



GDPrAPP

# Proteja Os Seus Educandos, E Os Seus Dados

Um Guia Para o Ajudar a Proteger os  
Dados Pessoais Online do Seu Educando



Co-funded by the  
European Union







# Sobre Este Guia

## A Importância Deste Guia

O projeto GDPrApp Erasmus visa ajudar os alunos a nível da UE a saberem mais sobre o Regulamento Geral de Proteção de Dados (RGPD) de uma forma lúdica.

O objetivo do projeto é que as questões relacionadas à privacidade se tornem claras para os alunos. Tendo em consideração que os jovens merecem proteção especial quando se trata do processamento dos seus dados pessoais, o uso da aprendizagem baseado em jogos é uma abordagem eficaz para que estes adquiram mais conhecimento sobre o RGPD. Ao mesmo tempo, o projeto oferece material, sessões de esclarecimento e um curso online para treinar adequadamente professores e encarregados de educação para que estes possam apoiar melhor os alunos e garantir a segurança das suas informações pessoais .

## O Que Encontrará Neste Guia

-  **Apresentação do RGPD** Diretrizes sobre o que é o RGPD
-  **Benefícios** Uma visão geral dos benefícios e recursos disponíveis para proteger as informações pessoais dos seus educandos
-  **Sugestões** Ferramentas para verificar e proteger as informações pessoais dos seus educandos
-  **Jogos** Verifique os seus conhecimentos sobre o RGPD de uma forma divertida

## Informações Complementares

- **Clareza** Este guia informa-o sobre seus direitos e responsabilidades
- **Coerência** Este guia apresenta dados sobre o RGPD de forma coerente e compreensível.
- **Apoio** Este guia é um recurso valioso para ajudá-lo a esclarecer quaisquer dúvidas ou preocupações relacionadas ao RGPD

## Nota Importante



Pode acompanhar as nossas atividades nos seguintes sites:

Site do Projeto	<b><a href="https://gdprapp-project.eu">gdprapp-project.eu</a></b>
Projeto eTwinning	<b><a href="https://school-education.ec.europa.eu/en/etwinning/projects/gdpr">school-education.ec.europa.eu/en/etwinning/projects/gdpr</a></b>
Facebook	<b><a href="https://www.facebook.com/Gdpr-App-Erasmus-Project">Gdpr-App-Erasmus-Project</a></b>
LinkedIn	<b><a href="https://www.linkedin.com/company/gdprapp-erasmus-project">gdprapp-erasmus-project</a></b>

# Índice

	<b>Sobre Este Guia</b>	02
	◉ A Importância Deste Guia	02
	◉ O Que Encontrará Neste Guia	02
	◉ Informações Complementares	03
	<b>Índice</b>	04
<b>01</b>	<b>O Que é o RGPD?</b>	06
	1.1 Breve História	07
	1.2 Os Objetivos do RGPD	07
<b>02</b>	<b>Dados Pessoais</b>	08
	2.1 O Que São?	09
	2.2 Como São Partilhados?	09
	2.3 Quem Quer os Seus Dados e Para Que Servem?	09
<b>03</b>	<b>Porquê Que é Importante Saber Sobre o RGPD como Encarregado de Educação</b>	10
	3.1 Crianças, Redes Sociais e Videojogos	11
	3.2 VOCÊ e as Redes Sociais	12
	3.3 Na Escola	13

<b>04</b>	<b>Como Proteger os Dados Pessoais do Seu Educando?</b>	14
	4.1 Fale, Fale, Fale	15
	4.2 Navegue em Segurança - Lista de Verificação	16
<b>05</b>	<b>Ciberbullying</b>	17
	5.1 O Que é Ciberbullying?	18
	5.2 Atenção ao Ciberbullying - Lista de Verificação	19
	5.3 Reivindique os Seus Direitos Digitais	20
<b>06</b>	<b>Teste os Seus Conhecimentos</b>	21



# 01

## O que é o RGPD?

## 1.1 Breve História

O Regulamento Geral de Proteção de Dados (RGPD) é uma lei de privacidade e segurança de dados aprovada pela União Europeia (UE). O RGPD aplica-se a qualquer organização, independentemente da sua localização, que recolha, processe ou tenha como alvo dados pessoais de indivíduos na UE e no Espaço Económico Europeu (EEE).

