Intellectual Output 2

Manual de Apoio ao Desenvolvimento da Literacia para as Redes Sociais na Escola

O que é o RGPD?

O que são dados pessoais?

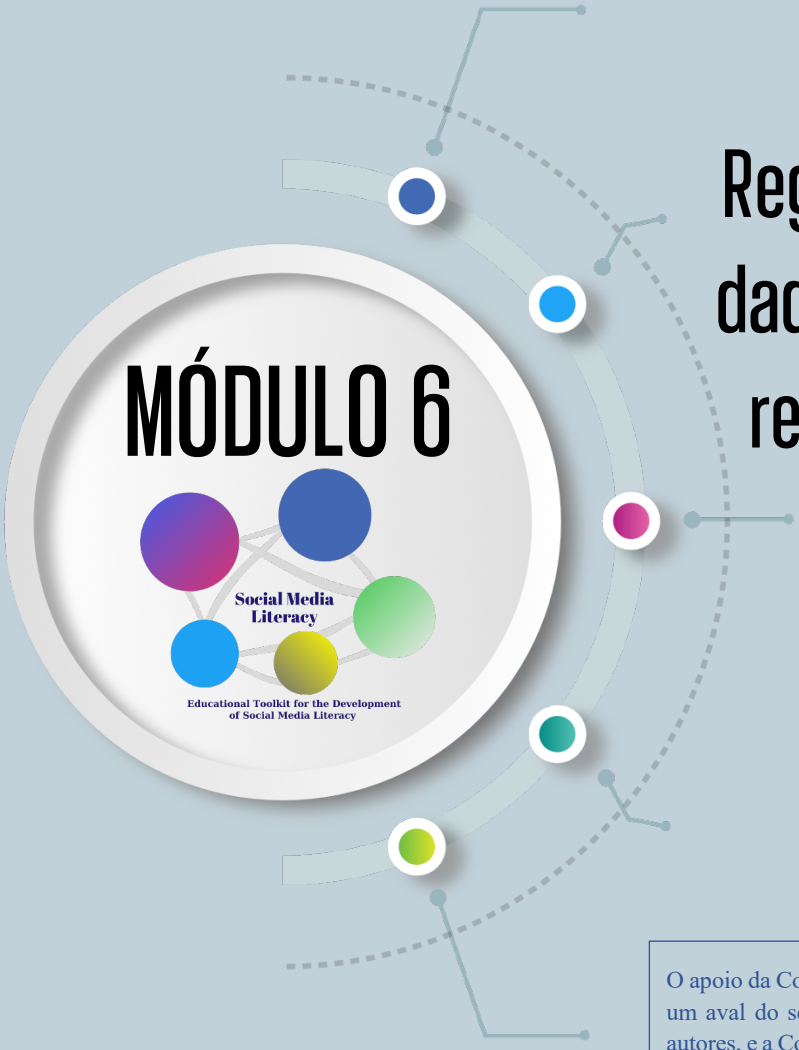
O que é processamento de dados?

Quem tem de seguir as regras do RGPD?

Regras do RGPD

Publicidade direcionada/comportamental

O que fazer em caso de infração



Regras de proteção de dados no contexto das redes sociais – RGPD

Cofinanciado pelo Programa Erasmus+ da União Europeia

Erasmus+ ref.no. 2019-1-RO01-KA201-063996

Objetivo do módulo

Ao recorrer às redes sociais, a privacidade e a proteção de dados entram inevitavelmente em jogo.

O mundo digital de hoje permite-nos partilhar tudo com todos. Todos os tipos de pessoas, organizações, empresas e até mesmo o governo processam informações sobre si, pense na sua escola, na sua comunidade ou na cidade, no seu clube desportivo, no seu empregador, etc. No entanto, a maioria das informações sobre si são recolhidas através da Internet. Especialmente em sites de redes sociais, como Facebook e Instagram, muitas informações pessoais são partilhadas. Um equívoco comum é pensar que os serviços das plataformas de redes sociais são gratuitos: na realidade são pagos, mas em vez de dinheiro, são pagos com os seus dados pessoais. Embora a interação com as redes sociais possa ser uma boa forma de se envolver com amigos e até mesmo uma forma divertida de fazer novos amigos, a partilha de informações pessoais também tem riscos. Tudo o que é partilhado *online* deixa pegadas digitais. Sempre que uma fotografia, vídeo, estado, *tweet* etc. é publicado na Internet (por exemplo, no seu perfil de redes sociais), deixa de ter controlo sobre ele: qualquer pessoa pode copiar, republicar ou guardar a fotografia, tornando-se impossível apagá-la completamente da Internet. Estas pegadas digitais podem ser "dados pessoais" (por exemplo, o seu nome, o seu endereço de e-mail, a data de nascimento, as suas fotografias). A partilha deste tipo de dados pode expô-lo a todo o tipo de riscos (por exemplo, roubo de identidade, assédio, conteúdo personalizado, publicidade direcionada entre outros). Por isso, é importante saber quais dados pessoais sobre si são recolhidos, de que forma são recolhidos, por quanto tempo e o que está a ser feito para proteger os seus dados pessoais. É aqui que o legislador intervém.

Os seus dados pessoais não podem ser utilizados por outros, nem podem utilizar os dados pessoais de outras pessoas. As leis de privacidade que limitam o uso de dados pessoais já existem há algum tempo. Devido ao surgimento das redes sociais, de plataformas *online* ou de aplicações móveis – todas com base no tratamento de grandes quantidades de dados pessoais – as leis tornaram-se obsoletas e deixaram de fornecer proteção suficiente às pessoas e aos seus dados pessoais. Por conseguinte, estas leis nacionais foram substituídas pelo *Regulamento Geral de Proteção de Dados* (RGPD), aplicável em toda a União Europeia.

O RGPD incumbe quem está a tratar dados pessoais a cumprir regras estabelecidas, onde se incluem também escolas e professores. A privacidade e a proteção de dados são direitos fundamentais

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia
Cofinanciado pelo Programa Erasmus+ da União Europeia

para todos. É importante que os jovens conheçam o RGPD e estejam conscientes dos seus direitos e obrigações a este respeito. Uma vez que os professores são muitas vezes um primeiro ponto de contacto para os alunos, estão numa posição privilegiada para informar e sensibilizar os alunos para o RGPD.

Número de horas: 2h

Resultados de Aprendizagem

- Sensibilizar tanto os alunos como os professores para conhecerem e familiarizarem-se com o RGPD, o seu objetivo e importância;
- Conhecimento das obrigações para com as empresas e organizações relativas ao tratamento de dados pessoais ao abrigo do RGPD;
- Conhecimento dos seus próprios direitos no tratamento dos seus dados pessoais;
- Compreensão do conceito e valor dos "dados pessoais" e do "tratamento";
- Criar uma atitude crítica com os alunos para refletir, antes de partilhar dados pessoais, sobre se a informação que pretendem partilhar não é demasiado pessoal e constitui um risco para a sua privacidade;
- O que pode ser encontrado/deve ser encontrado numa política de privacidade;
- A capacidade de utilizar as definições de privacidade da plataforma de redes sociais de forma a garantir que apenas as pessoas da sua preferência podem ver a informação do seu perfil;
- Compreensão sobre o que é publicidade direcionada;
- Conhecimentos por parte das escolas e professores sobre como utilizar legalmente as redes sociais;
- Conhecimento sobre o que fazer em caso de uso ilícito de dados pessoais;

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia

Cofinanciado pelo Programa Erasmus+ da União Europeia

Material de Apoio

1.1. O que é o RGPD?

O Regulamento Geral de Proteção de Dados entrou em vigor no dia 25 de maio de 2018 e aplica-se a qualquer organização estabelecida na UE ou estabelecida fora da UE, mas que esteja a tratar dados pessoais de pessoas na UE – incluindo escolas ou quaisquer outros estabelecimentos de ensino. Através da introdução de novas regras, o RGPD pretende devolver aos indivíduos o controlo sobre os seus dados pessoais, limitando a forma como outras pessoas e organizações podem utilizar os seus dados pessoais.

