GDPrAPP

Protect Your Child, Protect Their Data

Your Guide to Help You Protect Your Children's Personal Information Online

Co-funded by the European Union

About This Guide

Why This Guide Is Important

The GDPrApp Erasmus project aims at helping students at EU level to gain knowledge regarding GDPR in a playful way. The goal of the project is the privacy related issues to become very clear for the students. Taking into consideration that children warrant special protection when it comes to the processing of their personal data, the use of game-based learning is the most effective approach. At the same time, the project aspires to properly train teachers and parents to be able to support students.

This guide will give you access to useful information in order to guarantee your children's personal information safety.

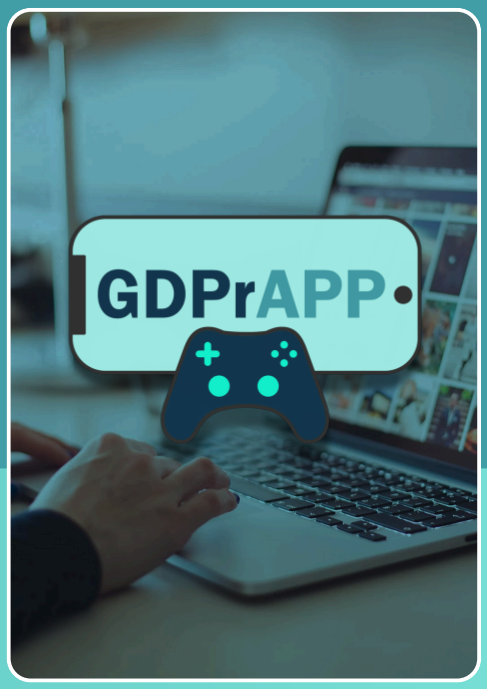
What You'll Find in This Guide

GDPR Presentation	Guidelines on what GDPR is
Benefits	An overview of the benefits and resources available to protect your children's personal information
Tips	Tools to check and protect your children's personal information
Games	See how well you are informed about GDPR in a fun way

Complementary Information

- **Clarity** — It ensures you are informed about your rights and responsibilities
- **Consistency** — It provides a unified understanding of GDPR
- **Support** — It is a valuable resource to help you navigate any questions or concerns related to GDPR

Important Note



You can follow the progress of our activities on the following websites:

Project Website	**gdprapp-project.eu**
eTwinning Project	**school-education.ec.europa.eu/en/etwinning/projects/gdpr**
Facebook	**Gdpr-App-Erasmus-Project**
LinkedIn	**gdprapp-erasmus-project**

Table of Contents

01 What Is GDPR?

1.1 A Brief History

The General Data Protection Regulation (GDPR) is a data privacy and security law passed by the European Union (EU). It applies to any organization, regardless of location, that collects, processes, or targets personal data of individuals in the EU and European Economic Area (EEA).

The GDPR came into effect on May 25, 2018, and imposes strict obligations on organizations while ensuring strong privacy rights for individuals. Violations of GDPR can result in severe penalties, with fines reaching up to tens of millions of euros.

Europe introduced GDPR as a response to the growing concerns over data privacy in the digital age. With the rise of cloud services, online banking, and social media, more personal data is being shared and stored than ever before.

1.2 The Goals of GDPR

- **Enhance Personal Data Protection –** Strengthen privacy rights for individuals.
- **Increase Transparency & Control –** Give individuals greater access and control over their personal data.
- **Unify Data Protection Laws –** Establish a single regulatory framework across the EU.
- **Improve Accountability –** Hold organizations responsible for data security.
- **Ensure Data Security –** Enforce strict security measures and penalties for non-compliance.