O RGPD entrou em vigor a 25 de maio de 2018 e impõe obrigações rígidas às organizações, e, ao mesmo tempo, garante fortes direitos de privacidade aos indivíduos. Violações do RGPD podem resultar em penalidades severas, com multas que chegam às dezenas de milhões de euros.

A Europa introduziu o RGPD como uma resposta às crescentes preocupações sobre privacidade de dados na era digital. Com o surgir de múltiplos serviços online, tais como: serviços bancários, sites de redes sociais, etc os dados pessoais são cada vez mais partilhados e armazenados.

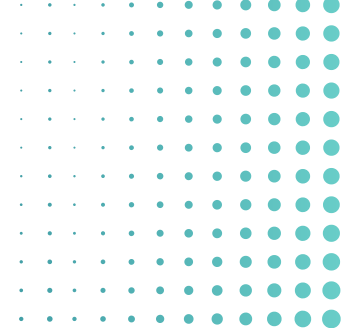
## 1.2 Os Objetivos do RGPD

- **Melhorar a Proteção de Dados Pessoais** – Fortalecer os direitos de privacidade dos indivíduos.
- **Aumentar a Transparência e o Controle** – Dar aos indivíduos maior acesso e controlo sobre seus dados pessoais.
- **Unificar as Leis de Proteção de Dados** – Estabelecer uma estrutura regulatória única em toda a UE.
- **Melhorar a Responsabilização** – Responsabilizar as organizações pela segurança dos dados recolhidos.
- **Garantir a Segurança dos Dados** – Aplicar medidas de segurança rigorosas e penalidades pela não conformidade.

# 02

## Dados Pessoais





## 2.1 O Que São?

Dados pessoais são informações que o identificam ou caracterizam:

- ◉ Sobrenome / Primeiro Nome
- ◉ Idade / Data de Nascimento
- ◉ Endereço Postal
- ◉ Endereço IP
- ◉ Endereço de Email
- ◉ Número da Segurança Social
- ◉ Voz / Rosto / Foto
- ◉ Gostos / Atividades / Profissão
- ◉ Registo Médico
- ◉ Opiniões Políticas
- ◉ Religião
- ◉ Orientação Sexual

## 2.2 Como São Partilhados?

- Sempre que está online (em qualquer dispositivo ligado à internet: tablet, computador, telefone, consola de jogos, etc).
- Quando efetua o login (accedendo a uma conta pessoal, uma conta de cliente, uma aplicação que descarregou, etc).

**Consente esta partilha ao não ler atentamente as condições gerais de uso de dados.**

## 2.3 Quem Quer os Seus Dados e Para Que Servem?

Empresas ou qualquer outra entidade individual ou coletiva querem acesso aos seus dados pessoais para que possam:

- Levá-lo a comprar produtos,
- Influenciar o seu comportamento e a sua maneira de pensar.

**Lembre-se! Não sabe quem está analisando os seus dados nem como estes podem ser usados. Algo que pode parecer irrelevante para si, pode acabar por lhe ser prejudicial.**

# 03

## Porquê Que é Importante Saber Sobre o RGPD Como Encarregado de Educação?





Da mesma forma que não deixaria o seu educando sozinho numa cidade desconhecida, não pode deixá-lo sozinho na Internet. A liberdade que dá ao seu educando depende da maturidade que este demonstra ter.

Os perigos podem encontrar o seu educando em vários locais, até mesmo naqueles que pressupõe serem seguros.

## 3.1 Crianças, Redes Sociais e Videojogos

As estatísticas mostram que muitas crianças de 8 anos já estão registadas em redes sociais como: YouTube, TikTok, Snapchat, Instagram, etc, ou então usam uma dessas contas graças a familiares mais velhos ou amigos. Os jogos online também os levam a estarem ligados à internet.

Às vezes nem têm consciência que estão numa rede social: uma plataforma de vídeo onde se pode publicar comentários, publicar vídeos e criar seu próprio canal é uma rede social; um serviço de mensagens instantâneas que permite criar grupos é uma rede social.