O RGPD protege os seus dados pessoais a partir do momento em que partilha estes dados com outros. Terceiros não estão simplesmente autorizados a partilhar, guardar, copiar, link... estes dados. O RGPD estabelece regras bem definidas para que as empresas, organizações e governos utilizem dados pessoais de indivíduos: o tratamento deve ser feito de forma legal, justa e transparente. Além disso, o RGPD estabelece uma série de direitos para ajudar as pessoas a manterem-se no controlo sobre os seus dados pessoais.

Uma vez que a partilha de informações pessoais em sites de redes sociais, ou a troca de dados pessoais para acesso a *apps* e outros serviços baseados na web é comum nos dias de hoje, este módulo irá focar-se no RGPD e na proteção de dados à luz desses serviços.

1.2. O que são dados pessoais?

1.2.1. Em geral

Os dados pessoais são qualquer tipo de informação que revele algo sobre si pessoalmente.

Por exemplo, nome, número de identificação, data de nascimento, morada, dados de localização, fotos ou vídeos de uma pessoa, religião, endereço IP, histórico de navegação, marcas, comportamento, perfis de redes sociais (incluindo os gostos, partilhas e amigos) etc.

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia
Cofinanciado pelo Programa Erasmus+ da União Europeia

Isto deve ser interpretado de forma muito ampla: se for possível identificar um indivíduo direta ou indiretamente a partir da informação em causa, então essas informações são dados pessoais.

- Identificação direta:

A informação permite identificar por si só a pessoa com quem esta informação se relaciona.

Por exemplo, nome, número de telefone, número de identificação, morada, endereço de e-mail, dados de localização, gravações de voz, etc.

- Identificação indireta:

A informação, como tal, não é suficiente para identificar uma pessoa, mas tendo em conta informações adicionais – que já estão disponíveis ou que precisam de ser obtidas de outra fonte – permite identificar a pessoa em causa.

Por exemplo, as matrículas podem ser consideradas dados pessoais, independentemente do facto do próprio não ter acesso a bases de dados que associam matrículas aos proprietários de automóveis. O facto de outras pessoas poderem fazer esta ligação é suficiente para qualificar esta informação como dados pessoais. O mesmo raciocínio aplica-se a informações recolhidas por *cookies*, IDs digitais e endereços MAC e IP (que são exclusivos de um dispositivo).

Uma única informação (por exemplo, cor do cabelo, ocupação, carro...) pode não ser capaz de identificar uma pessoa singular como tal, mas esta pode ser diferente quando estes dados são combinados com outros dados. As empresas que recolhem vários tipos de dados sobre pessoas (por exemplo, redes sociais) devem ter isso em conta.

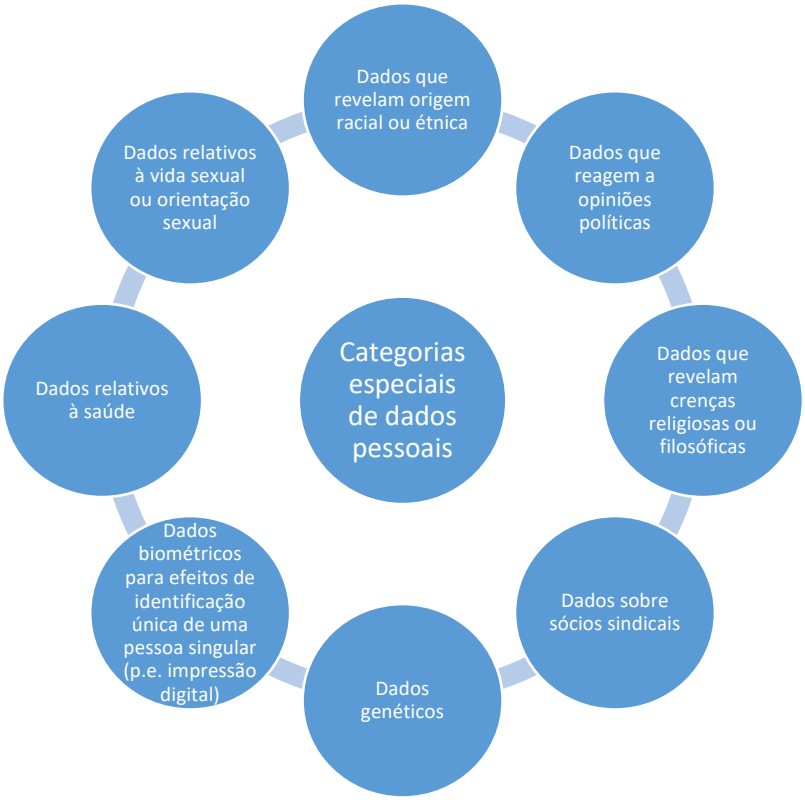
Dados pessoais
Informações relativas a uma pessoa singular. Não se refere às informações sobre empresas e outras organizações, pessoas falecidas, animais de estimação, objetos etc.
O formato é irrelevante: texto, imagem, vídeo, som etc.
As informações permitem identificar uma única pessoa, direta ou indiretamente (tendo em conta informações adicionais)

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia

Cofinanciado pelo Programa Erasmus+ da União Europeia

1.2.2. Categorias especiais de dados pessoais

O RGPD distingue entre dados pessoais "regulares" e categorias especiais de dados. Devido à natureza sensível deste último e ao elevado potencial de afetar negativamente a privacidade de alguém e outros direitos e liberdades fundamentais (por exemplo, o direito de não ser discriminado) quando são utilizados, este tipo de dados pessoais é, em princípio, proibido de ser tratado.



1.2.3. Porque é que os dados pessoais são valiosos?

Os dados pessoais são muitas vezes chamados de "o petróleo da Internet" e a nova moeda do mundo digital de hoje. Por outras palavras, os dados pessoais são considerados extremamente valiosos. Muitas empresas oferecem os seus serviços online gratuitamente, enquanto ganham o seu dinheiro com a publicidade. A publicidade que beneficia predominantemente do tratamento de dados pessoais.

Quando se está *online*, deixa-se pegadas digitais. O estado da tecnologia atual permite que as empresas utilizem e armazenem os dados pessoais que geram na compra de determinados bens ou serviços, ou apenas procurando determinadas informações (o nome, interesses pessoais, os seus desejos, o estilo pessoal, etc.). Vários cliques e gostos nas redes sociais (p.e., Facebook) são

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia
Cofinanciado pelo Programa Erasmus+ da União Europeia

suficientes para as empresas realizarem uma análise para determinar as suas preferências exatas. Ao combinar toda esta informação de diferentes fontes, as empresas são capazes de criar uma imagem clara de si. É aqui que observa o valor dos dados pessoais, se uma empresa identifica claramente o que procura ou o que lhe interessa, pode enviar-lhe anúncios especificamente para estes produtos ou serviços. *(Mais sobre este tema abaixo em **4. Publicidade direcionada**)*

Os dados pessoais não são apenas interessantes para as empresas, mas também para os *hackers*! Nos últimos anos, várias grandes empresas foram notícia à luz de grandes escândalos de *hacking*, no caso de terem sido roubados dados pessoais dos seus clientes (p.e., Cambridge Analytica, Facebook, Mastercard).