02
Personal Data

2.1 What Is It?

Personal data is information that identifies or characterizes a person:

- **Surname / First Name**
- **Age / Date of Birth**
- **Postal Address**
- **IP Address**
- **E-mail Address**
- **Social Security Number**
- **Voice / Face / Photo**
- **Tastes / Activities / Profession**
- **Medical Record**
- **Political Opinions**
- **Religion**
- **Sexual Orientation**

2.2 How Is It Communicated?

- When you're online (any device connected to the internet: tablet, computer, phone, TV, toy, console, speaker, etc.).
- When you've logged in (by going to a personal account, a customer account, by using your avatar to play, an application downloaded to your smartphone, etc.).

We consent to this by not reading carefully to the general conditions of use.

2.3 Who Wants It and What For?

Companies or any other structure can target audiences us to:

- Make purchases,
- Influence our behavior,
- Influence our way of thinking.

You don't know who is analyzing your data and how it might be used.

Something that seems irrelevant to you can be detrimental to you.

03

Why Is It Important To Know About GDPR As A Parent

As well as you wouldn't let your child unattended in an unknown city abroad, you cannot let them unattended on the Internet. The freedom you will give them goes along with their maturity.

What is published on the Internet stays as long as you do nothing about it!

Dangers can meet them in different places, even some you would find safe.

3.1 Kids, Social Media, and Video Games

Statistics show that many children as young as 8-years-old are already registered on a social network such as YouTube, TikTok, Snapchat, Instagram, etc., or use one thanks to older family members or friends. Online video games also lead them, logically, to be connected.

Sometimes you don't know you're on a social network: a video platform where you can post comments, publish videos and create your own channel is indeed a social network. An instant messaging service that lets you create groups is a social network.

Most of the time, children think they are just having fun but can be fooled online. Techniques to trap people have become more sophisticated.

What Are The Dangers?

- Have access to inappropriate content for their age.
- Meet the wrong people and be victims of stalking or cyberbullying.
- **Phishing:** unknowingly divulge personal information (location, family life and activities, bank details, health issues).
- **Scamming:** getting robbed online after a fake purchase, for example.
- **Hacking:** virus to weaken your network security and rob your information.

3.2 YOU and Social Media

Parents can also be the source for unsafe experience on the internet. Do you publish your children's photos online? Where are they stored? Who could distribute them?
Careful: you can't control who shares them among your contacts.

53% of French parents already share content about their children on social networks. In 2018, parents of 13-year-olds had already published an average of 1,300 photos of their children.
Source: Observatory of Parenting and Digital Education (OPEN)-POTLOC, 2023.

The Risks

- Creating fake profiles, share them with strangers, or even spread them on child pornography sites.
- Images and videos taken with smartphones or cameras often contain metadata (e.g., geolocation, date and time of the shot). This information can reveal important details about your child's habits and life, giving valuable clues to bad actors.
- Creating a digital identity can harm your children in the long run . This digital trace can have long-term consequences, affecting the child's reputation, school or professional life.

What To Do?

- Prefer private rather than public sharing.
- Ask your child and the other parent for their consent before posting.
- Avoid certain photos and videos (nudity), even on private mode and hide your child's face.

What Are The Rights of Your Children?

Children have a fundamental right to their image, which is linked to respect for their private life. Parents must ensure that their children's image rights are respected.

In case of posting without consent, a child can request the removal of photos or videos online. If a social network refuses to delete this content, you can file a complaint with the CNIL.

3.3 At School

Educational institutions handle a vast amount of personal data, including student records (social and medical information), and parental details.

You and your children have a right to privacy even at school.

As a parent you need to be informed about your school's GDPR policy and your rights as well as your children's to be able to protect them.

Schools are allowed to collect and process personal data, but with limitations, for example:

- Health records and learning issues details are limited to the medical staff.
- Family financial and administrative situation details are limited to the administrative staff.

They also must provide for a safe experience on the Internet:

- Limit exposure to advertising while students browse the internet at school.
- A GDPR friendly use of online platforms.
- Secure their school accounts if any online.
- Collect parental approval when students intellectual output / videos / pictures are shared online.

