Learning resources and scenarios

Deliverable D3.1

Editors
Georgia Panagopoulou (HDPA)
Konstantinos Limniotis (HDPA)
Contributors
Georgia Panagopoulou (HDPA)
Eleni Kapralou (HDPA)
Kyriaki Karakasi (HDPA)
Konstantinos Limniotis (HDPA)
Spiros Papastergiou (HDPA)
Stefania Plota (HDPA)
Simos Retalis (UPRC)
Reviewers
Costas Lambrinoudakis (UPRC)
Vasilios Zorkadis (HDPA)
Date
28/8/2023

Classification
Public

Table of Contents

1 Introduction

The byDefault project pursues two strategic goals:

I. To raise data protection and privacy awareness among the critical social group of children.
II. To provide Data Protection Officers (DPOs) and privacy professionals with continuous support in their activities, beyond a basic level, aiming towards specialized guidance on selected key sectors.

To this end, with respect to the first strategic goal, byDefault will focus on the following activities and deliver the corresponding results:

1. Development of a comprehensive education program about privacy, targeting children and especially while using electronic services. Based on this program, byDefault aims at training elementary and secondary school students, thereby enhancing their privacy awareness and data protection culture.
2. Provision of training and support to educators (teachers and professors), in order for them to be able to design and enact learning sessions according to the philosophy of the education program.
3. Performance of a set of pilot education activities to several elementary and secondary schools, to assess the effectiveness of the training program.

This work package (WP3) is linked to the strategic objective of raising data protection and privacy awareness among the critical social group of children. It will specifically develop the educational program. It pursues the following objectives: a) To develop the learning resources b) To evaluate and adapt the learning resources taking into consideration pedagogical issues c)To design the learning scenarios, and develop the tools d) To perform a set of pilot education activities to several elementary and secondary schools.

More precisely, for the WP3, the Task 3.1 (Learning resources development) deals with the development of the learning resources for familiarizing children with concepts such as: Personal data and special categories of personal data; Processing of personal data; Data Controller and Data Subject; Lawfulness of the processing; Consent of the data subject; rights of data subjects; Online personal data commercialization; Personal data protection risks and measures.

The Task 3.2 (Learning scenarios) will take over from Task 3.1, in order to design the actual learning scenarios on the basis of the initial learning resources. To this end, this task will first perform the formative evaluation of the learning resources, taking into consideration pedagogical issues, as well as tools that will be adopted, such as interactive games/AR applications /quizzes/use cases /surveys, for elementary school and high school children. Thereupon, this task will perform the design of learning scenarios and the development of the various components of the educational program using the learning resources.

The WP3 deliverables will be:

- D3.1 –Learning resources and scenarios
- D3.2 – Educational tools
- D3.3 – Pilot education and assessment

The present deliverable (D3.1) will provide the learning resources and learning scenarios that will be used for the development of the various components of the educational program.

2 Description of the learning resources

2.1 Program's general objectives

The educational program aims at explaining principles and key concepts of data protection, informing about the risks of Internet use, applying best practices to address these risks and protecting personal data based on the rights of data subjects. Based on active participation and communication between the participants, the training program aims to train and raise awareness among children in order to understand the importance of the awareness on data protection and privacy issues. The provision of diverse educational material, oriented to the needs of school reality and the continuous support of participants provides a suitable learning environment and enhances incentives to achieve the expected learning outcomes.

2.2 Basic elements for developing learning resources for children

The elements considered for the development of the learning resources include the definition of the goals of the education activities, as well as of the messages which have to be conveyed to the children. The learning path should be as intuitive as possible, adapted to the age of the children, involve various learning styles, including active learning. The description of the content should be as simple and short as possible and expressed in the right language for the targeted audience.

The personal data protection related topics cover a wide spectrum of personal data privacy concepts, progressing from foundational definitions to practical protective measures. The justification lies in providing children with a holistic understanding of their digital footprint, the potential risks, and the tools they can use to maintain their privacy. More specifically, the related learning topics will be (details in the following section):

Learning Topic 1: Real Cases, Statistics, Reports: Introducing real cases, statistics, and reports engages students by showcasing the real-world implications of personal data privacy breaches. Concrete examples make the concept relatable and emphasize the need for vigilance in safeguarding personal information.

Learning Topic 2: Basic Personal Data Concepts: Establishing foundational concepts is essential. This topic educates students about what constitutes personal data, laying the groundwork for understanding privacy risks and protective measures in subsequent topics.

Learning Topic 3: Personal Data Online Sharing: This topic explores the nuances of sharing personal data online. Students need to grasp the potential consequences of sharing too much information and the importance of making informed choices in their digital interactions.

Learning Topic 4: Personal Data Exchange on Social Media and Online Messaging: As social media and online messaging platforms are prevalent among students, delving into personal data exchange on these platforms is crucial. It highlights the privacy challenges specific to these environments.

Learning Topic 5: Online Profiling, Targeting, Advertising, and Influence: Understanding how personal data is used for online profiling, targeting, advertising, and influencing decisions is pertinent. This topic educates students about the mechanisms behind personalized content and its potential impact.

Learning Topic 6: Privacy Policies: Privacy policies play a vital role in data usage. Students need to know how to read and interpret privacy policies to ensure informed consent and understand how their data will be handled.

Learning Topic 7: Deceptive Patterns: This topic raises awareness about deceptive practices online that may lead to data breaches or exploitation. Educating students about these patterns empowers them to recognize and avoid potential traps.

Learning Topic 8: Identity Protection and Account Security: Security measures are essential in data protection. This topic educates students about identity theft risks and equips them with strategies to secure their online accounts.

Learning Topic 9: Personal Data Subject Rights: Ensuring students understand their rights over their personal data is vital. This topic empowers them to exercise control and make informed decisions about their information.

Learning Topic 10: Children and Parents Legal Responsibility: Clarifying legal responsibilities for children and parents in the realm of personal data is essential. This topic ensures a holistic understanding of the legal framework surrounding data privacy.

Overall, the progression of topics follows a logical sequence, starting with foundational concepts and gradually delving into more complex aspects. The program's design ensures that students develop a comprehensive understanding of personal data privacy and are equipped with the knowledge to navigate the digital landscape responsibly.

Designing a training program for school children on personal data privacy requires careful consideration of age-appropriate content and engaging learning resources. Here are some learning resources and topics that we have considered:

- Animated Videos: Create short animated videos that explain the concept of personal data and privacy in a simple and engaging manner. Use relatable scenarios to illustrate how personal information can be shared and the importance of protecting it.
- Interactive Quizzes: Develop interactive quizzes with multiple-choice questions to test students' understanding of key concepts. Provide immediate feedback to reinforce learning.
- Digital Storytelling: Craft digital stories that present real-life scenarios where children need to make decisions about sharing their personal data online. Encourage critical thinking by asking them to predict the outcomes of different choices.
- Interactive Games: Design educational games that teach personal data privacy through play. For instance, a game where students must identify and protect sensitive information while navigating online environments.
- Scenario-based Discussions: Create discussion prompts based on hypothetical situations that students might encounter online. Encourage them to share their thoughts on how they would handle these situations while considering privacy concerns.

With the learning resources, effort is being put on making children understand the content of their rights as data subjects and consolidating the core of their rights. These resources will be offered to students via well thought learning scenarios so that children will be better able to understand that the issues related to the protection of their personal data constitute an integral part of their daily life and the rights they have in this field may have substantial practical impact. In this direction, the children will be provided with detailed relevant guidance and advice on how to study the learning resources. Particular emphasis will be placed on analyzing feedback comments given in response to online quizzes. This process aims to not only present the correct answers but also to provide clear explanations for why other incorrect options were rejected, whenever deemed essential. This approach ensures comprehensive understanding for students.

2.3 Learning resources structure

The learning resources selected are structured in a way to address the topics which are important in the personal data protection legislation and which can by faced and applied to children everyday life - both in the physical as

well as in the on line world. The topics selection aims to cover both the basic personal data protection terms and basic concepts as well as specific data protection related subject matters which are related with the children online behavior. The long experience of the Hellenic Data Protection Authority in handling complaints related to minors, past and recent relevant decisions of European Data Protection Authorities, past and recent decisions of Greek courts were taken into account in the topics inclusion. Real stories and situations, as described in online articles, national, European and world statistical data and reports on the personal data protection issues affecting children through online applications and internet content were also included in the learning resources in order to stimulate the interest of children to the data protection topics and to highlight the range of the matter.

Every topic is developed by stating the relevant personal data protection background and legal provisions, defining the message and the goal of the learning resources and then present the content of the learning resources, in the form of cases and real life situations descriptions, focused questions and answers, together with relevant feedback.

2.4 Description of the learning topics

2.4.1 Learning Topic 1: Real cases, statistics, reports

2.4.1.1 Background

Cases related to problems caused illegal processing of personal data, including issues stemming from online platforms personal data sharing and leakage, are very often – especially within the very challenging, complicated and continuously evolving technological landscape in online platforms and applications. Incidents causing harm to citizens' data protection and overall impacting personal rights and freedoms receive also an extended publicity mainly due to the fact that the platforms involved are globally used. Special cases affecting children's lives and wellbeing are also found in press articles and reports. Surveys and research on children personal data processing are also useful to raise awareness with respect to the extent of the phenomenon and the importance of educating children regarding privacy.

Hence, in order to motivate a child in realizing why personal data protection is important, it is essential first to discuss known data protection "famous" incidents and their possible consequences, so as to illustrate the importance of the field.

2.4.1.2 Learning objective

The objective is for the children to understand the reason that the present education/information/action takes place, to understand the importance and extent of the subject in its European/global dimension and in everyday life of all citizens.

2.4.1.3 Learning resources

2.4.1.3.1 Posts with real facts, newspaper clippings

2.4.1.3.1.1 *Incidents (infringements) related to children personal data*

- TikTok 'mammoth' fine: Ordered to pay £12.7m for children's personal data: TikTok allowed up to 1.4 million children under the age of 13 in the UK to use its platform in 2020, although it sets a minimum age of 13 to create an account without parental consent. [The UK data protection authority fined TikTok £12.7m (€14.5m) for breaching the Children's Privacy Act.] Children's personal data may have been used to identify and profile them, potentially presenting them with harmful or inappropriate content.

(https://www.ethnos.gr/technology/article/254365/prostimomamoythstotiktokkaleitainaplhrosei127ekatliresgiaprosopikadedomenapaidion)

- TikTok cuts off access to users under 13: Popular video sharing app TikTok announced in February 2021 that following an agreement with Italian authorities, it would block access to users under the age of 13. The reason for this move was the death of a 10-year-old girl attributed to a "contest" about who will "hold his breath" the longest that is circulating on social media (https://www.capital.gr/diethni/3523335/to-tiktok-kobei-tin-prosbasi-se-xristes-kato-ton-13-eton/)
- Following an investigation launched in 2020 into Instagram's handling of children's data, found that users between the ages of 13 and 17 were allowed to operate business accounts, which facilitated the publication of the user's phone number and/or email address, a record fine of €405 million was imposed in September 2022 by Ireland's privacy regulator (https://www.neolaia.gr/2022/09/06/instagram-prostimo-405-ekat-eyrw-gia-diarroh-proswpikwn-stoixeiwn/).

2.4.1.3.1.2 *Incidents (infringements) related to citizens' personal data*

- Cambridge Analytica: Facebook announced on 04-04-2018 that the political consulting firm Cambridge Analytica may have improperly accessed the personal data of 87 million users, not just 50 million users as originally announced (https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.htm, https://thepressproject.gr/ti-sunebi-me-to-facebook-kai-tin-megaluteri-diarroi-prosopikon-dedomenon/, https://www.tovima.gr/2018/04/04/world/facebook-diarroi-stoixeiwn-87-ekat-xristwn-apo-tin-cambridge-analytica/)
- Artificial Intelligence: ChatGPT is blocked by the Italian data protection authority: ChatGPT, the best-known relational AI software that can simulate and process human conversations, suffered on March 20, 2023 a data loss (data breach) related to user conversations and payment information of its paid service subscribers. The Italian Data Protection Authority ordered, with immediate effect, the temporary restriction of the processing of the data of Italian users against OpenAI, the American company that developed and manages the platform, as, among other things, although the service is aimed at people over 13 years old, was found the absence of any mechanism to verify the age of users, which exposes minors to responses completely inappropriate for their level of development and perception (https://www.lawspot.gr/nomika-nea/tehniti-noimosyni-mplokarei-chatgpt-i-italiki-arhi-prostasias-dedomenon?lspt_destination=upgrade)
- Facebook: It admitted again that it shared data with third parties: Facebook has admitted to sharing data with third parties and estimates that the error affects about 5.000 third-party apps that continued to receive information about users even after the latter had stopped using them for more than 90 days. These apps had gained access to personal data because users had signed up to them through their Facebook account. The problem lies in the fact that they continued to receive information after the 90 days, because that is the time limit that Facebook gives them. The number of users affected by this breach is not known, while personal data includes information such as email addresses (https://www.techgear.gr/facebook-sharing-personal-data-third-parties-27521)

2.4.1.3.1.3 *Leaks of personal data*

- One of the biggest leaks of personal data that has happened through social media was recorded on Monday 20/5/2019, as according to techcrunch.com personal data of 49 million Instagram users was leaked. The leaked data includes users' profile photos, follower numbers, locations (city and country) and contact information (emails, phone numbers). (https://www.ethnos.gr/technology/article/40040/instagramdierreysanprosopikadedomena49ekatxrhston)