Por último, os dados pessoais também fornecem informações interessantes para as autoridades públicas, uma vez que lhes permitem obter novas informações sobre indivíduos ou grupos de indivíduos.

Uma utilização descontrolada de dados pessoais, no entanto, poderia colocar empresas privadas, *hackers* e autoridades públicas numa posição de poder.

1.3. O que é processamento de dados?

As regras do RGPD aplicam-se apenas ao tratamento de dados pessoais.

Processamento consiste qualquer operação ou conjunto de operações que seja realizada sobre dados pessoais ou em conjuntos com dados pessoais, seja ou não automatizado. Por exemplo, recolher, gravar, organizar (por exemplo, fazer uma lista de endereços de correio eletrónico), estruturar, armazenar, adaptar ou alterar, recuperar, consultar, utilizar, divulgar por transmissão, divulgar ou disponibilizar ou de outra forma disponibilizar uma mensagem ou imagem na página de Facebook de uma organização), alinhar ou combinar, restringir, apagar ou destruir dados pessoais.

Se uma das ações acima referidas for realizada nos seus dados pessoais, o RGPD aplica-se.

No entanto, é importante notar que o processamento de atividades puramente pessoais ou domésticas não se enquadra no RGPD (por exemplo, pais que captam fotografias dos filhos ou de colegas da escola num evento escolar para manter num álbum de fotografias familiar).

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia
Cofinanciado pelo Programa Erasmus+ da União Europeia

1.4. Quem tem de seguir as regras do RGPD?

O RGPD aplica-se a uma empresa ou entidade (ou seja, pessoa singular ou jurídica, autoridade pública, agência ou outro organismo), independentemente da sua dimensão, setor, número de trabalhadores ou volume de negócios, que:

- trata os dados pessoais no âmbito das atividades de um dos seus balcões estabelecidos na UE (independentemente do local onde os dados são tratados);
- é estabelecido fora da UE e está a tratar dados pessoais à luz da oferta de bens/serviços a particulares na UE, ou à luz do controlo do comportamento das pessoas na UE.

Tais empresas ou entidades são vistas como os controladores dos seus dados pessoais e precisam de garantir que o RGPD é respeitado.

As regras

2.1. Os princípios do RGPD

Qualquer empresa ou entidade que processa dados pessoais terá de seguir determinadas regras.

2.1.1. Legalidade, equidade e transparência

(a) Legalidade

Quando uma empresa ou organização quer processar os seus dados pessoais, antes de o fazer, tem de se certificar de que o seu tratamento pode basear-se numa base de justificação – uma **base legal** – no âmbito do RGPD. Uma base jurídica é uma razão para o processamento determinado e aceite pelo RGPD (ver artigo 6.º do RGPD).

As bases mais relevantes à luz das redes sociais são: o tratamento de dados pessoais é necessário **para realizar um contrato**; a empresa ou organização obteve o seu **consentimento**; ou a empresa ou organização tem (a) **interesse legítimo** no tratamento dos seus dados pessoais.

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia
Cofinanciado pelo Programa Erasmus+ da União Europeia

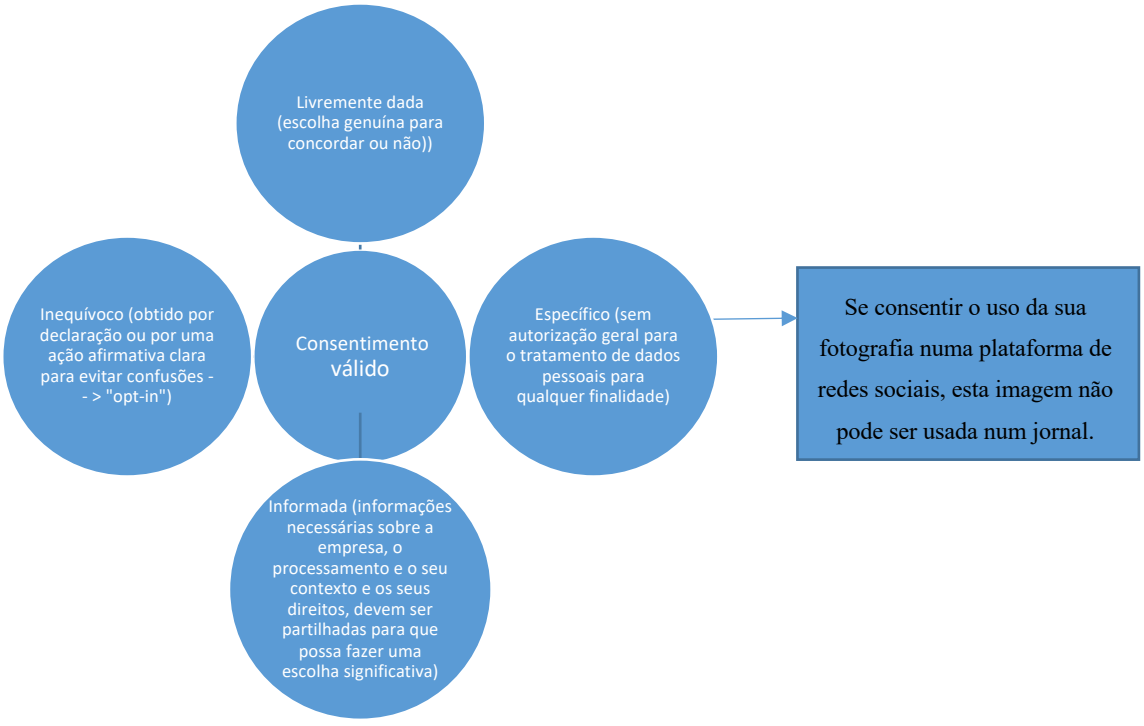
Necessidade contratual

Quando uma empresa ou organização precisa de processar dados pessoais para cumprir obrigações contratuais, ou para realizar pedidos pré-contratuais, pode contar com a base legal "contrato". Algumas obrigações contratuais simplesmente não podem ser executadas sem recolher e tratar determinados dados pessoais. O tratamento que seja útil, mas não objetivamente necessário, para a realização do serviço contratual ou para a realização de medidas pré-contratuais relevantes não são abrangidos por esta base legal.

Exemplo: o Twitter processa os seus dados pessoais – como, por exemplo, o nome e o endereço de e-mail – de forma a criar a sua conta, para efeitos de autenticação e para permitir a criação de conteúdos.

Consentimento

O consentimento tem um significado particular no RGPD e para ser válido, tem de ser:



Deve poder retirar o seu consentimento a qualquer momento. As informações sobre como fazê-lo devem ser fornecidas no momento em que lhe é solicitado o consentimento para uma determinada atividade de processamento. A forma de retirar o consentimento deve ser igualmente fácil como dar

consentimento e não deve levar a quaisquer consequências negativas para si (por exemplo, uma taxa ou níveis de serviço mais baixos).

Exemplo: o Facebook tem uma funcionalidade de reconhecimento facial que permite ao site da rede social reconhecê-lo em fotografias ou vídeos na sua plataforma. O uso de tal funcionalidade implica o tratamento de dados pessoais, nomeadamente fotografias ou vídeos de si. Para ativar esta funcionalidade, o Facebook pede o seu consentimento.

O mesmo se aplica à função "histórico de localização" que o Facebook oferece. Quando concorda com o uso desta função, os seus dados de localização estão a ser processados de forma a explorar o que se passa à sua volta, para lhe mostrar anúncios relevantes ou para procurar amigos na área.

Exemplo: o Twitter processa informações que recolhem de si, outras atividades suas *online* e dados dos seus parceiros, de forma a mostrar publicidade personalizada dentro e fora do Twitter, com base no seu consentimento.