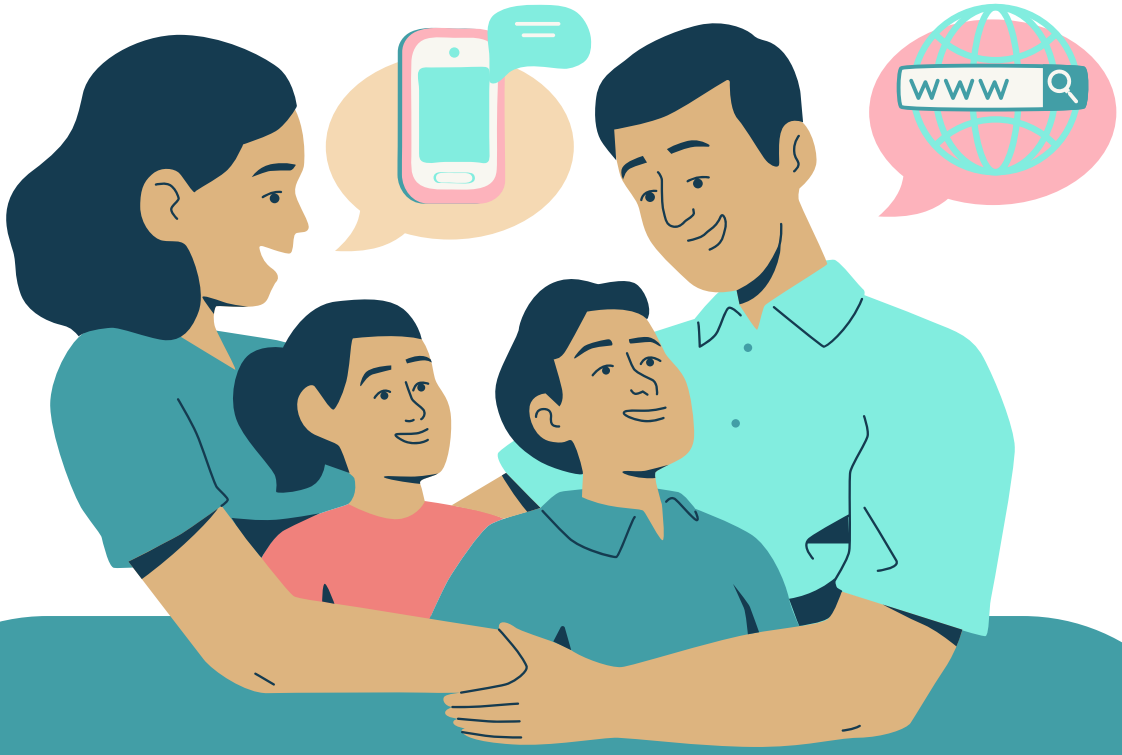
04

How To Protect Your Children's Personal Data

4.1 Talk Talk Talk

Forbidding or controlling isn't enough to protect your child . Plus digital technology has some positive sides and has become an important aspect of our social life.

As in real life you don't follow them everywhere, you need to teach them to be an autonomous e-citizen.



How?

You could ask them about:

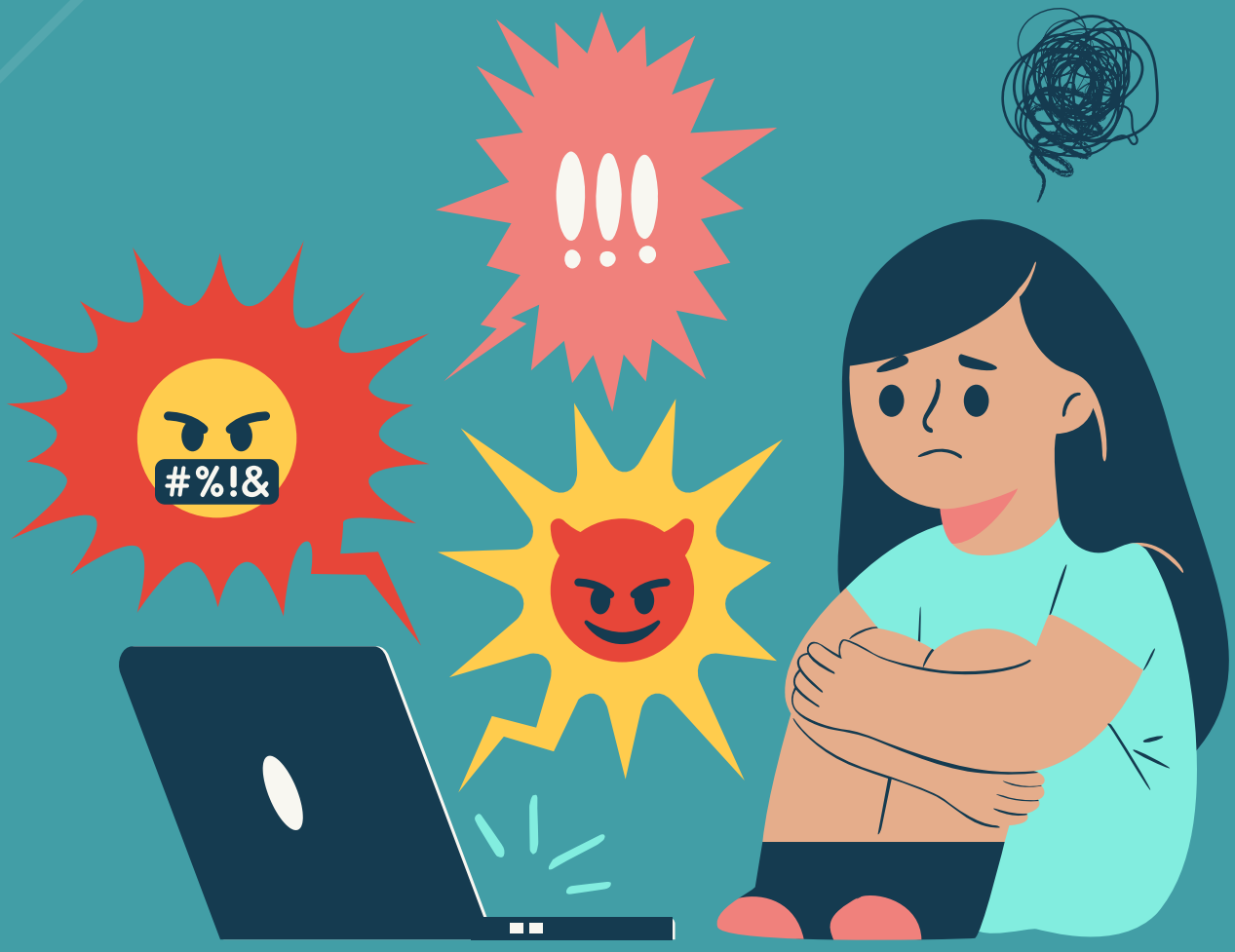
- Their favorite social media, videos, games and why they like them. Try them with them! Check their privacy status with them.
- What they don't like on the internet and help them stay away from it.
- What bad experience they've had so far and how to avoid them.
- If they drop some activities or meeting friends because of the internet.

4.2 Surf Safely - Checklist

Here is a list of facts to check with them about their use of the Internet:

- I give as little as possible information about my identity.
- I browse in private (“private window” on browsers).
- I refuse cookies and localization.
- I use a pseudonym on social networks.
- My social network accounts are in “private” mode.
- I use a search engine that's more respectful of my data.
- In online forms, I only fill in the essential boxes.
- When someone tells me “You've won...” or “Get your money back...”, I back out.
- I update my devices to keep away hackers. I activate automatic update options.
- I save a copy of my data in a safe place.
- I avoid unofficial content (illegal streaming) to keep away viruses.
- I use strong 2 factor authentification passwords for each account.
- I refuse cookies, I erase my history and block ads.