- WhatsApp failed to inform users about how it shared their data with Facebook and was fined €225 million by the Irish regulator (https://www.lifo.gr/now/tech-science/prostimo-225-ekat-eu-sto-whatsapp-den-elege-stoys-hristes-pos-moirazotan-dedomena)
- In February 2021, the largest combined data leak of the 21st century to date became known. This leak, with the acronym COMB (Compilation Of Many Breaches) concerns more than 3.2 billion unique email and password combinations for many platforms. It is a combination of leaks that happened from 2017 to 2019 and new combinations were added to them. To put the real size in perspective, if we assume that each of these combinations is for one user, then we have 40% of the earth's population or 70% of the people who have access to the Internet (about 4.7 billion people) (https://www.insider.gr/eidiseis/162634/i-megalyteri-diarroi-dedomenon-ston-21o-aiona-kai-emporio-dedomenon-simera)
- Facebook - leak of personal data of hundreds of thousands of Greek users: In April 2021, according to the Hackread website, information from 617.722 Facebook user accounts was leaked in Greece and data from 152.321 accounts in Cyprus. Globally, the leak concerns personal data of more than 500 million Facebook users. The leaked data involves data such as phone numbers, names, locations, birthdays, CVs and in some cases e-mail addresses. (https://ant1news.gr/texnologia-epistimi/article/600919/facebook-diarroi-prosopikon-dedomenon-ekatontadon-xiliadon-ellinon-xriston)
- A dataset, which appears to come from Facebook, appeared on a hacking website and contains files of 533 million people. A significant number of them are users from the EU, while over 600.000 are from Greece (see https://www.hackread.com/facebook-data-users-106-countries-leaked-online/, https://www.dpa.gr/el/enimerwtiko/deltia/emfanisi-synoloy-dedomenon-dataset-sto-diadiktyo HDPA Press Release 04-07-2021).
- Data leak of 350,000 influencers and social media users: According to security firm Risk Based Security, the social media marketing company Preen.Me suffered a hacking attack in June 2020 that allowed the attacker to gain access to the personal data of approximately 100.000 influencers and 250.000 social media users. The attacker then exposed the stolen data on hacking forums. This means that any cybercriminal can access them and use them to carry out attacks and fraud. The stolen information includes influencers' social media links, email addresses, names, phone numbers and home addresses. The influencers affected by the data leak deal with cosmetics and life-style issues. (https://www.secnews.gr/247999/diarroh-dedomenwn-influencers-social-media-xrhstwn/)

2.4.1.3.1.4 *Tracking and influencing*

- About 6 out of 10 have fallen victim to fake news (athensvoice.gr): During the lockdown period, Greeks mostly used their smartphone (63.3%) and much less their laptop (15.1%) to access the internet. More than half (55.2%) have fallen victim to fake news, 1 in 3 have been approached by people who hid their true identity and intentions, 26.9% have accepted requests for personal data (personal details, bank details), while cases of sexual harassment (15.1%), electronic fraud (12.4%) and cyberbullying (7.3%) are also common. (https://www.athensvoice.gr/advertorial/market/656069/peripoy-6-stoys-10-ehoyn-pesei-thymata-fake-news/)
- Over 150 million websites with tracked content: More than 150 million websites contain sensitive and tracked content related to personal data, including nationality, political, religious and philosophical beliefs, genetic and biometric data, health data and sexual orientation. This conclusion, which contradicts the European legislation on personal data protection, was reached by the international research team of the IMDEA Networks Institute of Madrid, which investigated over one billion English-language websites in the last two years through specialized machine learning classifiers. (https://marketingweek.gr/pano-apo-150-ekat-i-istoselides-me-tracked-periechomeno/)

- “Game" consisting of a series of dangerous challenges: Some people (one or many), under the name "Jonathan Galindo", create profiles on social media such as Facebook, TikTok and Instagram and send messages to children (usually between 8 and 15 years old), challenging them to participate in a "game" consisting of a series of dangerous challenges.(https://www.ant1news.gr/eidiseis/article/598119/diadiktyo-paixnidi-odigei-paidia-stin-aytoktonia-eikones)

2.4.1.3.2 Survey statistics

a) What happens in one minute on the Internet[1]!

Digital Services Act: Webinar for National Regulatory and Competent Authorities, Jan 2023.

b) According to EU Kids Online 2020 survey [2]:

- 57% of children connect to the Internet from their cell phone or smartphone several times a day or continuously, 23% daily or almost daily and 20% less often
- The estimated average time children are online is 167 minutes per day. More specifically, children aged 9-11 are online 114 minutes each day, children aged 12-14 are 192 minutes and children aged 15-16 are 229 minutes
- Children's daily activities on the Internet are, in order of preference, watching videos, listening to music, communicating with family or friends, visiting social media, playing video games, using it for school work, looking for items to buy or to see their price, watching the news
- 25% of children experienced something on the Internet that annoyed or disturbed them; for 7% of children this unpleasant event happens at least every month (and sometimes this holds the 17% of children).
- 39% of children always know how to react to third party behavior they don't like, 28% often, 20% sometimes and 13% don't know how to react

c) According to the Hellenic Safer Internet Center survey[3] of Greek school students:

[1] Digital Services Act: Webinar for National Regulatory and Competent Authorities, Jan 2023.
[2] EU Kids Online 2020 survey carried out in 2017 – 2019 on 25.101 children in 19 European countries [10]
[3] Research by the Hellenic Safer Internet Center conducted in November-December 2018 on 14.000 Greek school students aged 10-17 [11]

- The majority of children (41%) start using the internet at the age of 7-8 years while 20% state that they started using the internet at the very young age of 4-6 years.
- 69% use the internet every day, 17% about half the days of the week, 8% only at the weekend and 6% use it little.
- Primary school children use the internet by 39% every day, 25% about half the days of the week, 23% only on weekends and 13% minimally.
- High school children use the internet by 74% on a daily basis, 16% about half the days of the week, 5% only on the weekends and 4% very little.
- High school children make daily use by 89% of the internet, 7% do so about half the days of the week, 2% only on weekends and 3% hardly at all.
- To the question "What do you usually do when you're online?" children answer that they talk to their friends (25%), watch movies or listen to music (23%), play games (17%). Girls mainly talk with their friends (60% vs. 40% of boys), watch movies or listen to music (63% vs. 37% of boys) and boys play games (70% vs. 30% of girls). Engaging in online games comes first in preference for elementary school children, while the favorite activity on the internet for high school children seems to be communicating with their friends. Children from all three educational levels enjoy watching movies/listening to music online.
- The vast majority of children (86%) have a profile on a social network, of which 70% appear to start their occupation before the age of 13. In fact, 34% of children who have a profile on social networks opened it themselves, without their parents' consent.
- Children who enter social networks by majority (42%) are at the age of 10-12 (not permitted age).

d) In an even more recent Hellenic Safer Internet Center research[4] it appears that:

- 24% have received online very personal photos of others and 6% have sent online very personal photos of themselves
- 53% of students are not worried about how their online reputation will be shaped by what they upload, post, like, etc., 25% are not worried and 22% say they don't know
- 25% of high school students accept friend requests from strangers on social networks
- 34% of students have encountered hate speech online and 10% have been victims of online fraud
- 6% of students have been victims of cyberbullying and of these 35% reported it to an adult for support, while 34% were patient
- When asked what do you think is the biggest risk on the internet, students answered:
    - 26.1% the disclosure of personal data
    - 17.8% the contact with strangers
    - 15.8% cyberbullying
    - 14.6% sexting
    - 9.1% viruses/malware
    - 6.3% fraud and
    - 5.6% excessive busyness
    - 2.5% misinformation
    - 2.1% bad online reputation
- One in four children say they have been approached online at some point with malicious intent.

[4] Research by the Hellenic Safer Internet Center conducted in the 2021-22 school year on 5.000 Greek school students aged 12-18

2.4.2 Learning Topic 2: Basic personal data concepts

2.4.2.1 Background

The basic concepts related to personal data protection concern the definition of personal data, as well as the proper identification of which type information is considered as personal data. The concept of what is the processing of personal data is also of high importance, as it encompasses a lot of activities and different phases, such as collection, registration, organization, storage, retrieval, use, dissemination, alignment, restriction, or erasure or data destruction of persona data, as well as the meaning of profiling of a user. The roles of personal data controller and processor and the meaning of user's consent is important as children need to be aware of who has the responsibility for their personal data and when the consent given is valid. T

The above basic concepts are all defined in GDPR (General Data Protection Regulation) provisions [3]; the GDPR is the main legal instrument in Europe regarding personal data protection and it applies directly to all Member States – including, of course, Greece. Most importantly, although the GDPR is a European regulation, it applies to all organizations, regardless of their location, if they are involved with processing the personal data of individuals residing in the European Union.

2.4.2.2 Learning objective

The objective is to explain the concept basic concepts with examples from everyday life – physical and digital world - and to also explain how they related to their private lives on a daily basis, when and in what ways they are likely to give out personal data either in their social life or online, mainly through online games, social media services and content sharing.

2.4.2.3 Learning resources

2.4.2.3.1 Basic definitions: what is personal data with examples from everyday life – physical and digital world

- What is personal data?

  Personal data is any information that refers to you (data subject) or characterizes you, such as your name, your address, your telephone number, your school, your interests, your performance at school, your photos, videos with your friends, your profile on social media platforms like Instagram. Sometimes your personal data concerns sensitive elements of your private life, such as your religion, your state of health, your sexual orientation or your political beliefs.

  However, the notion of personal data is wide: even your device information (such as your device ID or IP address) constitutes personal data of yourself; they may suffice to fully identify you, whilst such information may allow associating network/application data with you and, thus, to extract information about you.
- What is the processing of personal data?

  Processing of personal data is any operation performed on personal data, such as collection, registration, organization, storage, retrieval, use, dissemination, alignment, restriction, or erasure or data destruction.
- Who are the data controller and the data processor?

  The controller is the natural or legal person that determines the purposes and means of the processing of personal data (such as, typically, your school for the data processes carried out in the context of the school's activities), while the processor is the natural or legal person that processes personal data on behalf of the controller (for example, a photographer who takes your class photo on behalf of your school or your school's Parents and Guardians Group.
- What is profiling of a data subject?

Any form of automated processing of personal data that uses such data to assess certain personal aspects of a person relating to their personal preferences, interests, work performance, health, behaviour, location or movements.

For example …

- Your Instagram or other social media account contains information about you and your friends, your interests and your photo albums, creating a profile of yourself and the platform records when you log in or log out.
- When you download a new application to your "smart" mobile (hereinafter "smartphone"), the application may collect various data of your device or your personal information.
- When you read your e-mails, your electronic communications provider records the time you logged into your account, the sender of your messages, and the time they were sent to you.
- When you surf the internet, the browser you use records the pages you visit. Some pages install small files (cookies) on your computer so that they can recognize you when you visit them again or send you advertisements for the product or service you saw.
- The paper form you fill in to participate in the competition of the electronic games company or the corresponding electronic form in an online (on-line) book store, contains your personal information, such as name, telephone, address and age.
- Your school keeps data on your grades and performance and the absences for each teaching hour are recorded in the department's absence register.
- The doctor you visited keeps a record of your medical examinations and other relevant information about your health.
- The sports club you are a member of keeps the information you provided during your registration, as well as medical certificates.
- The online music platform you have chosen contains information about your music preferences and the artists you are interested in.
- Your "smart" watch records the route you take, the number of your steps, your pulse and your heart function, creating a profile related to the activity in question (and it may automatically derive conclusions on your health status).
- The photos you took with your friends, which are likely to be posted on Instagram or another social media platform.

2.4.2.3.2 Basic definitions: what consent is with examples from everyday life – physical and digital world

- What is consent?

  Apart from the cases that persons or entities are entitled by law to process your personal data in order to carry out their work, such as the Municipality or your school, any other person/entity needs, in principle, to ensure that you have provided your consent in order to allow her/him use your personal data for a specific purpose. That means after you have previously been informed exactly who is the one who wants to use your personal data, for what reason, which of your data she/he wants to process, with whom she/he will share them and for how long he will keep them, you have accepted and said in a clear way that you agree. In addition, in typical Internet services (social networks, online games, etc.) since there are significant risks to personal data, your consent is valid if you are at least 15 years old; otherwise, the consent of your parent is required.

For example …

- According to the law, your school must collect and retain your name, address, date of birth, grades, absences, etc.

- If the school wants to take photos of the students in your class and give the photos to your parents, it must inform all the students' parents about this action and obtain their consent.
- In order for your classmate to upload to TikTok the video of you skateboarding, he must ask you about it and you must agree to upload it.