Uma empresa ou organização só pode processar os dados pessoais de uma criança com base no consentimento **explícito do seu pai ou tutor** até uma determinada idade. O limiar de idade para obter o consentimento das próprias crianças ou jovens diretamente pode variar de 13 a 16 anos dependendo do país da UE (verificar a idade limite com a autoridade nacional de proteção de dados).

Interesse legítimo

Os interesses legítimos para os quais é **necessário** processar dados pessoais, podem ser os seus próprios interesses ou os interesses de terceiros (por exemplo, interesses comerciais, interesses individuais ou benefícios sociais mais amplos). Este interesse tem de ser especificado na política de privacidade.

Assim, as empresas ou organizações devem processar os seus dados de uma forma que razoavelmente esperaria, sem causar danos injustificados. Se não for esse o caso, os seus interesses estão provavelmente a prevalecer os da empresa ou da organização, o que significa que não estão autorizados a processar os seus dados pessoais (nesta base legal), a menos que haja uma justificação convincente para o tratamento.

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia

Cofinanciado pelo Programa Erasmus+ da União Europeia

Exemplo: O Twitter recolhe informações sobre a sua conta – tais como interesses, idade e género – de forma a disponibilizar funcionalidades como sugestões de contas, publicidade, recomendações, ranking de linha do tempo, etc.

Exemplo: o YouTube (Google) processa os seus dados pessoais pelos seus interesses legítimos e pelos de terceiros, aplicando ao mesmo tempo salvaguardas adequadas que protegem a sua privacidade. Este é, por exemplo, o caso da personalização dos seus serviços para lhe proporcionar uma melhor experiência de utilizador, marketing para informar os utilizadores sobre os seus serviços, mas também para apresentar publicidade, que mantém muitos dos seus serviços gratuitos. (Quando os anúncios são personalizados, pedem consentimento.)

Categorias especiais de dados

Importante a acrescentar é que para categorias especiais de dados pessoais, existem 10 exceções à proibição geral de processar esses dados (ver artigo 9.º do RGPD). Se uma destas condições for satisfeita, as categorias especiais de dados podem ser processadas legalmente. A exceção mais importante à luz das redes sociais é quando há **consentimento explícito** da pessoa que tem dados pessoais.

Estas exceções formam uma camada adicional de condições em cima das regras habituais. Na prática, isto significa que, quando se pretende processar categorias especiais de dados, tem de haver uma base legal (art. 6.º) e deve ser aplicável uma exceção (art. 9.º).

Exemplo: O Google pede o seu consentimento antes de partilhar informações pessoais fora da empresa. Digamos que faça uma reserva de restaurante através do *'Google Home'*, a sua permissão será pedida antes de partilhar dados pessoais (por exemplo, nome, número de telefone) com o restaurante. Quando se trata de informações pessoais sensíveis (por exemplo, alergias), compromete-se a pedir consentimento explícito.

(b) Justiça

A empresa ou entidade que trata os seus dados pessoais deve fazê-lo de forma justa, o que significa, que não cause efeitos negativos pessoais injustificáveis ou que esteja a enganar deliberadamente.

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia

Cofinanciado pelo Programa Erasmus+ da União Europeia

(c) Transparência

Trata-se de um princípio muito importante, que está ligado à equidade! Desde o início, as empresas ou organizações devem ser claras, abertas e honestas sobre como irão utilizar os seus dados pessoais. Isto requer que a informação seja fornecida numa linguagem facilmente acessível e compreensível. É aqui que entra a política de privacidade. De acordo com o RGPD, devem ser evitadas políticas de privacidade longas e complicadas.

Uma política de privacidade

A política de privacidade pretende dar informações sobre como os seus dados pessoais estão a ser recolhidos, utilizados e protegidos pelas redes sociais (ou por qualquer outro website). Todas as políticas de privacidade devem conter obrigatoriamente um grande número de menções:

- nome e dados de contacto da empresa/organização
- detalhes de contacto do oficial de proteção de dados
- quais as finalidades para o processamento/tratamento de dados pessoais e em que base legal dependem
- o interesse legítimo para o processamento (se aplicável)
- as (categorias de) dados pessoais obtidos (se não obtidos diretamente de si)
- os (categorias de) destinatários dos dados pessoais (os dados pessoais serão partilhados com terceiros?)
- os dados relativos às transferências dos dados pessoais para países terceiros ou organizações internacionais (se aplicável)
- quanto tempo os dados são mantidos (período de retenção)
- os direitos que podem ser exercidos por si (por exemplo, direito de acesso, direito de esquecimento, direito de retificação, etc.)
- o direito de retirar o consentimento (se aplicável)
- o direito de apresentar reclamações com a autoridade de proteção de dados
- a origem dos dados pessoais (se os dados pessoais não forem obtidos diretamente de si)
- os detalhes da existência de tomadas de decisão automatizadas, incluindo perfis (se aplicável).

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia

Cofinanciado pelo Programa Erasmus+ da União Europeia

2.1.2. Limitação de propósito

O princípio da limitação dos objetivos significa que as empresas ou organizações devem definir claramente um propósito específico para cada uma das suas atividades de transformação, antes de iniciar. Esta exigência visa proporcionar transparência, previsibilidade e controlo do utilizador. Qualquer tratamento de dados pessoais deve ser feito para uma finalidade específica bem definida ou para fins adicionais que sejam compatíveis com o original. O tratamento de dados pessoais para fins indefinidos e/ou ilimitados é, portanto, ilegal.

Todas as novas finalidades para o tratamento de dados pessoais que não sejam compatíveis com a finalidade original devem ter uma base legal própria e não podem basear-se no facto de os dados terem sido inicialmente adquiridos ou tratados para outro fim legítimo.

Exemplo: Se conceder consentimento ao Facebook para utilizar a funcionalidade de reconhecimento facial para detetar imagens e vídeos na plataforma, não significa que o Facebook possa utilizar estes dados com o propósito de fornecer-lhe anúncios direcionados com base nestes dados pessoais. Necessitará de uma base legal distinta (por exemplo, consentimento) para tal.

2.1.3. Minimização de dados

As empresas e organizações só podem processar dados pessoais de que realmente precisam para atingir o seu propósito especificado, e não mais do que isso. Isto significa que terão regularmente de rever os dados que armazenam para apagar qualquer coisa de que não precisem.

2.1.4. Precisão

As empresas e organizações necessitam de tomar medidas razoáveis para garantir que os dados pessoais que possuem são corretos e não enganadores. Isto implica que terão de manter os dados pessoais atualizados, corrigindo ou eliminando os dados, sempre que necessário.

2.1.5. Limitação de armazenamento

Os dados pessoais não podem ser guardados para sempre. As empresas e organizações devem eliminar ou anonimizar os dados pessoais logo que deixem de precisar dos mesmos para atingir os fins(s) para os quais os dados foram recolhidos. As empresas e organizações precisam de pensar antecipadamente quanto tempo querem manter os seus dados pessoais e se este período é justificável, o que dependerá das suas finalidades de processamento. As informações sobre esta matéria devem ser implicadas nas políticas de privacidade.

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia

Cofinanciado pelo Programa Erasmus+ da União Europeia

2.1.6. Integridade e confidencialidade (segurança de dados)

A proteção de dados pessoais contra o tratamento não autorizado ou ilícito, perda acidental, destruição ou dano é o núcleo deste princípio de integridade e confidencialidade (segurança de dados). O princípio da segurança dos dados visa evitar efeitos negativos para si, obrigando à implementação de medidas técnicas (por exemplo, encriptação, pseudónimo) e/ou medidas organizacionais (por exemplo, garantir que os dados pessoais não estão disponíveis para todos dentro de uma organização, mas apenas para os que têm de tratar os dados).

