automatizar a sua decisão de conceder ou não um empréstimo a uma determinada pessoa, essa pessoa deve ser informada da decisão automatizada e deve ser-lhe dada a possibilidade de a contestar e de requerer a intervenção humana.

Notificação das violações de dados

Fala-se de violação de dados **se os dados pessoais pelos quais a sua empresa é responsável forem divulgados**, tanto acidental como ilicitamente, a destinatários não autorizados, forem alterados ou o acesso aos mesmos for temporariamente interrompido.

Se ocorrer uma **violação de dados que represente um risco para os direitos e liberdades individuais**, deve informar a **autoridade de proteção de dados no prazo de 72horas** depois de tomar conhecimento da mesma.

Se a violação representar um risco elevado para os titulares dos dados, a empresa poderá também ser obrigada a informar dessa violação todas as pessoas afetadas.

(fonte: https://europa.eu/)

Resposta a pedidos de titulares

Se a sua empresa receber um pedido de uma pessoa que pretenda exercer os seus direitos, deve responder a este pedido sem demoras indevidas e, em qualquer caso, no **prazo de um mês a contar da receção do pedido**. Este prazo pode ser prorrogado por um período de dois meses para pedidos complexos ou múltiplos, desde que a pessoa seja informada da prorrogação. Os pedidos devem ser tratados de forma gratuita.

Se um pedido for recusado, terá de informar o interessado das razões dessa recusa e do direito que lhe assiste de apresentar uma reclamação à autoridade de proteção de dados.

Avaliação de impacto

É obrigatório fazer uma avaliação de impacto sobre a proteção de dados sempre que o tratamento previsto possa implicar um risco elevado para os direitos e liberdades das pessoas, por exemplo, no caso de serem utilizadas novas tecnologias.

Existe um **risco elevado** em caso de:

- utilização do tratamento automatizado e de mecanismos de definição de perfis para fins de avaliação de indivíduos
- monitorização a grande escala de uma área acessível ao público (por exemplo, CCTV)
- tratamento a grande escala de categorias específicas de dados (por exemplo, dados relativos à saúde) ou dados pessoais relacionados com condenações penais e infrações

(fonte: https://europa.eu/)

Nota: as autoridades de proteção de dados podem também considerar de elevado risco o tratamento de outras categorias de dados.

Se as medidas indicadas no contexto da avaliação de impacto sobre a proteção de dados não eliminarem todos os riscos elevados identificados, a autoridade de proteção de dados deve ser consultada antes do início do tratamento de dados previsto.

Manutenção de registos

Deve poder provar que a empresa atua em conformidade com o RGPD e cumpre todas as obrigações aplicáveis, nomeadamente a pedido ou em caso de uma inspeção da autoridade de proteção de dados.

Para tal, deve **conservar um registo pormenorizado** de elementos como:

- nome e contactos da empresa envolvida no tratamento de dados
- motivo ou motivos do tratamento de dados pessoais
- descrição das categorias de pessoas que fornecem dados pessoais
- categorias de organizações que recebem os dados pessoais
- transferências de dados pessoais para outro país ou organização
- período de conservação dos dados pessoais
- descrição das medidas de segurança utilizadas quando do tratamento de dados pessoais

A empresa deve igualmente **definir e atualizar regularmente orientações e procedimentos escritos e manter os trabalhadores a par dos mesmos**.

(fonte: https://europa.eu/)

Proteção de dados desde a conceção e por defeito

A **proteção de dados desde a conceção** implica que a sua empresa tenha em conta a proteção dos dados desde as primeiras etapas do planeamento de uma nova forma de tratamento de dados pessoais. Em conformidade com este princípio, o responsável pelo tratamento deve tomar as medidas de natureza técnica e organizacionais necessárias para aplicar os princípios da proteção de dados e proteger os direitos dos titulares, por exemplo, através da utilização de pseudónimos.

A **proteção de dados por defeito** implica que a sua empresa adote sempre, como definições por defeito, as definições que mais protejam a privacidade. Por exemplo, se forem possíveis duas definições para a proteção da privacidade e uma delas impedir o acesso aos dados pessoais por parte de terceiros, deverá ser essa a definição por defeito.

Incumprimento das regras e sanções

O não cumprimento do RGPD pode traduzir-se em coimas significativas, que, para determinadas infrações, podem chegar aos 20milhões de euros ou a um valor equivalente a 4% do volume de negócios mundial da empresa. A autoridade de proteção de dados pode impor medidas corretoras adicionais, como obrigar a empresa a pôr termo ao tratamento dos dados pessoais.

(fonte: https://europa.eu/)

«Cookies» (testemunhos de conexão)

Pode utilizar vários tipos de «cookies» no seu sítio Web. Consoante a finalidade do «cookie», poderá precisar do consentimento prévio dos seus utilizadores.

«Cookies» que não exigem consentimento

Exemplos de casos em que o consentimento não é necessário:

- «Cookies» utilizados exclusivamente para proceder à transmissão de uma comunicação, por exemplo, os «cookies» utilizados para repartir o tratamento dos pedidos ao servidor Web por várias máquinas («equilíbrio da carga»).
- «Cookies» que sejam estritamente necessários para fornecer um serviço em linha solicitado de forma explícita pelo utilizador, por exemplo, «cookies» que permitem o contributo do utilizador (nomeadamente se pedir aos utilizadores que preencham um formulário em linha ou usem o cesto de compras quando compram produtos no seu sítio Web) ou «cookies» de autenticação (quando os utilizadores se autenticam no seu sítio Web para iniciar uma sessão e utilizar serviços em linha, por exemplo, serviços bancários).

«Cookies» que exigem consentimento

Antes de usar determinados «cookies» para recolher dados pessoais, tem de solicitar o consentimento explícito dos respetivos titulares. Isto significa que, a primeira vez que a página Web é aberta, os «cookies» não podem estar ativados. Só pode ativar os «cookies» e utilizar as informações recolhidas graças aos mesmos após ter obtido o consentimento do utilizador.

Exemplos de casos em que o consentimento é necessário:

(fonte: https://europa.eu/)

- «Cookies» de rastreamento da atividade nas redes sociais (como os usados na publicidade comportamental ou em análises ou pesquisa de mercado).
- «Cookies» de terceiros utilizados na publicidade comportamental.

Fins a que se destinam os «cookies»

Se se utiliza «cookies» que exigem o consentimento, deve facultar à pessoa que navega no seu sítio Web informações claras e exaustivas sobre os «cookies» utilizados e os fins a que se destinam. Os utilizadores devem poder dar o seu consentimento específico em função dos fins a que se destinam os diferentes tipos de «cookies», por exemplo, devem poder dar um consentimento distinto para a utilização de «cookies» de rastreamento.

Retirada do consentimento

Deve garantir que é tão fácil para os utilizadores retirar o consentimento como aceitar os «cookies». Se o utilizador optar por retirar o seu consentimento, tem de lhe disponibilizar um serviço mínimo, por exemplo, permitir o acesso a uma parte do sítio Web.

(fonte: https://europa.eu/)