2.4.2.3.3 Situations in which information requested is personal data or not

Is it personal data? RIGHT/WRONG

- The photos I sent to my friends only of landscapes from the city I visited do not contain personal data.
  WRONG – such photos provide information on the places I visited (and, possibly, when)
- The photo of the athletes of the basketball team of the school I participate in contains our personal data.
  RIGHT
- My Instagram account passwords that my friend is asking me to email him so he can log in to my account and change my photo is not personal data.
  WRONG – my password constitutes personal data (that should be highly secured, as discussed next). Also, any information that I post in my account constitutes personal data
- When the "location" indicator is activated on my mobile phone, my location is visible, which is personal data.
  RIGHT
- The video in which I have recorded my friend dancing is my friend's personal data.
  RIGHT – and this also holds for any other people possibly appearing in the video

2.4.2.3.4 Information activity in a school – knowledge quiz

"Someone went to the school to inform the students about personal data, on the occasion of the European day of protection.... Then the children write a quiz/test related to Privacy. Whoever gets 100% will win a gift... The story starts with the student reading the terminology and vocabulary. We will need the Vocabulary and the definitions. As the day progresses, the student will question whether they have fully grasped the above concepts and whether they have understood what constitutes personal data and what does not."

The vocabulary will be: *personal data, data subject, processing of personal data, controller, processor, data subject profile, consent*

Quiz questions (Yes, No):

a) Which of the following is personal data in the online world?
   A. Your favorite Spotify playlist (yes), B. Your photos and videos on social media platforms (yes), C. The recording of your location from the GPS of the smartwatch you are wearing (yes), D. Your preferences in music resulting from the choices you have made of specific songs (yes)
b) Which of the following is personal data?
   A. Your name, your age, your height (yes), B. Telling your girlfriend what your favorite band is (yes), C. The most popular band in Greece for 2023 (no), D. The written confirmation from the team doctor that you are able to compete after your injury (yes)
c) In which of the following cases is personal data processed?
   A. Your TikTok account stores the videos you upload with your friends (yes), B. You tagged your friend in the photo you uploaded to Instagram (yes), C. You have made a list of your favorite singers on Spotify (yes), D. You create a file with your photos on your computer (yes)
d) When you surf the Internet, which of the following actions reveal personal data about you?
   A. After reading the sports newspaper article, you delete the history of your visit to it (no), B. You do not delete the history of the pages you have visited in order to prepare the homework you have undertaken

in the history lesson (yes), C. You "like" videos, songs, articles you like (yes), D. In an online store, you provide your full details (name-surname-address-email) in order to receive the book you bought (yes)

e) In which cases do you have to give your consent for your personal data to be used?
A. In the application you have on the smartwatch you wear if you want the recording of your actions during the day to be visible to third parties (yes), B. To the school director for sending the four-month grades to your parents (no), C. Instagram or other social media platforms to display your date of birth (yes), D. To your friend who asks you to upload a picture of the two of you from Saturday's party to her Instagram account (yes).

f) An online game asks you to provide the following information. Which of the following is personal data:
A. Your full name (yes), B. The name of your friend you will play with (yes), C. The color of the game's surroundings (no), D. The date of birth of your friend you will be playing with (yes)

g) When the ticket inspector on the bus asks you to see if you have paid for your ticket, which of the following is or contains your personal data?
A. the electronic travel card with your photo (yes), B. the one-way paper ticket (no), C. your identity (yes), D. the newspaper that is your nearby seat (no)

h) At school, which of the following information pertains to your personal data?
A. The day and time you were absent from class is recorded in the class absence register (yes), B. The canteen manager asks you which foods you are allergic to (yes), C. The principal of the school asks you to provide a doctor's note stating that you can attend the gym class (yes), D. It was posted on the bulletin board that the 2nd class will go on a trip to Ioannina (no)

i) What information from what your "smart watch" records, according to the settings you have made, is personal data?
A. the locations in which you move and the number of steps you have taken in a day (yes), B. your heart rate, the calories you consume and the psychosomatic pressure (hrv status) of your body during the day (yes), C. if you move by car, bicycle, on foot, by plane (yes) D. the hours you sleep and the quality of your sleep (yes)

j) Which information that a social media platform asks for to register is personal data?
A. your age (yes), B. your gender (yes), C. if you are in a relationship (yes), D. which school you attend (yes)

2.4.3 Learning Topic 3: Personal data online sharing

2.4.3.1 Background

One of the main principles that need to be in place when personal data are to be processed is that this process should be performed lawfully, fairly and in a transparent manner (art. 5(1) of the GDPR). Moreover, the personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (art. 5(2)). In simple words, the above imply that the users should be fully aware of what exactly processing occurs with respect to their personal data (i.e., any “hidden” process of personal data is not allowed), and this process should be legitimate, for a well-determined and clear (transparent) purpose.

Unfortunately, the inherent nature of the Web, and especially the use of social networks, allows “malicious” users to easily collect (or even infer) personal data for several, non-legitimate and hidden purposes. This happens due to the fact that individuals – and especially children – tend to share large volumes of their personal data in the Web, without being aware of the risks stemming from this data sharing. More precisely, according to a specific study in Greece that is based on two large-scale surveys (Daskalaki et. al., 2020), a significant percentage of children put themselves at risk by adopting wrong practices such as accepting friends’ requests

from strangers, posting very personal photos on the web, and in general sharing material without thinking of the possible consequences. Such consequences could be, e.g., the use of personal information collected from social networking platforms for doxing—that is, the practice, or the menace, of revealing private information of a victim with the aim of extortion or for online shaming. Therefore, despite the fact that there exist explicit legal provisions that determine the main principles relating to processing of personal data that should be fulfilled, it is essential that children should be fully aware of the relevant risks from data sharing and how to confront them since, as it is stated above, there are always "malicious" users that violate these principles.

2.4.3.2 Learning objective

The main learning objective is twofold: first, the children will be fully aware that their personal data could be abused for purposes such as the following:

a) Malicious individuals may learn a child's personal data and, based on them, search in the real world for the child, putting her/his physical integrity at risk

b) Malicious individuals may uses a child's personal data for doxing, (cyber-) bullying, harassment, extortion or for unfair/abusive criticism

c) Malicious individuals may perform a digital identity theft, so at to create a digital account imitating that it belongs to a specific child, and subsequently posting and sharing information that embarrasses/humiliates the child

d) Potential employers may come to (possibly wrong) conclusions with respect to whether a person will be sufficient for a work position, based on posts that the person has made when she/he was a child

e) Malicious users may manage to get access to either family's bank accounts or credit card information, causing financial loss to the child's family

Second, the children will be aware of how to cautiously use the Internet and especially the social networks with respect to sharing personal data.

2.4.3.3 Learning resources

2.4.3.3.1 Material in the form of real life scenarios

We next present ten (10) learning scenarios, each of them focusing on specific aspects of possible risks that may occur due to the personal data that are being shared with others and, especially on the Web; for each scenario, we explicitly state the personal data that have been shared or inferred (or even found out due to the incautious data sharing), as well as the relevant risks. For the case of simplicity, with respect to the personal data being shared, we do not explicitly refer to the name, last name, the social network account name and the e-mail address of each user (child).

2.4.3.3.1.1 *Maria, a high school student, "uploads" on Instagram a photo from her summer vacation, at the sea. She then receives a series of negative comments from some classmates and followers, not being close friends with her, with regard to her appearance in this photo; comments are of the form "someone needs to start working out ASAP" or "not everyone should upload photos with swimsuit" etc. Despite the fact that her friends have posted good comments, Maria feels very sad, upset and emotionally stressed due to the negative comments.*

Personal data being shared or inferred: Photos, fitness, vacation place, vacation period (and these data may also hold for Maria's family/friends with whom she shares the vacation period)

Risks: Emotional stress/anxiety, sadness, feeling ashamed

2.4.3.3.1.2 *Chrysanthi, a high school student, "reveals" on Facebook that she will be at a certain bar in the evening; more precisely, in the bar's relevant invitation on its Facebook page, she checked the "is going" option which in turn is automatically appeared on her Fb profile. Moreover, one that checks her Fb profile, can draw the conclusion that she recently broke up with her boyfriend and that she is disappointed, whereas at the same time her posts indicate that "she wants to get over him"; more precisely, her posts include songs that refer to "betrayal", quotations of the form "the crucial point is to start getting over you: after this, everything is easier", and "every ending prepares a new wonderful beginning" etc. Chrysanthi posts this information because she is very sad and she really needs the support of real friends. Chrysanthi has among her Fb "friends" a person, Nikos, with whom she had some online (chat) conversations and she thinks that he is a very nice and interesting child. Chrysanthi though does not know Nikos in person. However, Nikos (whose real name is Haris) is a 22-year-old person who simply wants to have a romantic relationship with her for one night – and even against her will. Therefore, he considers the situation (as it is depicted in her Fb's profile) as the most appropriate opportunity to appear on this particular night at the bar as the "friend who cares and will support her", having though malicious purposes to take advantage of her because he knows that she is emotionally vulnerable.*

Personal data being shared or inferred: Photos, emotional status, relationship status, scheduled visit to a specific bar at a specific time

Risks: Damage to physical integrity, physical/emotional abuse

2.4.3.3.1.3 *Kostas, a high school student, makes comments on Fb about football news using slang words - e.g. "Dude, when we scored three goals at you for fun, you used to shut up – so shut up now too", "Did you enjoy the goal at the last minute? I am sure that you will never forget this", "Let's go my team! No mercy!". In fact, some of his posts have also spelling or grammatical errors. Kostas does not speak in this way in his daily life, but he likes, as a teenager, entering into such discussions of football interest with strangers (other unknown to him Fb users who comment on football news) and letting off steam using such language. At the end of the school year, Kostas submits an application to work with a three-month employment contract, as a secretary in a customer service company. The company had to consider two applications for this one position: the company's manager, looking for information on the Internet about the two candidates, found Kostas' profile and came to (wrong) conclusions regarding some aspects of his personality and how he can express himself in his daily life - even though Kostas would be perfect in this job. So he decided it was better to choose the other candidate.*

Personal data being shared or inferred: Favorite football team, way of expression in writing, (possibly erroneous) information about appropriateness for a specific work

Risks: Potential employer comes to (possibly wrong) conclusions about appropriateness for work, different (adverse) treatment with respect to hiring at work

2.4.3.3.1.4 *John has an "open" (i.e., public) profile on Facebook, having published therein information such as his date of birth (15/9/2006), the school he attends (3rd General High School in city A), the football team he supports (Olympiakos) and his email address (johnieA2006@provider.gr). Moreover, based on specific posts and comments that he has made in hid profile, it can also be concluded that there is a special emotional "bond" with his classmate Helen. Antonis is an 18-year-old boy, being in Helen's Fb contact list (i.e. list of friends). Helen has seen Antonis in person only once; he lives in another city and he is friend of one of her friend's cousins. Since Antonis is a Fb "friend" of Helen, he is able to see her other Fb friends, as well as their profiles in case that they are public. Therefore, he checks the John's Fb profile (they do not know each other) and realizes the "bond" he has with Helen. Having unfortunately bad intentions, he decides to make Helen get a bad impression about John. Therefore, Antonis first tries to see if he can guess John's Fb password – unfortunately he immediately finds, by doing a few tests based simply on the John's public information, that John has chosen "olympiakos2006" as his password. He also finds that John has chosen the same password for his e-mail account, so he logs into it and reads all of John's e-mails (incoming and being sent). Hence, Antonis learns the following information that constitute John's personal data: a) Several John's photos, not published in Fb. b) There is a health issue in John's family, which he has shared only with two very close friends of him. c) John, together with 3 classmates of him, call some of their teachers by mocking nicknames - e.g. Mr. Georgiou is "Gargamel", while Ms. Papantoniou is the "Ugly". d) Maria, a classmate of John, often sends him the school exercises she is solving, for help. Unfortunately, Antonis performs the following malicious actions: i) He creates a fake email account with a name "truth_teller", which hides his identity, and through this account he sends Helen screen samples of the e-mail messages that Maria has sent to John, telling Helen that there is a secret relationship between Maria and John. ii) Pretending to be John, he makes a post on John's Fb profile, revealing the mocking nicknames that John is used for some of his teachers – as well as revealing who are the John's classmates who also make fun through the use of these nicknames. This piece of information becomes now known to the whole class and to John's teachers – and of course Helen sees it too. iii) Pretending to be John, he also posts some photos of John from the past, which he has retrieved from his private e-mail messages, but edited through an image editing tool so that they are not flattering to him. iv) By using the above fake email address ("truth_teller"), he informs John that he has managed to gain access to his personal information and "intimidates" him not to tell anyone about this issue, because otherwise the whole school will learn about the health issue his family is facing.*

Personal data being shared or inferred: Personal information such as date of birth, school, friends, favorite football team, photos, emotional status. Based on this information, the user's password (also personal data) became known, which in turn allowed a malicious user to gain access to other personal data contained in personal emails (including photos, comments that the child use is her/his private life about others, sensitive health data for a family member).

Risks: Cyber-bullying, doxing, extortion, humiliation with respect to classmates/teachers/family (including girlfriend/boyfriend), emotional/psychological pressure/stress, feelings of fear and shame, identity theft. The humiliation may also affect the child's friends.