2.1.7. Responsabilidade

O princípio da prestação de contas exige que as empresas ou organizações assumam a responsabilidade pelo que fazem com os seus dados pessoais e pela forma como cumprem com o RGPD. Perante isto, têm de implementar medidas e registos que lhes permitam demonstrar o seu cumprimento quando lhes é pedido que o façam.

Os direitos

Na sociedade digital em que vivemos é importante conhecer os seus direitos do ponto de vista da proteção de dados.

3.1. O direito de ser informado

As empresas e organizações devem informá-lo sobre a recolha e utilização dos seus dados pessoais. Isto está relacionado com o princípio da transparência subjacente ao RGPD. Ver 2.1.1. (c) Sobre as informações que devem ser dadas.

As informações devem ser comunicadas:

- no momento em que recolhe os dados pessoais
- até um mês após a obtenção dos dados, caso tenham recebido os dados pessoais de outra pessoa

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia
Cofinanciado pelo Programa Erasmus+ da União Europeia

A informação deve ser concisa, transparente, inteligível, facilmente acessível, e deve utilizar uma linguagem clara e simples. Estas informações são fornecidas principalmente através de uma política de privacidade.

3.2. O direito de acesso

Cada indivíduo tem o direito de aceder aos seus dados pessoais, detidos por uma empresa ou organização. Na prática, isto significa que receberá a seguinte informação:

- Quer a empresa ou a organização esteja ou não a processar os seus dados pessoais
- Uma cópia desses dados (geralmente, gratuitamente)
- Informações adicionais: as empresas ou organizações têm de lhe fornecer as mesmas informações que são necessárias para estar numa política de privacidade (Ver 2.1.1.). c)).

O exercício deste direito ajuda-o a perceber como e por que as empresas ou organizações estão a usar os seus dados, e a verificar se estão a fazê-lo em conformidade com o RGPD.

É possível que a empresa ou organização recuse o acesso quando o pedido é manifestamente infundado (por exemplo, claramente apenas feito para denegrir a empresa) ou excessivo (por exemplo, sobrepõe-se a outros pedidos). As razões da recusa devem ser-lhe comunicadas claramente. As empresas e organizações têm um mês para responder ao pedido.

3.3. O direito ao esquecimento ("o direito a ser esquecido")

O RGPD concede-lhe o direito de ver os seus dados pessoais apagados. Este direito está associado aos princípios da minimização dos dados e da precisão dos dados, obrigando empresas e organizações a considerarem apagar os dados pessoais de um indivíduo em determinadas ocasiões. Pode exercer o seu direito ao esquecimento quando:

- os seus dados pessoais deixaram de ser necessários para a finalidade para a qual foram recolhidos pela empresa ou organização;

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia

Cofinanciado pelo Programa Erasmus+ da União Europeia

- Quando a empresa ou organização está a contar com o seu consentimento como base legal para a detenção dos dados, e pretende retirar o seu consentimento;
- Quando a empresa ou organização está a contar com interesses legítimos como base legal para o tratamento, pode opor-se ao tratamento dos seus dados, e se não houver interesse legítimo para continuar este tratamento os seus dados serão apagados;
- Quando a empresa ou organização está a processar os dados pessoais para lhe enviar marketing direto e se opõe a esse processamento;
- Quando os seus dados pessoais foram tratados ilegalmente (= sem depender corretamente de uma base legal válida);
- Quando existe uma obrigação legal de obrigar a eliminação dos seus dados pessoais;
- Quando os seus dados pessoais foram recolhidos de si quando era criança, com o objetivo de oferecer serviços online.

Dá-se particular ênfase ao direito ao esquecimento se o pedido se referir aos dados recolhidos junto das crianças. Se o consentimento para o tratamento de dados pessoais foi originalmente dado quando era criança (desconhecendo totalmente os riscos), pode ser muito importante poder retirar o seu consentimento e remover os dados pessoais *(provavelmente todos os alunos podem pensar em algo que publicaram online no passado, com o qual já não concordam ou acham embaraçoso hoje).*

A sociedade ou organização não é obrigada a conceder sempre (totalmente) o seu pedido, uma vez que, em alguns casos, o direito ao esquecimento não se aplica (por exemplo, se o processamento for necessário para cumprir a lei ou quando o tratamento ocorre para fins de registo para o interesse público ou para investigação científica ou histórica em casos onde o esquecimento conduza a graves prejuízos à investigação). Uma empresa ou organização também pode recusar o exercício do seu direito de esquecimento quando o pedido é manifestamente infundado ou excessivo (ver 3.2).

Uma observação a fazer-se é a dificuldade em garantir o direito ao esquecimento, pois será muito difícil (talvez mesmo impossível) apagar completamente os seus dados pessoais da Internet. Isto porque os dados são muitas vezes (não)legalmente partilhados por empresas e organizações que depois partilham novamente estes dados com outras partes e assim por diante.

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia

Cofinanciado pelo Programa Erasmus+ da União Europeia

3.4. O direito à retificação dos dados

Com base no direito à retificação dos dados, pode corrigir-se quaisquer erros nos seus dados pessoais detidos por empresas ou organizações: os dados pessoais imprecisos podem ser retificados e os dados incompletos podem ser preenchidos. Este direito está claramente associado ao princípio da exatidão que as empresas e as organizações devem ter em conta.

Mais uma vez, as empresas e organizações nem sempre têm de cumprir o seu pedido. Se as empresas admitem que os seus dados pessoais são precisos, é necessário indicar explicitamente a razão da sua decisão. Outra razão para não conceder (totalmente) o seu pedido de retificação pode ser quando o seu pedido é manifestamente infundado ou excessivo (ver 3.2).

3.5. O direito à restrição do processamento

Este direito é uma alternativa a solicitar o direito ao esquecimento de dados pessoais, que permite exigir que a empresa ou organização deixe de processar (alguns dos) seus dados pessoais apenas por um período tempo. O direito implica que a empresa ou organização só pode armazenar os seus dados pessoais, sem continuar a usá-los.

As empresas e organizações têm também a capacidade de recusar o pedido de restrição do processamento, sob a obrigação de fornecer uma explicação para tal. Uma das razões da recusa pode ser, mais uma vez, o facto de o pedido ser manifestamente infundado ou excessivo (ver ponto 3.2).

3.6. O direito à portabilidade dos dados

Este direito confere-lhe a capacidade de obter e mover os seus dados pessoais – que forneceu à empresa ou organização – para outro lado. Na prática, isto significa que pode facilmente mover, copiar ou transferir os seus dados pessoais de um ambiente para outro, de forma segura e comumente utilizada, ou pode pedir à empresa ou organização para o fazer.

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia
Cofinanciado pelo Programa Erasmus+ da União Europeia

Este direito só se aplica quando a empresa ou organização se baseia em "consentimento" ou "necessidade contratual" como base legal para o tratamento destes dados pessoais, ou quando são tratados por meios automatizados (isto é, através de programas e ferramentas de TI).

As empresas e organizações têm também a capacidade de recusar o pedido de restrição do processamento, sob a obrigação de fornecer uma explicação para tal. Uma das razões da recusa pode ser, mais uma vez, o facto de o pedido ser manifestamente infundado ou excessivo (ver ponto 3.2).

3.7. O direito de oposição

O direito de oposição não é um direito geral. Pode invocar o seu direito de se opor ao tratamento dos seus dados pessoais com base na sua situação particular e aos dados tratados com o objetivo de disponibilizar marketing direto. Isto permite-lhe parar ou impedir que empresas e organizações processem (parte) dos seus dados pessoais.