Na maioria das vezes, as crianças acham que estão apenas a se divertir, mas podem ser enganadas online. As técnicas para enganar pessoas online são cada vez mais sofisticadas.

### Quais São os Perigos?

- Terem acesso a conteúdo inapropriado para a sua idade.
- Conhecerem as pessoas erradas e serem vítimas de perseguição ou cyberbullying.
- **Phishing:** divulgarem, sem saber, informações pessoais (localização, vida familiar e atividades, dados bancários, problemas de saúde).
- **Golpe:** serem roubados online após uma compra falsa, por exemplo.
- **Hacking:** permitirem inadvertidamente a instalação de vírus que enfraquecem a segurança da sua rede e roubam informações.

## 3.2 VOCÊ e as Redes Sociais

Os pais também podem ser uma fonte de insegurança na internet. Publica as fotos dos seus filhos online? Onde armazena essas fotografias? Quem pode distribuí-las?

**Atenção: Não pode controlar quem as partilha entre seus contatos.**

53% dos pais franceses já partilharam conteúdo sobre seus filhos nas redes sociais. Em 2018, os pais de crianças de 13 anos publicaram uma média de 1.300 fotografias dos seus filhos.

*Fonte: Observatório de Parentalidade e Educação Digital (OPEN)-POTLOC, 2023.*

### Os Riscos

- Utilização das fotografias para a criação de perfis falsos; partilha das fotografias com estranhos ou até mesmo a publicação das mesmas em sites de pornografia infantil.
- Imagens e vídeos capturados com telefones ou câmeras frequentemente contêm metadados (geolocalização, data e hora da captura). Essas informações podem revelar detalhes importantes sobre os hábitos e a vida do seu filho, oferecendo pistas valiosas a cibercriminosos.
- A criação de uma identidade digital pode prejudicar seus filhos a longo prazo. Esse rasto digital pode ter consequências futuras, afetando a reputação ou a possível vida profissional do seu educando.

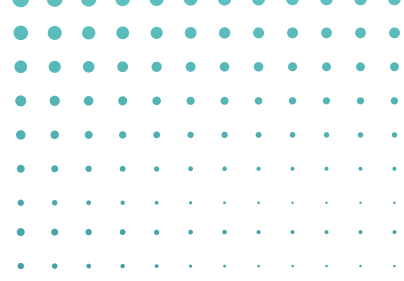
### O Que Fazer?

- Opte pela partilha privada em vez de pública.
- Peça o consentimento do seu educando antes de publicar.
- Evite certas fotos e vídeos (nudéz), mesmo no modo privado, e esconda o rosto do seu educando.

### Quais São os Direitos do Seu Educando?

As crianças têm o direito fundamental à sua imagem, que está vinculado ao respeito à sua vida privada. Os encarregados de educação devem garantir que os direitos de imagem dos filhos são respeitados.

Em caso de publicação sem consentimento, pode solicitar a remoção de fotos ou vídeos online. Se uma rede social se recusar a excluir esse conteúdo, pode submeter uma reclamação no Centro Nacional de Cibersegurança (CNCS).



## 3.3 Na Escola

As instituições educacionais lidam com uma grande quantidade de dados pessoais, incluindo registos de alunos (informações sociais e médicas) e detalhes dos encarregados de educação.

**Você e os seus educandos têm direito à privacidade, mesmo na escola.**

Como encarregado de educação, tem ser informado sobre a política de RGPD da escola e sobre seus direitos, bem como os dos seus filhos, para poder protegê-los.