2.4.3.3.1.5 *John has an "open" (i.e., public) profile on Facebook, having published therein information such as his date of birth (15/9/2006), the school he attends (3rd General High School in city A), the football team he supports (Olympiakos) and his email address (johnieA2006@provider.gr). Antonis is a 20-year-old man, being in John's Fb contact list (i.e. list of friends). John has never met Antonis in person; John has accepted a friend request from Antonis because they have a mutual Fb friend, who in turn is also not directly a friend of John in real life). Antonis unfortunately does not have good intentions and wishes to do malicious actions to other target users. So, he checks John's Fb profile, he feels jealously due to the John's popularity as it is illustrated in his Fb profile and, thus, he decides to make some damage on John. First, Antonis tries to see if he can guess John's Fb password – unfortunately he immediately finds, by doing a few tests based simply on the John's public information, that John has chosen «Johnie3HighSchool» as his password. He also finds that John has chosen the same password for his e-mail account, so Antonis logs into it and reads all of John's e-mails (incoming and being sent), as well as several photos of him that the has never published/posted. Unfortunately, Antonis performs the following malicious actions: i) He changes the Fb password for John's account, but also for his email account. Hence, by this, John has no access to these accounts and cannot control them. ii) Having full control over John's Fb profile, he makes several posts impersonating John. More precisely, he uploads photos of John that he found from his personal e-mails (photos that John would never publish), while he "makes fun" of friends and teachers, based on information he obtained from John's personal email messages. All of John's acquaintances are initially very surprised by this behavior that John seems to have. Some of his friends are also feeling offended by some posts.*

Personal data being shared or inferred: Personal information such as date of birth, school, friends, favorite football team, photos. Based on this information, the user's password (also personal data) became known, which in turn allowed a malicious user to gain access to other personal data contained in personal emails (including photos and comments that the child use is her/his private life about others).

Risks: Identity theft, humiliation with respect to classmates/teachers/family/friends, emotional/psychological pressure/stress, feelings of fear and shame

2.4.3.3.1.6 *Sofia will be away for a month (the whole July) with her family for a vacation trip to Europe. She "announces" it on her social networks (Fb, Instagram), and while she is there she also uploads photos from the vacation trip. From the various comments of friends on her social media, one can conclude that she has a holiday house in Rafina, which will remain closed throughout July; this becomes evident from comments from her friends like "What about Rafina this year?", to which Sofia replies "Only in August! The lovely isolated house close to the quiet beach is free for this month! Too bad I can't send the keys for you….". Unfortunately a gang of burglars in the wider area of Eastern Attica monitors user posts in social media in order to learn such information (which houses are to be uninhabited for a specific time period). Sofia's profiles in social networks are public and, thus, these burglars find out that Sofia's family own this house which will be uninhabited in July, it is isolated, whilst they also manage to locate the geographical information of this house based on Sofia's posts on Fb from the previous year, where she has uploaded photos of her while being in this house with location information – i.e., being tagged with location information of the form "Sophia feels relaxed in….".*

Personal data being shared or inferred: Information about vacation (location, vacation period), photos, information about the existence of a holiday home and its address, information that the house will not be visited by anyone for a month

Risks: Facilitating the illegal act of burglary/theft of home's assets

2.4.3.3.1.7 *Alkmini, a 16-years old student, loves dancing and uploads related videos on the Tik Tok platform in which she appears dancing. She has a public account on Tik Tok through which she interacts with hundreds of users (followers, people who make comments and Alkmini replies etc.). One day, Alkmini receives a message on Tik Tok from a stranger, who tells her that he is a professional in the field of seeking for new talents in dance, in order to promote them appropriately in educational schools but also to introduce them in theater/music events for possible participation. This stranger provided to Alkmini information about specific dance schools that collaborates with, as well as some corresponding dancing events that have taken place and in which young dancers participated after his suggestion/promotion. Alkmini, in order to be cautious, searched for information on the Internet and found that the aforementioned dance schools do exist, as well as that all the dancing events that he mentioned indeed took place, while from the electronic communication with him concluded that he is knowledgeable and a serious person (he also sent to her a business card with his e-mail address). Therefore, being excited about the good impression that her videos have given to "talent hunters", she provided to him any material that he asked for (resume, pictures, videos from her dancing – including material that she has never posted online). Her resume contains information such as her age (exact date of birth), the area she lives in, her phone number, the school she goes to and other information such as her personal interests. After some time, Alkmini is worried: there is no progress in the matter, while the stranger starts to become "pressing" to a great extent, asking for more and more personal photos of her. Alkmini actually realizes that this man is dangerous when he suggests that he visits her school by his car so that they can go for a car ride to talk more. Alkmini refuses and tells him that she doesn't trust him and he should not bother her again. But unfortunately he starts blackmailing and terrifying her by saying that he knows too much personal information about her, that he can very easily, with a simple "click", leak photos and videos of her, possibly edited by him, to online adult services, that he can easily create a fake profile impersonating her and so on. At the same time, Alkmini starts receiving many "missed" phone calls at inappropriate times, with a hidden caller's ID phone number.*

Personal data being shared or inferred: Photos, videos, preferences/hobbies, artistic ambitions, any information found in a resume/CV (age, personal interests, home address, phone number, school address, etc.)

Risks: Stalking, extortion, emotional/psychological stress, fear, damage to physical/emotional integrity

2.4.3.3.1.8 *The 15-year-old Eleftheria uses the Web and social networks up to a great extent, while she also likes e-shopping: she always informs her parents about online purchases she likes to have and, if they approve, she proceeds in performing these purchases electronically by using her father's credit card (her father is always present in this online purchase). One day, while surfing on Facebook, she sees that a friend of hers posted an advertisement from an online store referring to great deals on designer clothes and sunglasses: their prices correspond to about 90% discount (e.g. 10 Euros instead of 100 Euros for her favorite sunglasses). Her friend herself writes "Amazing!" in her post. But the offers are about to end within just one hour. Eleftheria's parents are sleeping and she doesn't want to wake them up for this. Being excited about this shopping opportunity, and in order not to miss out the offer on the sunglasses, she takes the credit card from her father's wallet, being sure that he would not object since he would only charge it a few euros in total and also her birthday were approaching (and, thus, she would tell her father that this will be the gift for her birthday and she doesn't want anything else), and makes the purchase herself at the said store, giving her father's information (name, address, all credit card information). After one hour, she sees that her friend who appeared to have made the previous Facebook post wrote on her Fb profile: "I've got a virus! Please do not open messages I send you! Whatever posts you see today on my profile, I didn't make them!". Eleftheria realizes that something suspicious is happening and is very worried. She now immediately informs her father, who in turn immediately contacts his bank, which unfortunately informs him of various, unknown to him, transactions made in the last hour through his card with a total cost of 1000 Euros.*

Personal data being shared or inferred: Credit card details, father's personal data that are being used for online payments. Moreover "fake" personal data ("fake posts") was published on the Fb profile of Eleftheria's friend - and this was the cause of further data leakage for Eleftheria and her father.

Risks: Loss of money, cancellation of credit card, leakage of personal data to unknown third parties with unknown further consequences

2.4.3.3.1.9 *Elpida, a high school 17-years-old student, goes to a party organized by Orestes' classmate at his house. She is having a great time with lots of dancing, while many people are taking pictures of her (along with others) and upload the photos to Facebook tagging her. Some photos depict her in a state of great cheerfulness; Elpida, however, had not consumed any alcohol and was in a completely sober state (some photographic "frames", however, may lead to misinterpretations). The next morning, she sees on her Fb profile a lot of positive comments from classmates about how much fun they had last night. However, there were some comments, from people who weren't at the party, of the form "is that due to whiskey or vodka?". When she goes to school, she learns that another classmate has returned home from the party in a bad state due to heavy drinking. There was a relevant report from the parents to the school, which began to investigate the issue by discussing with those students who participated in the party and also by drawing information from social networks. Elpida heard that some 19-years-old boys (not being students) had brought several bottles of alcohol to the party, and that many of her classmates consumed alcohol, either in small or large quantities. However, even though she did not consume alcohol, she realized that both her teachers at school, and even her parents, have a hard time believing her, once they have learned what happened at the party in question and at the same time seeing some photos that can lead to unsafe conclusions.*

Personal data being shared or inferred: Image data (photos) from party - within a specific time frame, at a specific date, with specific classmates. From these photos, conclusions can be drawn on how the child spent the party time

Risks: The family/school environment get wrong impressions about the child, feeling of injustice, bad feelings due to a somehow prejudicial treatment.

2.4.3.3.1.10 *Eugenia, 15 years old, is a user of many social networks (Facebook, Instagram, Tik Tok), with public profiles, in which she regularly posts photos and comments from her everyday life. She also has no hesitation in making public personal information of her such as place of birth, place of residence, date of birth. She receives many comments, replies to them, she "likes" others posts whereas her posts are also "liked" by others, etc. One day, some of her friends inform her that there is a second profile on Facebook for which is completely believable that it belongs to her (it has the name "EvgeniaB"); this profile has many photos of her and many of the people from the contact list in her original profile has been also "connected" with this second Fb profile. One of her friends, Maria, was concerned because, through this second Fb account, Eugenia seems to have asked her, via chat, some very personal questions, as well as for some vacation photos from the beach (Maria "understood" that something is wrong from this type of conversation, because she thought that Eugenia would not ask for such things by this way). Eugenia is now very worried because she does not know, for all this time that this fake account was active, what actions/posts its user performed and what opinion may have been formed by others who communicated with this fake account, having the belief that they actually communicate with Eugenia.*

Personal data being shared or inferred: Any data that a child "posts" on social media – i.e., apart from full name/email address, photos, place of birth, place of residence, date of birth, personal life data such as friends, posts, likes, personal preferences.

Risks: Identity theft, the friends/school environment get wrong impressions about the child, feeling of anxiety/stress and possibly shame

2.4.3.3.2 Material in the form of questions regarding risks stemming from sharing personal data

List of risks related to publishing/sharing on social networks of various personal data types:

a) Home address: Information that may pose risks for monitoring/stalking by malicious individuals, risks for the physical integrity, for theft/burglary, causing feelings of fear/stress etc.

b) Phone number**:** Information that may pose risks for stalking/permanent annoyance, harassment, psychological pressure, extortion, etc.

c) The daily program**:** Information that may pose risks for monitoring/stalking by malicious individuals, risks for the physical integrity, psychological pressure, causing feelings of fear/stress etc.

d) Credit card information or banking account information**:** Information that may lead to loss of money, card cancellation (and therefore possible difficulties for the next period of time to make purchases) but also of other illegal actions by unknown third parties for which the child's family may "suffer" in order to accommodate the relevant impacts

e) Password or personal information that could allow password guessing**:** Information that may allow a malicious third party to gain access to child's personal data that she/he has not shared/published. It can

also lead to identity theft, interception of personal data from the child's family/classmates/friends, humiliation, cyber-bullying, extortion etc.

f) Photos/videos from vacation period**:** Information that may allow a malicious third party to comment negatively/abusively/insultingly and therefore to cause feelings of shame, psychological stress, sadness, depression, anger. Also, this information may be the "vehicle" for sexual harassment, with risks of physical integrity and abuse. There is also the risk that a malicious third party may share the child's photos, without the child's knowledge, on other platforms (with possibly illegal material). This information also reveals the place that the child is at a certain time period (and, accordingly, that she/he is not at home). Moreover, it is possible that other users may "upload" photos/videos depicting a child, without the child being aware of this - and even if the child is not a user of the relevant social network. So, even if a child does not use social networks or uses them very carefully, the above risks remain and can be caused simply by third party posts, as long as they do not ask for consent before uploading.

g) Photos/videos from walking around/having time with friends (from parties, café etc.): Information that may allow a malicious third party to comment negatively/abusively/insultingly and therefore causing feelings of shame, psychological stress, sadness, anger. Maybe the photos leave wrong impression – the child may also felt humiliated due to these comments. Moreover, it is possible that other users may "upload" such photos/videos depicting a child, without the child being aware of this - and even if the child is not a user of the relevant social network. So, even if a child does not use social networks or uses them very carefully, the above risks remain and can be caused simply by third party posts, as long as they do not ask for consent before uploading. This information could also reveal the place that the child is at a certain time.

h) Interests/ambitions**:** Information that may be exploited by a malicious third party, in order to approach a child as someone who has the same interests or who can help the child achieve her/his goals. His intentions may be a danger to the child's physical integrity, to emotional harm, to intimidation, or even extortion.

2.4.3.3.3 Material in the form of suggestions with good practices/tips for using social networks

- We don't have a public profile for everyone– if someone doesn't know us in person, there's no reason for him/her to access our profile
- We do not disclose/share, in our social network profile, information such as home address, telephone number, date of birth
- We do not accept friend requests from strangers, even if they "seem" interesting persons and do not raise any suspicion
- We do not chat with strangers – including commenting in strangers' posts – mentioning personal information of us, not even to simply mention our emotional state (eg, "I'm disappointed in my parents or school today" or "I recently broke up » etc.)
- We do not use abusive/offensive speech. Accordingly, we should have the expectation/requirement that others do not use such speech for us. We don't hesitate to delete posts and block users if their comments make us feel bad by any means.
- Before any post/action, even if it is a simple click in a "like" button, let's think about the following: "what information am I revealing with what I'm going to do? Am I sure that I certainly won't mind if other people, apart from those having in my mind right now, also see it?"
- We use strong (secure) passwords, which we protect from any disclosure to anybody (see below)
- We will not schedule a meeting with a stranger we met through a social network

2.4.3.3.4 Material in the form of “profiles” of malicious individuals (“who are these people?”)

- Criminals looking for children as victims to abuse (sexual or otherwise) or to collect highly personal photos/videos for their personal life and/or to share with others
- Criminals who are seeking for personal information in order to be able to carry out criminal acts that will bring them financial benefits (theft of money, financial fraud, burglaries, etc.)
- Jealous/vicious people who seek to morally harm some children and/or intimidate them; they usually belong to either the immediate or the wider social environment of the child.
- People who, although they do not basically carry out malicious actions, decide due to specific circumstances (e.g. strong personal disappointment, feeling of jealousy, bullying that they themselves have received) to hurt another child – e.g. to "get revenge" on her/him for an issue, according to their understanding of what a revenge means. They usually belong to either the immediate or the wider social environment of the child.
- People who spread fake news in order to cause disruption. This category may also include people who want to make other illegal actions such as, e.g., having financial gain through illegal means – e.g. by tricking children into clicking on a link that appears to correspond to a very important breaking news story, but the purpose is to install malware on the child’s device.