O direito de se opor ao processamento para fins de marketing direto é um direito absoluto, o que significa que as empresas e organizações têm sempre de conceder este pedido. Quando o direito de objeção é exercido por outra razão, as empresas e organizações podem decidir continuar a processar os seus dados pessoais se puderem provar que há uma razão convincente para o fazerem. As empresas e organizações têm também a capacidade de recusar o pedido de oposição do processamento, sob a obrigação de fornecer uma explicação para tal. Uma das razões da recusa pode ser, mais uma vez, o facto de o pedido ser manifestamente infundado ou excessivo (ver ponto 3.2).

3.8. Os direitos relativos à tomada de decisões automatizadas, incluindo a perfis

Perfis referem-se à avaliação dos seus aspetos pessoais para fazer previsões sobre si.

Exemplo: Um site de redes sociais avalia certas informações sobre si (como a idade, sexo, altura) e com base nisso classifica-o num determinado grupo, por razões de recomendação de conteúdo ou publicidade.

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia

Cofinanciado pelo Programa Erasmus+ da União Europeia

A tomada de decisão baseada apenas em meios automatizados refere-se à situação em que a própria tecnologia toma decisões sobre si, sem qualquer envolvimento humano.

Com base no RGPD, tem o direito de não estar sujeito a uma decisão baseada em meios exclusivamente automatizados, se a decisão resultar em efeitos legais (ou seja, os seus direitos legais são impactados) sobre si ou o afeta significativamente de forma semelhante (isto é, influencia as suas circunstâncias, comportamentos ou escolhas). Uma vez que tais decisões provavelmente têm um impacto significativo nas vidas de cada indivíduo (podem relacionar-se, por exemplo, com a solvabilidade, o recrutamento eletrónico, o desempenho no trabalho) é necessária uma proteção especial.

Exemplo: As companhias de seguros que analisam publicações nas redes sociais de clientes (potenciais) utilizando um algoritmo que procura determinadas palavras e frases que indiquem um comportamento cauteloso ou que sejam saudáveis para lhe atribuir um nível de risco e decidir o valor do prémio de seguro.

3.9. Aspeto Prático

No exercício dos seus direitos, as empresas e organizações têm um mês para responder aos seus pedidos e fornecer informações para apoiar a sua decisão. Os pedidos devem ser apresentados com a empresa ou organização, verbalmente ou por escrito (geralmente através de um e-mail ou de uma secção específica do site). Deve ser tão fácil exercer estes direitos como o é fornecer os seus dados pessoais em primeiro lugar.

Publicidade direcionada/comportamental

No passado, as empresas investiam principalmente na publicidade televisiva e radiofónica. Uma desvantagem associada a este tipo de publicidade é que todos os indivíduos são confrontados com o mesmo anúncio, seja do seu interesse ou não, o que não se torna muito eficiente. Atualmente, as redes sociais e os avanços tecnológicos permitem que as empresas optem por divulgar os seus produtos e serviços aos consumidores de uma forma direcionada: por exemplo, um anúncio de calçado de corrida

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia
Cofinanciado pelo Programa Erasmus+ da União Europeia

só é apresentado aos utilizadores das redes sociais que regularmente vão correr, e nos dias em que não está a chover. Tais anúncios direcionados podem ser encontrados no seu *feed* de notícias das redes sociais e podem ser reconhecidos por palavras como "patrocinado".

Qual dos seus dados é usado para publicidade?

1. Os dados pessoais que introduz ao criar a sua conta nas redes sociais (por exemplo, idade, onde vive, data de nascimento)

2. O que publicar na sua conta nas redes sociais, como fotografias, vídeos e comentários. Por exemplo, se publicar algo como "estou com tanta fome neste momento", é possível que receba um anúncio de uma cadeia de *fast food*;

3. Coisas que faz e procura fora da plataforma das redes sociais. Por exemplo, se visitar o site de um determinado evento, poderá receber anúncios sobre este evento ou um evento semelhante na sua conta nas redes sociais. Este último é possível através de *'cookies'*.

> Os *cookies* são pequenos ficheiros armazenados no seu computador, portátil, *smartphone* ou *tablet* para acompanhar os websites que está a visitar. Note que as empresas precisam de pedir a sua permissão antes de usar *cookies* publicitários (existem outros tipos de *cookies* também). Se não deseja ser rastreado em diferentes sites *online*, lembre-se de recusar *cookies*. A utilização de *cookies* e outras tecnologias de rastreio é regulada pelas regras de *ePrivacy*, não pelo RGPD.

Importante a acrescentar aqui é que algumas empresas de redes sociais possuem várias plataformas e, portanto, podem utilizar informações obtidas sobre si em ambas as plataformas (Facebook e Instagram, por exemplo);

4. A sua localização (em tempo real). As plataformas de redes sociais podem obter a sua localização, com base no *wifi* e no gps-tracker no seu telefone. Isto poderia resultar em receber anúncios para um determinado ginásio, se estiver geograficamente perto.

Toda a informação acima mencionada, é lembrada e interpretada por algoritmos e, claro, não por seres humanos reais. Com base nestes dados, as empresas que optam por fazer publicidade nas redes sociais podem escolher um "grupo-alvo" (por exemplo, rapazes de 16 anos na zona de Amesterdão que gostam de futebol). O anúncio certo, no momento certo e no lugar certo, pode

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia
Cofinanciado pelo Programa Erasmus+ da União Europeia

influenciar seriamente o seu comportamento, o que beneficia as empresas. Embora a publicidade personalizada nem sempre seja vista como uma coisa má, deve ser-se cauteloso. Especialmente quando existem dados sensíveis (por exemplo, raça, preferências políticas, etc.), este tipo de publicidade pode ser complicado e os seus dados pessoais podem ser mal utilizados (por exemplo, direcionar-se para si com conteúdos falsos, para alterar ou radicalizar as suas preferências políticas).

O que fazer em caso de infrações?

Alguém partilhou ilegalmente o seu perfil pessoal? Criou um perfil falso nas redes sociais? Ou talvez tenha tentado exercer um dos seus direitos protegidos sob o RGPD, mas não está satisfeito com a resposta da empresa ou da organização? Em primeiro lugar, pode solicitar à pessoa ou organização que infringiu os seus direitos de proteção de dados, para apagar ou corrigir os dados pessoais em causa (por exemplo, uma imagem, perfil falso, dados de contacto). Se nada acontecer, pode dirigir-se à plataforma de redes sociais para eliminar ou corrigir os dados pessoais. Se estes passos não forem satisfatórios, pode apresentar uma reclamação à sua autoridade nacional de proteção de dados. (Outra opção é fazer valer os seus direitos através de uma solução judicial.)

Todos os países da UE têm a sua própria autoridade de proteção de dados. Pode encontrar a lista aqui: https://edpb.europa.eu/about-edpb/board/members_en

As autoridades de proteção de dados são autoridades públicas independentes que monitorizam e supervisionam se as empresas e organizações do seu território estão a aplicar corretamente as regras de proteção de dados. Também fornecem aconselhamento especializado sobre questões de proteção de dados e lidam com queixas. As autoridades podem emitir avisos, repreensões, uma proibição temporária ou definitiva do processamento e multas (muito elevadas).

Nos sites das autoridades de proteção de dados pode encontrar forma de apresentar uma reclamação, através de telefone, e-mail ou através de um formulário de contacto disponível no website.