---

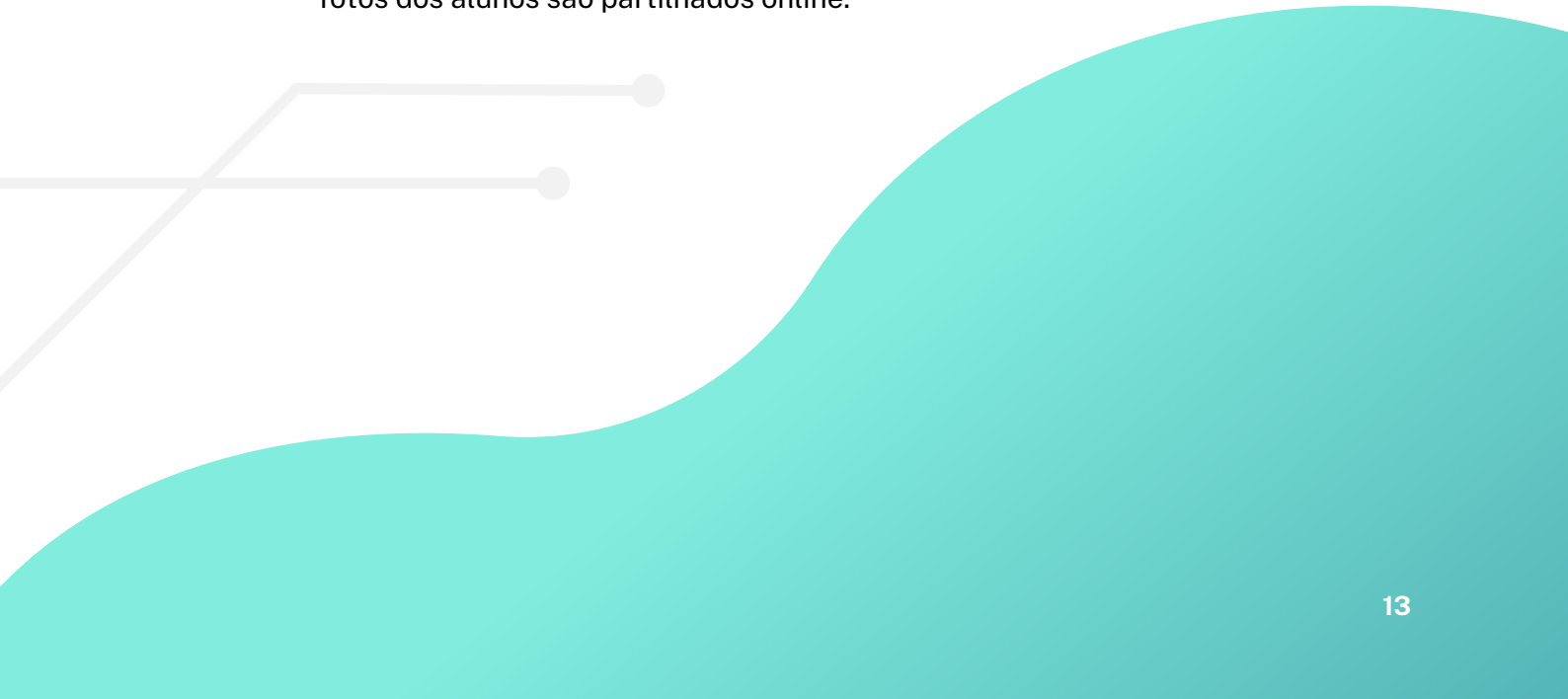
As escolas estão autorizadas a recolher e processar dados pessoais, mas com limitações, por exemplo:

- Os registos de saúde e os detalhes dos problemas de aprendizagem são limitados ao conselho de turma e pessoal administrativo.
- Os detalhes da situação financeira e administrativa da família são limitados ao pessoal administrativo.

---

A escola também deverá proporcionar um acesso segura à Internet:

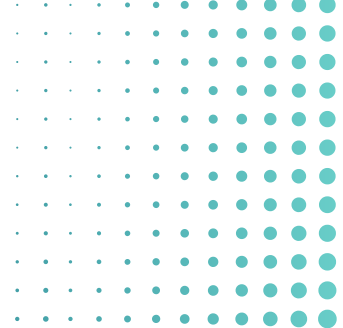
- Limitando a exposição à publicidade enquanto os alunos navegam na internet na escola.
- Utilizando plataformas online que respeitem o RGPD.
- Protegendo as contas escolares quando estas estão disponíveis online.
- Solicitando a aprovação dos pais quando a produção intelectual / vídeos / fotos dos alunos são partilhados online.



# 04

## Como Proteger os Dados Pessoais do Seu Educando?





## 4.1 Fale, Fale, Fale

Proibir ou controlar não é o suficiente para proteger seu educando. Além disso, a tecnologia digital também tem aspetos positivos e já se tornou uma parte importante da nossa vida social.