2.4.4 Learning Topic 4: Personal data exchange on social media and online messaging

2.4.4.1 Background

Personal data processing on social media and in chat platforms can be an extremely challenging task due to the vast amount of information involved, the constant evolution of privacy settings and policies, and the potential risks associated with data breaches and unauthorized access.

This section aims to increase students' understanding and awareness of personal information handling. It goes one step further with respect to the previous Learning Topic 3, emphasizing the importance of prevention and giving unique insight into the crucial considerations that are essential before exchanging personal data. By highlighting the potential consequences and risks, students are urged to make wise decisions about their online activities. The objective is to promote responsible behavior and enhance awareness of the importance of personal information protection in the digital age.

2.4.4.2 Learning objective

In this context, children should be made aware of the following points:

- Emails or messages on mobile or social media platforms that request information should be disregarded, if the identity of the sender is not known.
- The students need to acknowledge that different individuals have different privacy concerns, preferences, and behaviors towards their personal data. It is important to fully understand and respect these differences, acknowledging that each person may have their own expectations regarding the use of its personal information.
- The students need to respect the personal moments of a person, recognizing that individuals have a right to privacy.

- The students need to comprehend the boundaries between the virtual and real worlds, along with the potential consequences that delinquent attitudes and behaviors in one world may have to the other. For example delinquent attitudes and behaviors in the virtual world can lead to direct psychological and physiological effects in their real-world.
- The students have to handle the Sharenting' phenomenon dealing with its negative consequences in terms of privacy, autonomy and emotional well-being.

2.4.4.3 Learning resources

2.4.4.3.1 Material in the form of real life cases, options and feedback.

2.4.4.3.1.1 How do you react if you receive an email coming from an unknown or suspicious sender with the following content "Do you want to hang out after school at the park across street? Don't tell anyone about it".

A. Do you reply to this email? *Never respond to emails like this, you don't know the sender of the email*
B. Do you delete the email? *No, the deletion of the email could put burden on the authorities to further investigate this unwanted communication uncovering the identity of the sender behind an email address.*

C. Should you report it to someone you trust and who is in the position to report it to the appropriate authorities? *Yes, that is correct.*

2.4.4.3.1.2 How do you react if you receive a text (SMS) coming from an unknown or suspicious sender with the following content: "I have in my possession some photos that depict special moments of you and your beloved and intend to publish them if you refuse to me in person. Don't tell anyone about it."

A. Do you reply to this text (SMS)? *No, never respond to message like this, you don't know the sender of the text (SMS)*

B. Do you delete the email? *No, the deletion of the email could put burden on the authorities to further investigate this unwanted communication uncovering the identity of the sender behind an email address.*

C. Should you report it to someone you trust and who is in the position to report it to the appropriate authorities? *Yes, that is correct.*

2.4.4.3.1.3 You received a message in chat while you played your favorite online game, saying: *"*Please send me your mobile number to send you game cheats, tips and walkthrough guides*"*

A. You reply to this message. *No one in the game needs to know your mobile number.*
B. You don't reply to this message. *Yes, that is correct.*

2.4.4.3.1.4 What do you do when your friend asks for your username and password of your favorite online game?

A. It is okay for friends to share usernames and passwords. *No, never share your username and password with anyone other than your parents.*

B. You should not share your username and password with anyone other than your parents. *Yes, that is correct, it is generally not recommended to share your login credentials with anyone (only with your parents).*

2.4.4.3.1.5 You want to post or publish a photo showing other identifiable persons.

A. Publishing a photo of other identifiable persons requires their consent. You should reach out to everyone whose face is recognizable in the photo and get his or her permission. *Yes, that is correct.*

B. It is not necessary to get permission from all identifiable individuals in a photo before posting it. *That is not correct.*

2.4.4.3.1.6 You found out that someone posted either photos or videos of you on a social media platform without your permission. The photo is publicly accessible by anyone who has access to this content.

A. I don't do anything about it. *That is not correct*

B. I can reach out to them and explain why I am uncomfortable with them posting such a photo without your consent and ask them to take it down. *That is correct, if your request is not satisfied or is delayed, you should report it to someone you trust and who is in the position to report it to the appropriate authorities.*

2.4.4.3.1.7 You received a message in chat while you while you are scrolling on your favorite social media platform, saying: “Hi, we go to the same school, you look amazing. Do you want to hang out after school?”

A. The message was sent by a person unknown to you. *Yes, that is correct, even if someone says that you are going to the same school, this does not necessarily mean he/she is telling the truth.*

B. The message was sent by a trusted person. *No, that is not correct, some persons do not reveal their true identity.*

2.4.4.3.1.8 You received an instant message from a stranger on your favorite social media platform saying: “You're a grand prize winner!!! To get your gift click on this link.”

A. The message was sent by a person unknown to you. *Yes that is correct, these kind of messages aims to trick someone into clicking on a link or opening an attachment or download a malicious file in order to gain access to his/her personal information.*

B. The message was sent by a trusted entity. *No, that is not correct, these messages aims to trick someone into revealing personal information.*

2.4.4.3.1.9 You received a personal message from your mother on your favorite social media platform saying: “Your dad will drop you off to school 'just for tomorrow'”

A. The message was sent by a person unknown to you. *No, that is not correct.*

B. The message was sent by a trusted person. *Yes that is correct. Of course, you should talk with your mom in person or by phone to ensure that she sent the message*

2.4.4.3.1.10 You are having a good time with your friends at the party and many of these funny moments have been captured on photos and videos. In particular, one of your friends, Bill, was caught on camera doing something hilarious during the party. You thought it would be a good idea to share this video with other friends of yours who couldn't attend the party, and you trust and know they will enjoy it.

A. You are allowed to share the video. The recipients are close friends, and also please note that the video will not be posted on the Internet or publically presented. *That is not correct, be aware that photo and video-sharing can lead to a widespread leakage of personal data. In addition, sharing a video of your friend, Bill, requires his consent.*

B. You are allowed to share the video. The recipients are close friends, but you should make sure to mention it to your friend Bill. *That is not correct, be aware that photo and video-sharing can lead to a widespread leakage of personal data. Bill should not only be informed by you but he should give his permission for you to share the video. Please note that his consent must be freely given, specific, informed and unambiguous.*

C. You are not allowed to share the video, even if the recipients are close friends. *That is correct, sharing/publishing a video or a photo of other identifiable persons (like Bill) requires their consent. You should reach out to everyone whose face is recognizable in the photo and get his or her permission. Please note that their consent must be freely given, specific, informed and unambiguous.*

2.4.4.3.2 Social media security and privacy settings, background and recommendations

Security and privacy settings on a social media platform allow users to control the access to their profile and personal information. An indicative list of security settings that are commonly found on Social Media Platforms is the following:

a) Privacy settings: Users may opt to have their profile as either private or public, allowing them to control the visibility of their personal information. In particular, they should be able to customize the privacy settings for their posts, messages, and friend requests, allowing them to control who has access to these aspects of their profile. In accordance with the Privacy by Default data protection principle (art. 25 of the GDPR), applications and online services default settings (initial settings) should be privacy friendly, thus allowing the least of personal data processing.
b) Request Management on Social Media: Users have control over who can send them friend requests or follow them, enabling them to manage their social circle. For example, they can enable accepting friend request from "Friends of Friends" and disable friend requests from public.
c) Blocking and Reporting: Users should be able to block or report accounts they consider suspicious or abusive. To this end the Social Media Platforms should provide a blocking and reporting functionality where users can take action against accounts they deem suspicious or engaging in abusive behavior. For example, they can report comments or posts with illegal content or illegal source promotion (insults, prohibited political propaganda, hate speech, and violence etc). This important feature promotes a safer and more positive online environment by allowing users to block or report such accounts, thereby addressing inappropriate or harmful conduct and ensuring a better online experience for everyone.

You want to create an account on a social media platform or on a gaming platform and you need to limit the information available to the other accounts. Please manage the privacy settings of your account, following the following recommendations:

- What should you use as a username? You should use a pseudonym or a nickname and NOT your real name.
- Who can see your profile posts, timeline's content and status updates? Only your friends can see your profile posts, timeline's content and status updates, NOT anyone
- Who can send you direct messages? Only friends, NOT everyone.
- You want to play an online game and looking for other players. With whom can you play? You should accept to play only with your friends, NOT with anyone
- Who can access and see your profile details? Only your friends can see your profile details and NOT anyone

2.4.5 Learning Topic 5: Online profiling, targeting, advertising and influence

2.4.5.1 Background

The GDPR defines profiling in Article 4(4) as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is a procedure which may involve a series of statistical deductions. It is often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar. (see [4]).

Behavioural advertising is advertising that is based on the observation of the behaviour of individuals over time. Behavioural advertising seeks to study the characteristics of this behaviour through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests. Behavioural advertising entails the tracking of users when they surf the Internet and the building of profiles over time, which are later used to provide them with advertising matching their interests. Online advertising is a key source of income for a wide range of online services and is an important factor in the growth and expansion of the internet economy. However, the specific practice of behavioural advertising raises important data protection and privacy related concerns. Basic internet technology allows advertising network providers to track data subjects across different websites and over time. Information gathered on the surfing behaviour of data subjects is analysed in order to build extensive profiles about data subjects' interests. Such profiles can be used to provide data subjects with tailored advertising. Most tracking and advertising technologies used to deliver behavioural advertising use some form of client-side processing. It uses information from the user's browser and terminal equipment. In particular, the main tracking technology used to monitor users on the Internet is based on "tracking cookies". Cookies provide a means to track user browsing over an extensive period of time and theoretically over different domains. There is an obligation to obtain data subjects' prior consent to engage in behavioural advertising: pursuant to Article 5.(3) of the ePrivacy Directive, an ad network provider who wishes to store or gain access to information stored in a user's terminal equipment is allowed to do so if it has provided the user with clear and comprehensive information and it has obtained the user's consent to the storage of or access to information on his or her terminal equipment (see [6]).

Some material on how to explain the online advertising and influence ecosystem to children were inspired from the Australian parenting website content [9], which includes information on how advertising influences children and teenagers.

2.4.5.2 Learning objective

Children should be able to understand that they leave "traces" when browsing the internet that reveal their personal data and can be used to sketch their portrait in all aspects of their virtual or physical life (place of residence, shopping choices, places of entertainment etc.). Awareness will be raised on the risks of using applications on smartphones: special reference to the electronic applications of mobile phones, in relation to the tracking possibilities through e.g. the permission model in android. They will get insights on the real cost of "free" online services, in exchange for the use of their personal data and knowledge on how online services work with monetization of their personal data. They will also be shown the application of the basic concepts of AI, Machine Learning (e.g. chatbots, targeting).

The overall goal is to help children understand how navigation works as a means of leaving online traces and the risks of forming a detailed profile. They should also be aware of the available means of protection such as refusing tracking, cookies or customizing the settings for private browsing.

2.4.5.3 Learning resources

2.4.5.3.1 Examples of questions and feedback related to influence from online media content

a) Influenced by online media (directly and indirectly)

Can you think of how you are influenced by online media?

Direct influence: For example, advertising often targets children of all ages. This means that children are increasingly aware of product/service brands and images.

Indirect influence: For example, this can include images and content on Instagram, Snapchat, TikTok and YouTube. It may also include violent or (or sexual) images and vulgar language in informational content sites, video games and song lyrics. This type of media influence can suggest/give the impression to children that certain ways of behaving and looking are 'normal'.

b) Influence: Self-image and body image

Can you imagine how social media and advertising can affect the way you see yourself, your image? For example, you regularly see staged and filtered images on social media, everyone is perfect! How can one be affected? You may feel that you are not good enough, you may think that you are not interesting/cool enough, you may think that your daily life is boring. If you often see unrealistic "thin" or "muscular" body types. These images can be even more powerful when accompanied by messages such as 'thin is beautiful'. How can one be affected? You may think that only you (and a few others) have "flaws" in their bodies, you may change the way you perceive your body image, it can affect your eating behaviour.

c). Influence: Health and lifestyle

Online social or news media can influence the health and lifestyle decisions you make. For example, media messages and content can make it seem 'normal', 'cool' or 'advanced': to eat junk food, to smoke, to vape, to drink alcohol, to take drugs, to self-harm, treat others badly or accept being treated badly

4. Influence: Attitude as citizens

To be a responsible citizen, you need reliable and good quality information. But online social or news media is sometimes used in a negative way, especially during the pre-election period by presenting false standards or misinforming users.