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia

Cofinanciado pelo Programa Erasmus+ da União Europeia

Recursos

- https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf (Manual Geral sobre proteção de dados)
- https://www.youtube.com/watch?v=XVBHishpew8 (vídeo do YouTube: o que é o RGPD?)
- https://www.youtube.com/watch?v=3fuirT_PwDI (vídeo do YouTube: RGPD explicado)
- https://www.youtube.com/watch?v=PVaVIOJniSQ&t=6s (vídeo do YouTube: os meus dados, a minha escolha)
- https://cris.vub.be/files/27962258/arcades_teaching_handbook_final_EN.pdf (Free university of Brussels (VUB): The European Handbook for Teaching Privacy and Data Protection at schools)
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf (UK GOV: Proteção de dados: um kit de ferramentas para escolas)
- https://www.gdpr.school/free-resources/ (fontes úteis do RGPD para as escolas)
- https://edpb.europa.eu/about-edpb/board/members_en (Lista das autoridades nacionais de proteção de dados)
- https://ico.org.uk/ (Autoridade de Proteção de Dados do Reino Unido do Site uk muita informação!)
- https://en.mediawijs.be/poster-step-by-step-how-should-i-protect-my-privacy-on-social-media (website mediawijs "Como proteger a minha privacidade nas redes sociais?")
- https://www.youtube.com/results?search_query=internet+safety+tips+for+teens (vídeo do YouTube com dicas de segurança na Internet para jovens)
- https://www.youtube.com/watch?v=yrln8nyVBLU (YouTube: Safe Web Surfing: Top Tips for Kids and Teens Online)
- https://mediawijs.be/nieuws/slag-gdpr-jouw-klas (Mediawijs sobre a utilização do RGPD como parte das suas aulas em holandês)→

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia

Cofinanciado pelo Programa Erasmus+ da União Europeia

Fontes extra

- https://d1afx9quaogywf.cloudfront.net/sites/default/files/Resources/School%20College%20Personal%20Data%20Advice%20and%20Guidance.pdf (Informação para as escolas - RGPD)
- https://www.youtube.com/watch?v=xtLR0Ey5-vo&t=76s (vídeo do YouTube com informação para as escolas - RGPD)
- https://www.youtube.com/watch?v=SpjpxspJNew&t=7s (vídeo do YouTube com informação para as escolas - RGPD)

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia

Cofinanciado pelo Programa Erasmus+ da União Europeia

Snacks de Aprendizagem

Aumentar a consciencialização do RGPD é crucial

É essencial que, na era digital, os alunos e professores e todos os outros quadros de estabelecimentos de ensino estejam conscientes do RGPD e da legislação em matéria de proteção de dados em geral. A quantidade de dados pessoais que circulam *online* é enorme e continuará a crescer, pelo que todos precisam de aprender a lidar com os seus dados pessoais e com os seus dados pessoais de forma responsável.

Porque é que o RGPD é importante? O valor dos dados pessoais!

Atualmente, todos nós produzimos enormes quantidades de dados pessoais diariamente, especialmente *online* (por exemplo, publicando fotografias, vídeos ou atualizações de estado nas redes sociais, mas também através de compras *online*, leitura de um jornal *online* ou jogos *online* – tudo isto gera dados que podem estar associados a si). Algumas empresas – além de recolher e processar dados pessoais para prestar um serviço específico – têm como objetivo recolher o máximo de dados possível para o direcionar eficazmente com publicidade. Os dados pessoais têm, assim, um importante valor económico para empresas e organizações. Além disso, as autoridades públicas estão interessadas em dados pessoais, uma vez que lhes podem fornecer novos conhecimentos. Um uso descontrolado de dados pessoais poderia, consequentemente, colocar empresas privadas, hackers e autoridades públicas numa posição de poder e colocá-lo numa situação indesejável.

Pense antes de partilhar

Pense sempre cuidadosamente sobre os dados pessoais que partilha, com quem e de que forma se quer expor nas publicações das redes sociais (texto, imagens, vídeos). É importante pensar a longo prazo porque a informação está acessível para sempre, uma vez que não é fácil apagar informação da Internet. Cuide das suas definições de privacidade para que as pessoas que não conhece não possam visualizar (grande parte) dos seus dados pessoais. Mesmo exercendo o direito de apagar, provavelmente não será capaz de eliminar todos os seus vestígios digitais.

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia
Cofinanciado pelo Programa Erasmus+ da União Europeia

Posso dar o meu próprio consentimento para o tratamento dos meus dados pessoais?

Existe uma idade legal para as crianças poderem consentir (ou não) o tratamento de dados pessoais por fornecedores de serviços online. Este limite de idade pode variar entre os 13 e os 16 anos em cada Estado-Membro da UE.

Transparência / informação é fundamental

Um dos principais princípios subjacentes ao RGPD é o princípio da transparência: as empresas e organizações têm de ser claras quanto ao facto de processarem os seus dados pessoais, quais os dados pessoais que processam, por que razões e como o fazem, por quanto tempo, etc. Este princípio traduz-se no direito de as pessoas serem informadas, o que lhe deve permitir fazer escolhas informadas sobre os seus dados pessoais. Desta forma, o RGPD pretende colocar os indivíduos no comando do que acontece aos seus dados pessoais.

Como identificar o que uma empresa ou organização está a fazer com os meus dados pessoais?

A primeira coisa que deve fazer quando pretender descobrir o que as empresas ou organizações estão a fazer com os seus dados pessoais é verificar a política de privacidade. Esta política implica uma série de elementos obrigatórios. Se faltar alguma coisa ou algo não for claro, poderá tentar contactar a empresa ou as organizações para mais esclarecimentos.

O que fazer quando alguém está a usar mal os meus dados nas redes sociais?

Opção 1: contacte a pessoa/empresa/organização que está a utilizar os seus dados pessoais de forma ilícita e peça-lhes que apague ou corrija os seus dados pessoais.

Opção 2: entre em contato com a plataforma de redes sociais para solicitar a eliminação ou correção dos seus dados pessoais.

Opção 3: apresente uma reclamação à sua autoridade nacional de proteção de dados (ver o seu website).

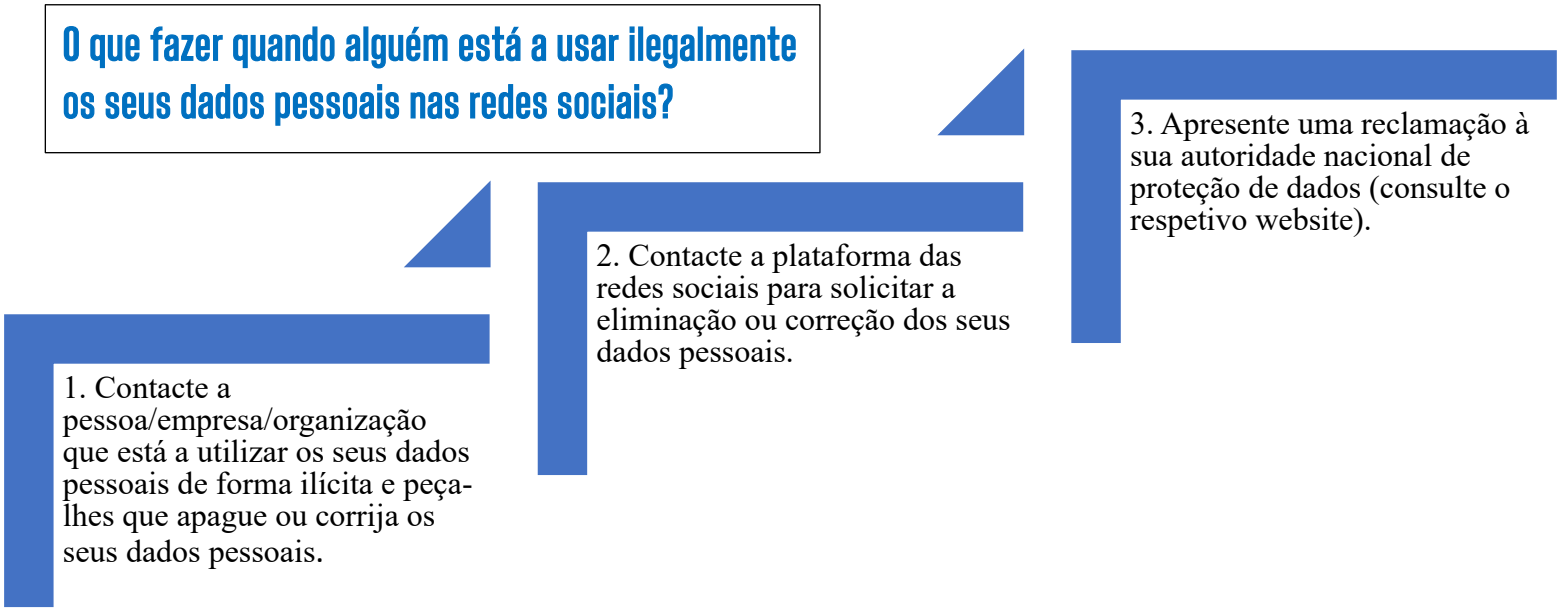
(Opção 4: ir ao tribunal)