Tal como na vida real não seguiu o seu educando para todo o lado, mas ensinou-o a estar em segurança, também precisa de ensiná-lo a ser um e-cidadão autónomo.



### Como?

Pode lhe fazer perguntas sobre:

- ❖ As suas redes sociais favoritas, vídeos, jogos e por que motivo essas são as suas preferidas. Experimente-as com ele! Verifique com ele qual é o seu estado de privacidade nessas plataformas.
- ❖ O que ele não gosta de ver/lidar na internet e ajude-o a criar formas de evitar esse conteúdo.
- ❖ Se ele já passou por más experiências até agora e como evitá-las.
- ❖ Se ele alguma vez desistiu de alguma atividade ou encontros com amigos por causa da internet.

## 4.2 Navegue em Segurança - Lista de Verificação

Utilize esta lista para verificar com o seu educando a utilização que ele faz da Internet.



Eu dou o mínimo de informações possível sobre minha identidade.



Eu navego em privado (“janela privada” nos navegadores).



Eu recuso cookies e localização.



Eu uso um pseudônimo nas redes sociais.



As minhas contas nas redes sociais estão no modo “privado”.



Eu uso o motor de busca que mais respeita/protege os meus dados.



Nos formulários online, preencho apenas as caixas essenciais.



Quando alguém me diz “Você ganhou...” ou “Recupere seu dinheiro...”, eu termino o acesso/ligação.



Eu atualizo meus dispositivos para manter os hackers longe. Eu ativo as opções de atualização automática.



Eu guardo uma cópia dos meus dados num lugar seguro.



Evito conteúdo não oficial (streaming ilegal) para não correr o risco de infectar o meu computador com vírus.



Eu uso senhas fortes e únicas, com autenticação de 2 fatores em todas as minhas contas.



Eu recuso cookies, apago meu histórico e bloqueio anúncios.

# 05

## Ciberbullying



## 5.1 O Que é Cyberbullying?

O cyberbullying, que pode ter consequências dramáticas, é um fenómeno que afeta crianças, adolescentes, e adultos. O cyberbullying refere-se a comportamentos maliciosos online, tais como:

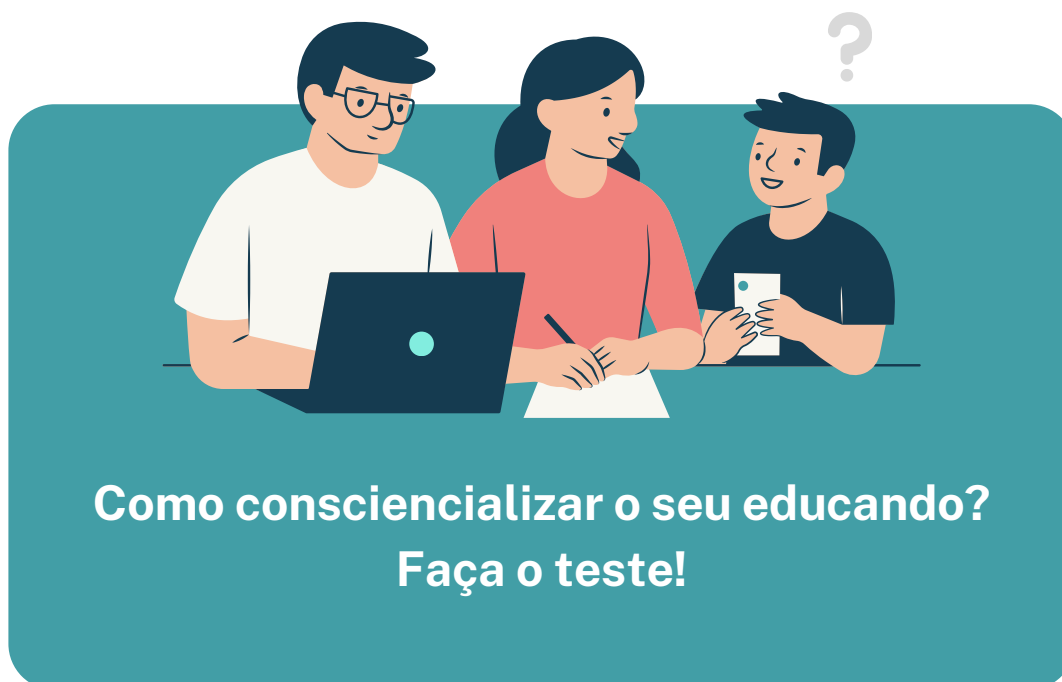
- Insultos,
- Ameaças,
- Rumores,
- Disseminação de conteúdo humilhante.