05 Cyberbullying



5.1 What Is Cyberbullying?

Cyberbullying, which can have dramatic consequences, is a phenomenon that affects children and adolescents as well as adults. It refers to repeated malicious behavior online, such as:

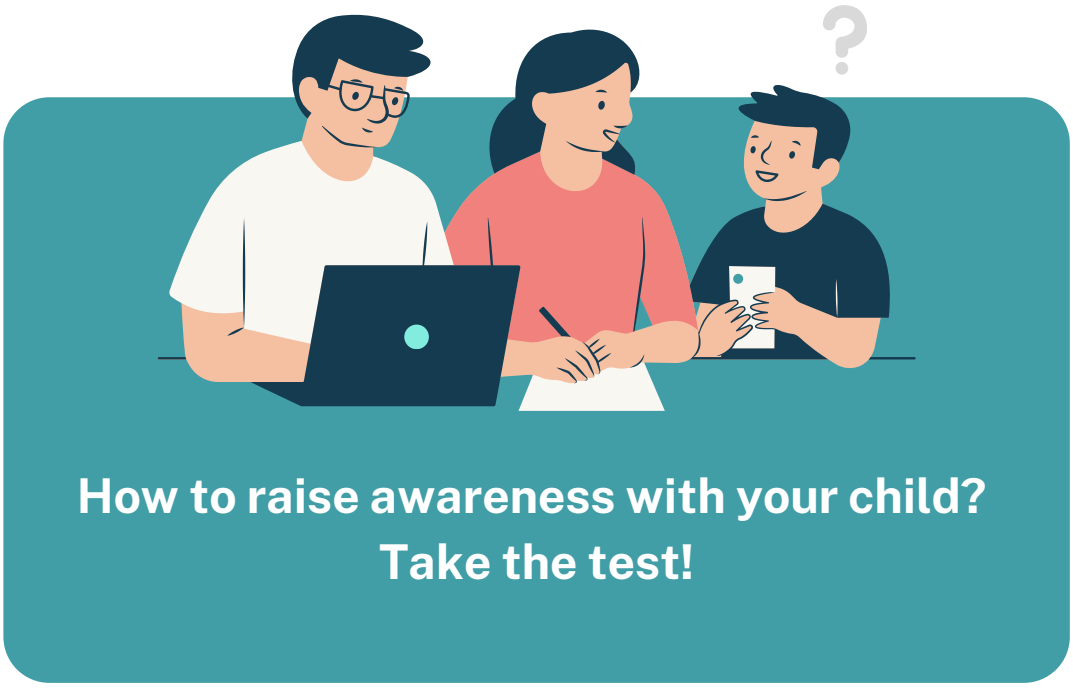
- Insults,
- Threats,
- Rumors,
- The dissemination of humiliating content.

These acts can be committed by a single person or several and take place on social networks, messengers, forums or blogs.

Children and adolescents are particularly vulnerable to cyberbullying. A study by the Association e-Enfance reveals that 24% of families have been confronted with a cyberbullying situation at least once. The Ministry of National Education estimates that 1 in 5 middle school students is a victim of cyberviolence.

Bullying often starts in the school environment and continues outside of school, through smartphones and social networks.

Protecting personal data limits the risks.



5.2 Beware of Cyberbullying - Checklist

- **I think before I act online.** Every post, every comment, even a simple sharing of humiliating content can be considered cyberbullying.
- **I ask for people's consent** before posting a photo or video of someone.
- **I don't share too much personal information:** my opinions, phone number, religion, or health status online.
- **I remain vigilant** and report illegal content, even if I am not a direct victim of harassment.
- **I talk to someone** I trust.
- **I keep evidence of the facts** (screenshots of messages or posts, including date and time).
- **I block perpetrators:** Block the accounts of perpetrators of violent content.
- **I report content:** You can report harmful content directly to the relevant platform.