What is Fake news? Fake news or false news is a type of yellow press or propaganda that is made with intentional misinformation

What are Deep fakes? They are videos that, with the help of artificial intelligence, replace the face of the person depicted with that of another person, with absolute accuracy in capturing the image and voice, in order to deceive and manipulate the public, leaving them to believe that it is a real image.

For example, fake news or deep fakes may influence you to believe misinformation about a politician, public figure or celebrity or/and may promote discriminatory or hateful attitudes towards groups of people.

2.4.5.3.2 Paid posts, the business model explained

a) Do you know that influencers and some celebrities are paid to advertise the products they endorse? How can one tell the difference between influencers and ordinary people – or even celebrities – who post videos and other content for fun? Influencers must declare if they have been paid using hashtags like #ad or #sponsored or words like "ad" or "sponsored" in their posts. => it is good to watch out for these signs! (Example from such a post)

b) You can choose one of the YouTube channels or Instagram accounts you follow. Do you know or can understand: Who is behind it? What is his motivation? What do they want from you? How does it make you feel? Do they want you to feel this way? For what reason?

c) You can do the same for celebrities and influencers. Ask yourself: Why do I like these people? Are they presented in a realistic manner? Is it like this in real life? What values does this person project or have? How does this person make me feel about myself? Why is this person telling me about this product or activity? Are there indications that this person is an influencer?

2.4.5.3.3 Understanding advertising

a) How does advertising sell ideas and products? You can tell from the ad: Does this ad associate the product with a certain type of lifestyle? How does the product make you feel? What messages does this ad send about how people should look, wear, do, eat and drink?

b) During an election campaign, you can see political news and memes. You may ask yourself: What ideas are promoted in this news or meme? Who wrote this story or made this meme and why? How might this meme influence voters during elections?

c) Who will see which ad? Is it “random"? Why would your parent or a friend see other ads, other suggestions when they visit the same website? Because we do leave "traces" on the internet, give information so that those who want to "target" us can "get to know" us, sketch our portrait/profile. The more they know the more "targeted" they are and the more successful the ads are.

2.4.5.3.4 Tracking and behavioral advertising example

Traces while browsing the internet reveal personal data, such as age, place of residence, what we "like" on the internet, how we have fun, what Hobby, what ideologies, what preferences (music, cinema, group, games, etc.) or even our financial status. Tracks are used in Behavioral Advertising. What is Behavioral Advertising? Using information about the user's browsing in order to display advertisements tailored to his interests or targeted to a specific group of users. How this is all organized? Advertising Network: Connects websites with advertisers, who collect and use information from visits to websites that participate in that network

Tools: Cookies and more. The ad is shown to whoever pays more for a guest profile.

Example: *Your mom visits a celebrity news site. She always does "accept all" for cookies. Your dad, at the same time, is viewing the same website (and he always does "accept all" for cookies). So do you, with your tablet (and you almost always accept everything, you're in a hurry). The website has many ads, on the right, one below the other. The family sits on the couch, each with their own laptop or tablet, and compare what ads each sees. They have absolutely nothing to do with each other. They are completely different, for completely different products. Same page, same moment...* Yes, what has happened is that because you are different "targets", you have been "targeted" by different companies. They know you because of the traces you leave, and because you have allowed by "accepting all" cookies.

2.4.5.3.5 Cases regarding cookies acceptance and rejection and recommendations

You help your mom look for a present for your grandpa. His doctor recently told him that it is good to walk a lot, every day. You are looking for sports shoes. You are visiting the website of an online store. The cookie banner appears and you click 'Accept all' because you are in a hurry. You are searching the internet for an electronic watch that counts steps and heart rate. You visit your favourite sports newspaper, 'agree' to cookies and read what interests you. You “like” a video with a snapshot of your favourite team's match. The next time you log on to the internet, you are constantly being shown ads for sportswear and nutrition!

What happens every time you accept cookies? Cookies, which are small files with information about your navigation, are placed on your device. Based on this information, advertisers infer what you prefer, what you are interested in and "bombard" you with ads that "fit" you.

Of course, the conclusions may not be correct, but even if they are correct, surely you want someone to know your interests or your preferences?!…

What can you do? Click reject all cookies, if this option is available in the cookie banner. You close the cookie banner box without any other action, if this option exists. If there are none of the above, then check the 'settings' option and state there what you do not accept. You do not continue browsing on websites that only have the option to accept cookies. You regularly delete cookies from the browser you use

If you constantly see videos, ads, posts about a topic, and you haven't paid attention to privacy settings and cookies: A. You may be bombarded with information on the same topic B. Think about influence: It will become more and more intense. The more you see, the more are suggested to you. C. The possibility of becoming something like an "addiction" and being badly affected is high D. The same can happen with adults? Of course!

2.4.5.3.6 Smartphone applications examples

Apps should limit their access to sensors (location, motion, camera and microphone) and locally stored data (images, contacts) to a minimum, and only when clearly relevant to the proper operation of the app.

Examples with Yes/No

a) You download a "flashlight" application, to make the mobile phone brighter in the dark. The flashlight application asks for access permission for location, movement, camera, microphone, pictures and contacts.

A. It is justified, they know how it can run, since the code writes it (No)

B. It is not justified, I should not accept it, what do these have to do with the lens (Yes)

C. Find out if it explains it somewhere, otherwise I'll download another app (Yes)

D. Did it install a virus? He tells us strangely... I don't trust him (Yes)

b) You download a weather app that asks for location to provide local weather information

A. No, I won't give access, I don't want the app to know where I am (Yes)

B. Better, he will tell me right here where I am what the weather is like (No)

C. But isn't the selection of the city I've made enough? Why should he know exactly where I am? (Yes)

c) Activity: See the website that an x character enters on youtube. Let's say you don't know him. Can you put yourself in the shoes of an advertiser, youtube itself? What kinds of conclusions can be drawn about the unknown x? What can we learn about character by looking at the data? Would your classmates draw the same conclusions as you? Can you compare what each of you imagined? Inferences are not always accurate, but they can be used to judge a person or make decisions about a person.

2.4.6 Learning Topic 6: Privacy policies

2.4.6.1 Background

Privacy Policies serve a few specific purposes: Privacy Policies compel businesses to act more transparently. A Privacy Policy gives individual website users and consumers more control over their personal information and can help build trust between website/apps owners and users because both parties know what is expected of them. Privacy Policies strike a balance between the rights of individuals to control who they share data with, and the need for businesses to process some personal information for commercial purposes. The goal is that the users, as personal data subjects, are fully informed about the circumstances and the conditions that their personal data is processed, so that they can adjust their preferences and know how to exercise their rights. Children, as users should also be able to understand the basics in a privacy policy.

Note that the GDPR puts emphasis on the transparency of the processing (art. 13 and 14); all data processes should be clearly defined, in a comprehensible and easily accessible way, to all data subjects. The GDPR explicitly determines which exactly pieces of information need to be conveyed by the data controllers towards the data subjects; therefore, the content of a privacy policy actually reflects how the data controllers are compliant with these legal provisions.

2.4.6.2 Learning objective

Children should know how to:

- adjust their privacy and settings for online services (when we have not activated the privacy settings in the social networks we use, anyone can access our personal data)

- assess what data is used by each online service

- make decisions about sharing information with each application they use

- recognize when they provide their personal information for free services

- describe how the sites generate revenue.

- read and understand the terms of use and privacy policy before using the online services.

2.4.6.3 Learning resources

Example privacy policy (e.g Snapchat https://values.snap.com/el-GR/privacy/privacy-policy)

- Did you find in the text who the controller is? What are the details of the company that owns the application, address, email, etc.? Were they easy to find?
- Does the text state for which purposes the personal data is processed?
- What are the types of personal data?
- Does it justify why this data is necessary?
- Is the information on how someone can exercise their rights clear?
- Does it state what rights users have?
- Are there relevant forms for exercising the rights?
- Is the language correct, simple and understandable?
- Is there an easy way to search for privacy information?
- Is the information about the privacy settings complete?

- Is all the information also in Greek?
- Is it easy to read and understand the main points of the policy? (E.g. is it a long text or a layered text? Does it have illustrative pictures?)
- Is there a reference to minor data processing issues?
- Are there ways to contact the company for data protection issues?
- Does it state which person is designated as Data Protection Officer?
- Does the policy state which country and which Data Protection Authority is responsible for the enforcement of the GDPR for this specific case?
- Does the cookie policy give instructions on how one can avoid their use and what are the consequences? Do you think the practice he mentions is correct?
- Can you check if the privacy policy is also available within the app and how?

2.4.7 Learning Topic 7: Deceptive patterns

2.4.7.1 Background

Regarding the data protection compliance of user interfaces of online applications within the social media sector, the data protection principles applicable are set out within Article 5 GDPR. The principle of fair processing laid down in Article 5 (1) (a) GDPR serves as a starting point to assess whether a design pattern actually constitutes a "deceptive pattern". Further principles playing a role in this assessment are those of transparency, data minimization and accountability under Article 5 (1) (a), (c) and (2) GDPR, as well as, in some cases, purpose limitation under Article 5 (1) (b) GDPR. In other cases, the legal assessment is also based on conditions of consent under Articles 4 (11) and 7 GDPR or other specific obligations, such as Article 12 GDPR. Evidently, in the context of data subject rights, the third chapter of the GDPR also needs to also be taken into account. The EDPB has recently published the Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognize and avoid them.

2.4.7.2 Learning objective

Users of social media platforms might come across so-called "deceptive patterns" in social media interfaces that infringe on GDPR requirements. It is important that users understand what a "deceptive pattern" is, in what forms it could occur, and how to avoid it.

The goal is to make students aware of the use of deceptive patterns on the internet, especially on social media platforms, and the risks they entail with regards to personal data protection, as well as to give to them hints on how to avoid them.

2.4.7.3 Learning resources

"Deceptive patterns" are considered as interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data. Deceptive patterns aim to influence users' behavior and can hinder their ability to effectively protect their personal data and make conscious choices. Data protection authorities are responsible for sanctioning the use of deceptive patterns if these violate the GDPR requirements. The deceptive patterns can be divided into the following categories:

a) Overloading means users are confronted with an avalanche/large quantity of requests, information, options or possibilities in order to prompt them to share more data or unintentionally allow personal data processing against the expectations of the data subject. The following three deceptive pattern types fall into this category: Continuous prompting, Privacy Maze and Too Many Options

b) Skipping means designing the interface or user experience in a way that users forget or do not think about all or some of the data protection aspects. The following two deceptive pattern types fall into this category: Deceptive Snugness and Look over there

c) Stirring affects the choice users would make by appealing to their emotions or using visual nudges. The following two deceptive pattern types fall into this category: Emotional Steering and Hidden in plain sight

d) Hindering means obstructing or blocking users in their process of becoming informed or managing their data by making the action hard or impossible to achieve. The following three deceptive pattern types fall into this category: Dead end, Longer than necessary and Misleading information

e) Fickle means the design of the interface is inconsistent and not clear, making it hard for the user to navigate the different data protection control tools and to understand the purpose of the processing. The following two deceptive pattern types fall into this category: Lacking hierarchy and Decontextualising

f) Left in the dark means an interface is designed in a way to hide information or data protection control tools or to leave users unsure of how their data is processed and what kind of control they might have over it regarding the exercise of their rights. The following three deceptive pattern types fall into this category: Language discontinuity, Conflicting information and Ambiguous wording or information

2.4.8 Learning Topic 8: Identity protection and account security

2.4.8.1 Background

One of the key challenges in the digital world is to ensure secure access to services while effectively protecting users' personal data. In this context, it is essential to address the strict privacy requirements imposed by the existing legal and regulatory framework (e.g. The General Data Protection Regulation (GDPR), e-privacy legislation) that minimize the potential risks and negative impacts associated with unauthorized access or misuse of personal Information.

The objective of this section is to raise awareness about fundamental principles of privacy, including anonymity, unlinkability, pseudonymity, and partial Identity. In this context, it aims to provide a better understanding of the distinctions between these various aspects, emphasizing their importance and relevance in ensuring the protection of personal information. Moreover, since protection of an electronic account is strongly related with the protection of passwords, this topic also puts emphasis on the importance of protecting passwords.

The fundamental privacy aspects that must be addressed are the following:

- Anonymity, which allows individuals to use a resource or service without revealing their personal identity.
- Unlinkability, which ensures that a user may interact with resources without these being linkable to the same individual
- Pseudonymity, which allows a user to use a resource or service without revealing their real identity, while still being accountable for their actions.
- Partial Identity, which includes a subset of data (such as first name, last name, address, age, gender etc) from a complete identity. A user should have the capability to manage and maintain multiple partial identities, where a complete identity represents the union of all data associated with an individual.

The importance of using strong credentials, in order to improve the security of personal data processed through children accounts using online services should be also be pointed out, as it is crucial for children's online privacy protection.

2.4.8.2 Learning objective

Children should be aware of, despite the fact that they should be very cautious when providing personal information and, if it is not necessary, they should not reveal either their real name, full anonymity is difficult to be achieved. Moreover, children should be aware of the importance of passwords. The message should be that a password has, in a sense, the same importance as the key to our house: it must under no circumstances fall into the hands of third parties. This applies to any password, regardless of the application we use it for.

The message is that as long as we don't give our password to third parties, we are unfortunately not safe: although it is necessary, it is not enough.