Esses actos podem ser cometidos por uma única pessoa ou por várias e podem ocorrer em redes sociais, plataformas de mensagens, fóruns ou blogs.

Crianças e adolescentes são particularmente vulneráveis ao cyberbullying. Um estudo da Association e-enfance revela que 24% das famílias já foram confrontadas com uma situação de cyberbullying pelo menos uma vez. O Ministério da Educação Nacional estima que 1 em cada 5 alunos do ensino médio é vítima de ciber-violência.

O cyberbullying geralmente começa no ambiente escolar e continua fora da escola, nas redes sociais.

**Proteger os dados pessoais limita os riscos.**



## 5.2 Atenção ao Cyberbullying - Lista de Verificação



**Eu penso antes de agir online.** Cada publicação, cada comentário, até mesmo uma simples partilha de conteúdo humilhante pode ser considerado cyberbullying.



**Eu peço o consentimento** das pessoas antes de publicar uma foto ou vídeo de alguém.



**Eu não partilho informações pessoais online** (as minhas opiniões, número de telemóvel, religião, estado de saúde, etc.)



**Eu permaneço vigilante** e denuncio conteúdo ilegal, mesmo que não seja eu a vítima direta do assédio.



**Eu falo apenas com quem confio.**



**Eu mantenho evidências dos factos** (capturas de ecrã de mensagens ou publicações, incluindo data e hora).



**Eu bloqueio utilizadores:** bloqueia as contas de autores de conteúdo violento.



**Eu denuncio conteúdo:** pode denunciar conteúdo prejudicial diretamente à plataforma relevante.



## 5.3 Reivindique os Seus Direitos Digitais



Se conteúdo violento ou comprometedor for publicado online, a lei permite que as vítimas solicitem a sua eliminação.



Pode solicitar a exclusão dos seus dados (imagens, vídeos, etc.) de qualquer site ou rede social onde eles foram publicados (direito de apagamento).



Se o conteúdo que pretende eliminar ainda surgir nos resultados dos motores de busca, também pode solicitar a desreferenciação.

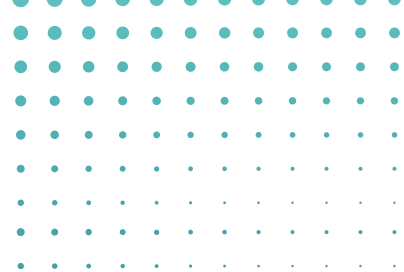


Se as plataformas ou os motores de busca não responderem ou se recusarem a agir dentro dos prazos estabelecidos, pode encaminhar o caso às autoridades para fazer valer os seus direitos.

# 06

## Teste os Seus Conhecimentos





**GDPPrAPP**

**Vamos ver o que aprendeu.  
Aceda a este jogo online!**





# Obrigado!

Este folheto foi escrito e concebido graças ao cofinanciamento Erasmus do Projeto KA220 GDPR App.

## Versão Original

### Texto

M. Hamrit

### Design

M. Klein

### Jogo

R. Pirman

## Versão Portuguesa

### Texto

A. Francisco

### Design

I. Loja

### Jogo

R. Pirman

---

## Informações de Contacto

**Telefone** +33 1 60 73 55 50

**Site** [gdprapp-project.eu](http://gdprapp-project.eu)

**Email** [ce.0770053p@ac-creteil.fr](mailto:ce.0770053p@ac-creteil.fr)

### Endereço

College Elsa Triolet  
Rua Malik Oussékine 2,  
77130 Varennes-sur-Seine,  
França



Co-funded by the  
European Union