5.3 Exercising Your Digital Rights

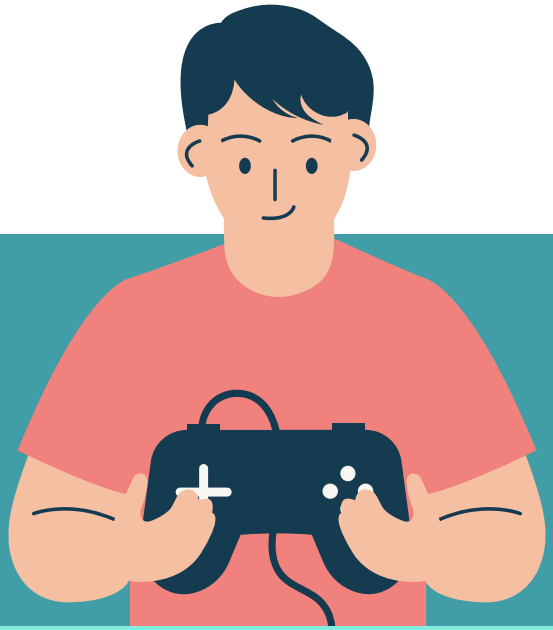
If violent or compromising content is published online, the law allows victims to request its removal.

You can request the deletion of your data (images, videos, etc.) on any site or social network where it is published (right to erasure).

If this content appears in search engine results, you can also request de-referencing.

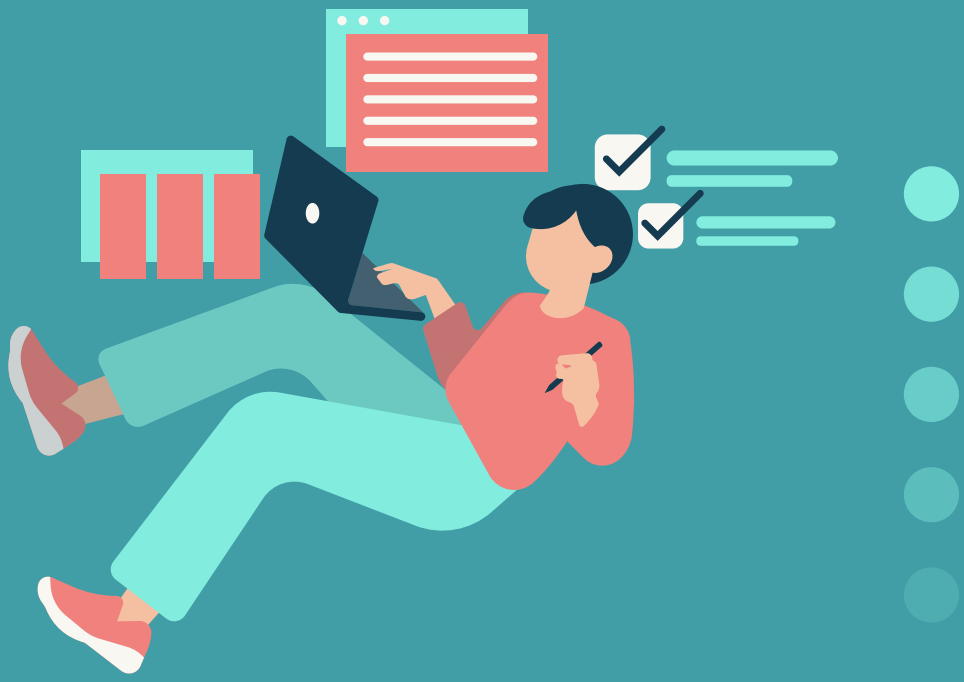
If the platforms or search engines do not respond or refuse to act within the set deadlines, you can refer the matter to the authorities to assert your rights.

06 Test Your Skills



GDPrAPP

Let’s see what you have learned and play this game online!



Thank You

This booklet was written and designed thanks to Erasmus co-funding of the KA220 Project GDPR App.

Text
M. Hamrit

Design
M. Klein

Game
R. Pirman

Contact Information

Phone +33 1 60 73 55 50
Website gdprapp-project.eu
Email ce.0770053p@ac-creteil.fr

Address College Elsa Triolet
2 Rue Malik Oussékine,
77130 Varennes-sur-Seine,
France

Co-funded by the European Union