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia

Cofinanciado pelo Programa Erasmus+ da União Europeia

Infográficos

Veja no material de ensino + a infografia abaixo:



Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia

Cofinanciado pelo Programa Erasmus+ da União Europeia

Propostas de atividade com os alunos

- Comece a aula perguntando se os alunos sabem o que são dados pessoais e por que acham que é importante proteger os dados pessoais.
- Deixe que os alunos verifiquem as suas definições de privacidade no Facebook (ou noutro site de redes sociais): quem é capaz de ver que tipo de informação sobre si? Depois pode promova uma discussão entre colegas que partilham porque querem que as suas configurações sejam de uma determinada forma ou se gostariam de mudar as suas configurações.
- Os alunos procurem o limiar de idade para dar o seu consentimento ao abrigo do RGPD no seu país. Isto pode ser feito através do site da autoridade nacional de proteção de dados do seu país. Vê: https://edpb.europa.eu/about-edpb/board/members_en.
- Depois de receberem a informação sobre o princípio da transparência, um dos princípios centrais do RGPD, e o papel das políticas de privacidade a este respeito, os estudantes poderiam inspecionar a política de privacidade de um site nas redes sociais para ver se toda a informação obrigatória está presente. Depois, promova o debate.
- Depois de explicarem aos alunos que têm certos direitos em relação ao tratamento dos seus dados pessoais, apresente um "pedido de acesso" ao Facebook (ou outra plataforma de redes sociais), para ver quais os dados pessoais que o Facebook detém sobre os mesmos. Ver em: https://www.facebook.com/help/contact/2032834846972583.

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia
Cofinanciado pelo Programa Erasmus+ da União Europeia

Avaliação da atividade

Pode avaliar facilmente se os alunos compreenderam a informação sobre o RGPD aplicando questionários com perguntas curtas cuja resposta é verdadeira ou falsa, como nos exemplos abaixo:

1. Uma imagem com uma pessoa de costas, completamente irreconhecível, não é considerada dados pessoais ao abrigo do RGPD. (**Falso**: a imagem como tal, sem qualquer outra informação, não faz parte do conjunto dos dados pessoais, mas a partir do momento em que alguém adiciona o nome, endereço ou número de telefone desta pessoa à imagem, a imagem torna-se uma dado pessoal uma vez que está ligada a uma pessoa específica).

2. A maioria dos websites e aplicações que eu utilizo, processam os meus dados pessoais. (**Verdade**: a finalidade do tratamento de dados pessoais pode diferir. Por exemplo, normalmente o processamento de um nome e palavra-passe é necessário para efeitos de autenticação. Muitas vezes, dados pessoais como sexo, idade, interesses são tratados para fins de marketing).

3. O RGPD não trata todos os dados pessoais da mesma forma. (**Verdade**: a principal clivagem feita no RGPD é entre dados pessoais "regulares" e categorias especiais de dados pessoais (por exemplo, saúde, orientação sexual, religião). Estes últimos devem ser tratados com mais cuidado devido à sua natureza sensível (a partilha desses dados implica um maior risco, uma vez que poderiam conduzir a consequências indesejáveis, como a discriminação, a exclusão, etc.) e é por isso que, em princípio, é proibido o tratamento desses dados. (Os dados relativos à infração penal e os dados das crianças estão igualmente sujeitos a um regime especial)

4. Uma escola publica *online* os relatórios de cada aluno para permitir que os pais comparem os resultados do seu filho com os dos seus colegas. Isto é permitido porque é do interesse da criança. (**Falso:** Para cada processamento que está a decorrer, uma empresa ou outra organização – incluindo uma escola – tem de se basear numa base legal válida determinada no RGPD. Uma vez que isso poderia afetar negativamente as crianças, a única forma de uma escola poder fazê-lo é quando obtém o consentimento de cada criança e/ou dos pais.

5. No tratamento de dados pessoais, é sempre necessário o consentimento da pessoa que tem os dados em causa. (**Falso**: o consentimento é apenas um de uma lista limitada de bases legais em que empresas e outras organizações podem confiar para justificar as suas atividades de processamento (ver artigos 6.º e 9.º RGPD). Portanto, o consentimento nem sempre é necessário. Para cada atividade

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia
Cofinanciado pelo Programa Erasmus+ da União Europeia

de processamento deve sempre escolher uma base legal para o processamento, dependendo da base mais adequada para a situação.

6. No passado, consentiu que a sua fotografia fosse publicada na página de uma empresa nas redes sociais e já não gosta da fotografia. Infelizmente, porque deu o seu consentimento para publicar a foto no passado, não há nada que possa fazer. (**Falso**: pode sempre retirar o seu consentimento, o que significa que a empresa terá de apagar a imagem)

7. Alguns alunos foram fotografados nas aulas e deram consentimento para que a fotografia fosse usada no âmbito escolar. Mais tarde, a escola decidiu partilhar essa brochura nas páginas das redes sociais. Isto é permitido no âmbito do RGPD. (**Falso**: o consentimento tem de ser dado de forma específica e não pode ser agregado para fins múltiplos. Isto significa que a escola deveria ter obtido consentimento separado e explícito para a utilização do prospeto nas suas redes sociais.

8. O principal objetivo do RGPD é restringir a publicidade *online*. (**Falso**: na sociedade digital de hoje, em que os dados pessoais são supervaliosos, o RGPD pretende devolver aos cidadãos o controlo sobre os seus dados pessoais, proporcionando-lhes uma maior proteção e direitos, aplicando-se diretamente em toda a UE, em harmonização com as 27 diferentes leis de proteção de dados).

9. Quando guarda uma fotografia de terceiros que encontrou no Instagram, apenas para mostrar no cabeleireiro o corte de cabelo que gostaria, o RGPD não se aplica. (**Verdade**: o RGPD não se aplica às atividades pessoais e domésticas).

10. A publicidade personalizada/comportamental nas redes sociais só é permitida se tiver o seu consentimento? (**Verdade**: para publicidade com base no seu comportamento de navegação, é necessário o uso de *cookies*. Para que os websites armazenem estes *cookies* no seu dispositivo, o seu consentimento prévio é necessário, com base nas regras de ePrivacy, e não no RGPD. Além disso, as empresas devem sempre proporcionar-lhe a oportunidade de retirar este consentimento).

Material criado no âmbito do projeto no. 2019-1-RO01-KA201-063996 – *Kit de Ferramentas Educativas para o Desenvolvimento da Literacia para as Redes Sociais* – cofinanciado pelo Programa Erasmus + da União Europeia
Cofinanciado pelo Programa Erasmus+ da União Europeia