2.4.8.3 Learning resources

2.4.8.3.1 Identity protection cases and recommendations

- You want to create an account on a social media platform. As part of the Account creation process, you need to provide personal information like username, first name, last name, age, email address, mobile number, bank details, credit card number, gender, nationality, height etc. Some are mandatory, while others are optional.

  You should provide only the minimum data necessary for the creation of the account and NOT provide all the personal information requested (both required and optional).

- You recently wrote a post on your favorite social media platform. Here's what you shared: ”the bleached-blond hair girl sitting next to me in class is wearing a very simple and loose shirt.”

  This is a post that indirectly reveals the identity of the person. The person to whom the specific post refers can be easily inferred, even without explicitly stating their name. Unlinkability principle should be fulfilled

- How do I react to a post or a comment published by a stranger under the nickname “friend” that contains illegal content (e.g. abuse, hate speech, and violence)?

  You can request directly to the person to delete the post and remove the illegal content. If your request is not satisfied you should report it to someone you trust and who is in the position to report it to the appropriate authorities or the platform where it was published.

2.4.8.3.2 Password leakage cases

With respect to the passwords, there are even greater risks of their leakage, compared to the key to our house: even if we do not "lose" it, it can still end up in the hands of third parties - and even without being aware of this (whilst, if we lose the key to our house, we will realize it). For example:

I. A malicious third party may guess our password (e.g. based on our personal information, which he already knows; even if such personal information is not a priori known, there may be the case that this malicious party is in a position to learn it).

II. Even if our password is not related to our personal information, a malicious third party may be able to find it out, because it is somehow easily predictable – and, thus, "easy to find" (even if this party does not have any prior communication with us).

III. A malicious third party may "trick" us so as to let us to communicate our password to him by ourselves; this could be done through either, e.g., sending misleading/phishing messages or secretly monitoring our device/communications.

The cases I and II indicate that we should be very careful when we choose a password; a strong password is a password for which the threats I and II cannot be implemented in practice. The case III indicates that we should be very cautious in order to protect the password that we have chosen.

2.4.8.3.3 Guidance on how to choose a strong password

When a password can be considered as strong?

Strong (i.e., secure) passwords are those that cannot be "guessed", either by a human (who can guess, infer or "fish" personal information about us), or by a computer (which can perform automated tests, checking for potential passwords). This practically means that:

- The password should not be related with our personal information (e.g., with the date of birth, the name of loved one/pet, loved band, football team, etc.)

  Examples of insecure passwords, not fulfilling the above principle, are the following: Jenny2005, panagiotis19092010, #19092010#, panathinaikos2012!, Antetokounmpo!, JustinBieber100

  - Activity 1: Could you think of other “bad” passwords of the same type?

- The password must consist of at least 8 characters.

  Examples of insecure passwords, not fulfilling the above principle, are the following: Abc15, qeAD, asdf!, ks2012

  - Activity 2: Is it possible that any of the above passwords also violate the first principle with respect to relation with personal information?

    The password ks2012 could have been chosen by a student being born on 2012, whereas her/his first name and last name could start by the letters “K” and “S” respectively. Similarly, the password Abc15 could have been chosen by a student being born on the 15th day of a month. Similarly, if the name’s initials of the child are present in either the word qeAD or asdf!, then these passwords also violate the same principle. In any case though, even if they do not violate the first principle, they still constiture insecure passwords.

- The password must not be a word (or combination of words) that exists in a language dictionary or that is a proper noun: this applies even if it is "enriched" by other characters.

  Examples of insecure passwords, not fulfilling the above principle, are the following: Victoria, Password1234, mylove2000, school5!

- Activity 3: Could you think of other “bad” passwords of the same type? Check also the “bad” passwords that are given as examples for the previous cases; does any of them also violate the present principle?

  The aforementioned passwords “Jenny2005”, “panagiotis19092010”, “panathinaikos2012!”, “Antetokounmpo!”, “JustinBieber100” also violate this principle.

- We need to think more broadly: could a third party "guess" our password, even if the password satisfies the above principles?

  To illustrate this, it is important to know that every year, users’ passwords that were leaked because they were predictable are published (to see them, just search on the Internet with the search term "most common passwords"). You might be surprised by some of these passwords, because you might have thought they were safe. Examples of such "bad" passwords that were leaked (for the year 2022): abc123, password, qwerty, 123456789, col123456, 110110jp, 1q2w3e4r, pass@123

  - Activity 4: Find such a list of commonly used passwords that have been leaked. Do you consider any of them as secure? (of course before finding out your list). Do you find passwords in this list that also violate any of the previous principles?

Recommendations: How to choose a strong password?

- It is important to ensure that the password we choose not only satisfies all the above principles but that it also contains not only alphabetic but also numerical characters (e.g. "0", ""9") as well as other symbols (e.g. "!", "# » etc.).
- However, the password should also be easy to remember. We should not write it down on paper or in a notebook app, etc. in order to be able to recall/remember it.
- To achieve all these goals, a proper way to proceed could be the following:
  - First, select a sentence that's memorable to you.
  - Then, assign each word of the sentence a series of characters related with this word.
  - Finally, combine the result with some personally memorable tricks to modify the resulted sequence of characters into a password satisfying all the desired principles.
- An example (see [2]) is the following:
  - Consider the phrase “When I was seven, my sister threw my stuffed rabbit in the toilet” as an easily memorable phrase
  - Assign each word with its first letter, while replace the word “seven” by the number “7”
  - Place a “!” at the end of the phrase
    - The result is the password: WIw7,mstmsritt!

By these means, we have, an unpredictable (strong) password, that when we need to enter it we type it very easily since it is easily memorable (as long as we have the starting phrase in our mind), without having to write it down to memorize the password itself.

- Activity 5: Can you “construct” such a strong password? Present it in the class, explaining why it is strong and easily memorable for you. Do not forget: after this task, this password should be never used by you!

2.4.8.3.4 Guidance on how to protect our (strong) password

It is not enough to choose a strong password to be sure that it will not fall into the hands of third parties. We also have to make sure that no one else will finds it out or will be able to eavesdrop it – not even our close friends!

Main rules that should be followed:

- We do not spread it orally to anyone
- We do not record it anywhere (i.e., notebook, post-it paper, etc.)
- We do not "save" it in a digital file (e.g., in a .txt file or in some "smart" application, etc.)
- We do not share it through chat communications or through any electronic message (e.g., sms, email, Viber message, Whatsapp message etc.)
- When we are being asked by an application, while entering our password, to "save it for the future so there will be no need to retype it", we choose "NO".
- We regularly change our password (e.g., every six months)
- We change the password immediately if we have the slightest suspicion/indication that it may have been compromised. If we use it in more than one application (which is good to avoid as a practice), then it must be also changed in all these applications.
- When we want to visit a website that will require from us to enter our password, we cautiously type by ourselves the URL (address) of the site. We do not trust other "sources" that they claim to provide direct access to this website.
    - We do not click on links that (supposedly) correspond to links for this website, in case that these links come from e-mails or pop-up windows.
    - If our friend sends us such a link via chat, we first confirm by talking to him directly that she/he indeed sent this link and that it is valid
- We never enter our password in insecure websites – that is, websites whose address starts with "http" and not "https", or websites for which the browser displays security warnings.

2.4.9 Learning Topic 9: Personal data subject rights

2.4.9.1 Background

In today´s society, personal data are processed by public and private entities, during many activities, for a wide array of purposes and in many different ways. Individuals may often be in a disadvantaged position in terms of understanding how their personal data are processed, especially considering the technology used in each particular case. In order to protect personal data of natural persons in these situations, the GDPR has created a coherent and robust legal framework, generally applicable with regard to different types of processing, including specific provisions relating to data subject rights. The children are independent data subjects and therefore they are themselves holders of the rights provided for by the GDPR (see articles 15-22 GDPR) which they can exercise through their legal representatives (such as those who exercise their parental care).

The rights that most commonly concern children as data subjects are the right of access, the right to erasure, the right to object and the right to rectification. The said rights are exercised by the children through their legal representatives, as mentioned above, to whom they must address themselves, while they must also find their educators as helpers (teachers and professors) for any directions they need to exercise their aforementioned rights. From the above it becomes clear that both the children themselves and their legal representatives

(usually their parents) as well as their teachers, must be aware of the action of the Personal Data Protection Authority, in order to ensure the most effective protection of children's rights as data subjects.

2.4.9.2 Learning objective

Children should be aware, in particular, of their above rights as independent data subjects. They should also know the exact content of these rights, what the latter mean for them, when and how they can exercise them.

To understand the rights in question and their content, as well as what each of them cures so that the students can orientate themselves on how to react depending on the situation they are facing.

At the same time, children will understand when and how they can appeal to the Personal Data Protection Authority, to protect their rights as data subjects.

2.4.9.3 Learning resources

2.4.9.3.1 Data subjects rights definitions

- Right to information: It is the right to know who is processing your data, which data specifically and for what reason. Organizations that process your data must provide you with clear information in plain language.
- Right of access: You have the right to request free access to your personal data held by an organization.
- Right to rectification: You have the right to request the correction of inaccurate personal data and the completion of incomplete information.
- Right to erasure: You have the right to request the erasure of your personal data, under certain conditions, such as when the data is no longer necessary, you have withdrawn your consent, the data has been unlawfully processed, etc. As part of this right, you have the possibility, under certain conditions, to request that your personal data be deleted from a list of search engine results.
- Right to restriction of processing: You have the right to request the restriction of processing of your personal data when its accuracy is disputed, the processing is unlawful, the data is no longer needed by the controller, you object to automated processing.
- Right to data portability: You have the right to request the transfer of your data to another controller.
- Right to object: You have the right to object to the processing of your personal data by an organization, provided that the public interest is not affected.
- Right to non-automated individual decision-making, including profiling: You have the right to object when a decision concerning you is based solely on automated processing, including profiling, and that decision produces legal effects or significantly affects you.

2.4.9.3.2 Examples and cases regarding the definitions of rights

Matching activity: Do you know your rights under the General Data Protection Regulation (GDPR)? Match each right with the possibility that provides you.

Right under the GDPR	Possibility that provides the corresponding right

Right to restriction=> 3	1.You can request the deletion of your data if they are no longer necessary
Right to rectification => 7	2. You can request and receive a copy of your personal data (which a company or public service keeps in its records about you)
Right to erasure => 1	3. You can ask to temporarily stop the use of your personal data (to "lock" your data)
Right to be forgotten => 6	4. You can request that your data aren't used for advertising purposes by a company that sends you advertising messages
Right to access => 2	5.You can request the transfer of your data to another company
Right to object => 4	6. You can request to delete the search engine results when a search is based on your first and last name
Right to data portability=> 5	7. You can request the modification of your personal data if you think that they have an error or inaccuracy

Question activity: How long can one wait to get a response to a right that had exercised?

A. One day B. It is not defined C. For one month maximum D. For 10 days maximum

Option C is correct. According to Article 12 para. 3 of the GDPR, the Data Controller has in principle one month from the receipt of the relevant request of the data subject in order to respond. The aforementioned deadline can be extended to 2 more months, as long as there is relevant information about the extension within the first month from the submission of the request, including the reasons for the delay (see article 12 paragraph 3 of the GDPR).

2.4.9.3.3 Material in the form of real life scenarios: data subject rights

2.4.9.3.3.1 *Right to access*

During swimming practice, two students, members of the same swimming club, argue because they dispute the total number of swimming events each of them has won in the last year, since the one with the most wins will represent the club in a European match. The data in question are recorded in each person's record, which is kept in the archive of the club's Secretariat. How will they have a secure image of their victories? As their parents arrive and find them disputing, they head to the secretariat, asking each other for information about each other's matches. The secretariat of the swimming pool as Controller explains that each of the fellow athletes has indeed the right *to address to the Secretariat through his parents (or his legal representative) exercising in writing a* right *of access to the sports register that concerns him individually, and not to a register of a third party, where the matches they participated in per year and the scores they achieved as well as the victories they scored are listed, requesting also to take a copy of the records in question. In this case, each minor athlete applies through his parents to the secretariat of the data controller (swimming club), where his data, which are of interest to him, are kept, as long as they concern only him.*

2.4.9.3.3.2 *Right to erasure*

A high school student has registered with his email address on the website of a well-known chain of sporting goods stores to receive newsletters. He gave his personal data in question on the basis of consent, which is the only legal basis for the processing in question, being excited immediately after ordering a snowboard from the company in question, with the help of his parent. However, disappointed after receiving the said board he ordered as it was defective (scored and unpolished on its lower surface) he wishes to stop receiving the above newsletters from the company as well. We see the 17-year-old student purchases the board from his PC in the presence of his mother, and in the final phase of completing the purchase, "clicks" on the option box to receive the newsletter of the specific company. After a few days it seems that when opening the package that he receives from the

company, the board on the bottom surface of it has scratches and it seems that it is not as smooth as it should be because it has not gone through the waxing process. The above defects will be reported by the student to his mother who is present at home when the package is opened. Answering a question from his mother about what he would like to do, the high school student states that he will return the product but since he no longer wishes to have any information and any contact with this particular company precisely because of their unreliability, he informs that he doesn't want to receive the newsletters he has chosen to be sent to him. He wonders how he will achieve this.

Answer: The student concerned can exercise the right to erasure by using directly the contact details that the controller must have posted on his website for the data subjects.

2.4.9.3.3.3 *Right to rectification*

A student of the 6th grade shortly before the publication of the school newspaper that is posted on the school website and has a great impact, receives the court decision of recognition of a child that he was expecting, which results in the change of his surname. Therefore, through his mother, he submits the decision in question and the other necessary documents to the school's Secretariat in order to make the appropriate changes to the student's personal data. However, 2 months later the school newspaper is published in which the student is listed as a member of the editorial team under his old surname.

What right*(s) will be exercised before the Principal of the Primary School to remedy the error in question regarding the entry of his family name?*

Dialogue: The child appears with his mother in the school Secretariat

Mother: We are providing you with the court decision recognizing X from his father and all related documents, from which it follows that his surname has been changed to P. With the relevant update of my son's record, which we also request in writing from you, we expect to carry the new last name in the school newspaper that will be published and where X will be mentioned as a member of the editorial team.

Secretariat: Thank you. We will take the relevant actions.

2 months later, the school newspaper is posted on the school's website and X, holding it in his hands, realizes that in the list of 6th grade students, he is listed under his old last name. Therefore, going home, he worriedly informs his mother about the fact in question.

X: Mom, the school newspaper mentions me with my old last name, while we submitted all the necessary information to the Secretariat's Office. How do we fix it?

Answer: The student can exercise through his legal representative (parent, guardian, etc.) the right to object in order to express his opposition to this processing, i.e. to the publication of his name with an incorrect surname, which concerns his particular family situation and subsequently to exercise the right to rectify his surname, in order to restore the above inaccuracy. You can request directly to the person to delete the post and remove the illegal content (That is correct). If your request is not satisfied you should report it to someone you trust and who is in the position to report it to the appropriate authorities or the platform where it was published

2.4.9.3.3.4 *Right to erasure*

A high school student, navigating to his account on a well-known video posting platform (tik tok), realizes that there is an account with his own photo and a variation of his own name (fake account=fake profile). He finds out that the other published information mentioned in this open to third parties (public) profile of this false account is identical to his own. However, the student does not have another account and has not made the posts that are visible on that account he identified. How will he solve his problem?

Answer: First of all, he must inform his parent/guardian and then, if necessary, inform the Cybercrime Prosecution. At the same time, for the treatment of the problem he identified, he can exercise (with the help or in any case after informing his guardian) the right to erasure of the account in question by addressing a relevant request to the platform by completing the corresponding form available in the privacy policy of the platform in question (under "your rights and choices").

In particular, by choosing the right of erasure, he can choose, within the framework of the aforementioned right, to report the suspicious account he has identified as a fake one. The above navigation path is reflected in the following links: https://www.tiktok.com/legal/page/eea/privacy-policy/el-GR, https://support.tiktok.com/en/safety-hc/report-a-problem, https://tiktokimpersonationusca.zendesk.com/hc/en-us/requests/new

2.4.9.3.3.5 *Failure to satisfy a right– appeal to the Authority*

In case that the Data Controller does not respond within one month from the submission of the requests regarding the exercise of a right, or if it responds partially/unsatisfactorily, there is the possibility for the student to appeal through his parent/guardian to the Data Protection Authority by submitting the relevant complaint of violation of a right: https://www.dpa.gr/el/syndesi/polites/kataggelia/paraviasis_dikaiomatos

With the submission of each complaint, in addition to the critical facts that must be stated, all the documents that prove the allegations stated in the body of the complaint are also submitted. Contact information for the Authority: Data Protection Authority, 1-3, Kifisias, P.C. 115 23, Athens, Tel.: 210-6475600, email: contact@dpa.gr.

2.4.9.3.4 Examples and advice on data subject rights

Example 1: Which of the following I cannot demand when I exercise the right of access before someone who keeps my personal data:

a. copies of recorded calls of mine.

Wrong answer. The recorded conversation of the person exercising the right *of access in order to obtain it constitutes his/her personal data. This is because it includes information that concerns the data subject and makes them directly identifiable (such as a reference to their name in the context of the recorded conversation or whether they have been previously identified) or indirectly identifiable through a combination of information such as their telephone number and voice which is an element of the data subject's physiology.*

b. information on the recipients who might have my personal data

*Wrong answer. Article 15 GDPR (*right *of access) explicitly states that in the context of the* right *of access, the data subject has the* right *to know, inter alia, 'the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations'.*

c. copies of data concerning another person

Right answer. A data subject's right *of access cannot, in principle, cover data relating to third parties.*

d. information on the time of storage of my personal data.

*Wrong answer. Article 15 GDPR (*right *of access) explicitly states that in the context of the* right *of access, the data subject has the* right *to know, inter alia, "if possible, the period for which the personal data will be stored or, where this is impossible, the criteria determining that period".*

Example 2: The wording 'I wish to have access to the personal data you keep about me' means that the controller must provide, if it isn't particularly difficult for the latter, all the personal data that concern you. Please select: RIGHT/WRONG

Feedback if the 'RIGHT' answer is selected: Right answer. A request for access made by the data subject should in principle be understood as referring to all the personal data of that data subject, unless the latter explicitly limits it only to specific data (see also EDPB, Guidelines 01/2022 on data subjects' RIGHTs — RIGHT of access, Version 2.0, adopted on 28 March 2023, Chapter. 2.3.1, par. 35, p. 16, https://edpb.europa.eu/system/files/202304/edpb_guidelines_202201_data_subject_RIGHTs_access_v2_en.pdf[5])

Feedback if the 'WRONG' answer is selected: Wrong answer. Since the data subject does not place a restriction on his/her data to which he/she requests access, the controller must, in principle, assume that the request in question extends to all the personal data of the applicant which the controller will have to provide (see also EDPB, Guidelines 01/2022 on data subjects' rights — Right of access, Version 2.0, adopted on 28 March 2023, Ch. 2.3.1, para. 35, p. 16, https://edpb.europa.eu/system/files/202304/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf)

Example 3: You send, through your legal representative, a request for access to your personal data to the company from where you bought a pair of sneakers. You send the above mail to the email address 'info@Company_X.gr' of the controller's company, which is listed on the controller's website as an e-mail address for regular customer communication with the company. You don't send the access request to the email address of the Data Protection Officer 'dpo@Company_X.gr', which has been designated in the company's data protection policy as the contact point for the exercise of the rights of data subjects.

What should you do, through your legal representative? Select one or more correct answers.

a. to exercise the right of access in any event by sending it to the correct e-mail address.

This answer is wrong. If a right *of access is clearly and explicitly formulated and is brought to the attention of the controller through a communication channel provided by the controller and even addressed to an e-mail address indicated for regular customer communication with the controller's company, the controller must examine it even if it needs to be transferred from a department of the controller's company which lacks the relevant authority to the competent department authorized to handle the requests of the data subjects (see in this regard EDPB Guidelines 01/2022 on data subjects'* rights —Right *of access*[5]*, paragraphs 55-56, p. 23, where it is further noted that it is recommended as a good practice to improve internal-intra-corporate communication in order to redirect requests from data subjects to the controller's competent department for further processing). It is therefore not mandatory for the child to resubmit the request by sending it to another address of the same controller.*

b. to wait for 30 days in principle because the request must be forwarded to the competent department in order to be examined and satisfied accordingly.

This answer is correct. If a right *of access is clearly and explicitly formulated and is brought to the attention of the controller through a communication channel provided by the controller, and even addressed to an e-mail address indicated for regular customer communication with the company, the controller must examine it even if*

[5] *https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_RIGHTs_access_v2_en.pdf*

it needs to be transferred from a department of the controller's company which lacks the relevant authority to the competent department authorized to handle the requests of the data subjects (see, to that effect, EDPB, Guidelines 01/2022 on data subjects' rights —Right *of access, Version 2.0, adopted on 28 March 2023, Ch. 3.1.2, paragraphs 55-56, p. 23, where it is further noted that it is recommended as a good practice to improve internal-intra-corporate communication in order to redirect requests from data subjects to the controller's competent department for further processing, https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf). It is therefore recommended that the child wait for 30 days from the submission of the request for access, giving the controller the period they are granted, in principle, under article 12 of the GDPR, in order to fulfil the* right *exercised before them.*

c. to contact the Data Protection Authority.

This answer is wrong. The child is not recommended to lodge a complaint with the Authority, through their representatives, before 30 days have elapsed since the exercise of the right *of access and provided that no reply has been received from the controller. This is because the deadline provided for in the GDPR to the controller to examine and respond accordingly to the data subject's exercised* right *has not expired.*

d. to contact the Controller by phone.

This answer is RIGHT. It is at the discretion of the data subject to contact the controller. However, it should be noted that the controller is, in any event, under an obligation to handle and examine a clearly formulated request for access even if it was initially received by a non-competent department of the company, in particular if it is sent to an e-mail address indicated for regular customer communication with the company (see, to that effect, EDPB, Guidelines 01/2022 on data subjects' rights *— R*ight *of access, Version 2.0, adopted on 28 March 2023, Ch. 3.1.2, paragraphs 55-56, p. 23, where it is further noted that it is recommended as a good practice to improve internal-intra-corporate communication in order to redirect requests from data subjects to the controller's competent department for further processing, https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf*

Example 4: The Data Controller is not obliged to respond to your request for access to your personal data when it has not found any of your requested personal data in its file. RIGHT/WRONG

Feedback if RIGHT is selected: This answer is wrong. Even if the data controller does not keep any of your data, he is obliged to give you a negative answer (see relatively 65/2022, reas. 6, 61/2021, 2/2020, reas. 1 και 43/2019 Decisions of the Hellenic Data Protection Authority, available in the website www.dpa.gr, see also EDPB, Guidelines 01/2022 on data subjects' rights – Right *of access, Version 2.0, adopted on 28 March 2023, Chap. 2.2.1.1, par. 18, page 12).*

Feedback if WRONG is selected: This answer is correct. Even if the data controller does not keep any of your data, he is obliged to give you a negative answer (see relatively 65/2022, reas. 6, 61/2021, 2/2020, reas. 1 και 43/2019 Decisions of the Hellenic Data Protection Authority, available in the website www.dpa.gr, see also EDPB, Guidelines 01/2022 on data subjects' rights – *R*ight *of access, Version 2.0, adopted on 28 March 2023, Chap. 2.2.1.1, par. 18, page 12).*

Example 5: when someone who keeps your personal data and refuses to provide you with any of these you have asked for, he/she must give reasons why he/she does not satisfy you. RIGHT/WRONG

Feedback if RIGHT is selected: In the case where the data controller refuses to satisfy an access request either in whole or in part, he must inform the data subject of the reasons that led to this non-satisfaction or partial

satisfaction, as the case may be, and indeed within the 30-day period from the submission of the request. The said justification that the data controller shall provide, must be detailed and specify the circumstances that did not allow the access request to be satisfied or only allowed its partial satisfaction. And this, in order to be feasible a possible appeal from the part of the data subject against the non- or the partial satisfaction. The above reasoning must also mention the possibility of the data subject to submit a complaint before the Data Protection Authority (see article 77 of the GDPR) and also to exercise the prescribed legal remedies (see article 79 of the GDPR) (see relatively for the above EDPB, Guidelines 01/2022 on data subjects' right*s – R*ight *of access, Version 2.0, adopted on 28 March 2023, Chap. 6.2, par. 174, page 55).*

Feedback if WRONG is selected: This answer is wrong. In the case where the data controller refuses to satisfy an access request either in whole or in part, he must inform the data subject of the reasons that led to this non-satisfaction or partial satisfaction, as the case may be, and indeed within the 30-day period from the submission of the request. The said justification that the data controller shall provide, must be detailed and specify the circumstances that did not allow the access request to be satisfied or only allowed its partial satisfaction. And this, in order to be feasible a possible appeal from the part of the data subject against the non- or the partial satisfaction. The above reasoning must also mention the possibility of the data subject to submit a complaint before the Data Protection Authority (see article 77 of the GDPR) and also to exercise the prescribed legal remedies (see article 79 of the GDPR) (see relatively for the above EDPB, Guidelines 01/2022 on data subjects' right*s – R*ight *of access, Version 2.0, adopted on 28 March 2023, Chap. 6.2, par. 174, page 55).*

Example 6: You exercise the right of access to all your personal data held on a website, of which you are a member, by sending an e-mail to the data controller (e.g., company that owns the website), requesting a copy of them at the same time. Which of the following is/are correct?

a. The data controller asks you to pay a reasonable fee in order to examine/satisfy your request.

This answer is wrong. The data controller shall examine your request and provide you with a copy of your personal data that keeps without asking you to pay a fee. If multiple copies are requested, only then the data controller may request payment of a reasonable fee (see article 15 par. 3 of the GDPR).

b. The data controller asks you to justify why you are requesting access to your personal data and if you do not do so, he has the option to refuse to proceed with the request

This answer is wrong. It is not necessary to state the reasons for which you wish to exercise the right *of access. The data controller shall satisfy the* right *of access you have exercised to your personal data, without asking you the reasons for which you are requesting it and by extension regardless of these reasons (see Hellenic Data Protection Authority's Decision 26/2021, reas. 2, available on the website of the Authority).*

c. The data controller asks you to tell him where you will use the copy he will give you, otherwise he tells you that the law allows him not to give you a copy.

This answer is wrong. The data controller shall examine and satisfy accordingly the right *of access that you have exercised without making its actions dependent on where you will use the copy of your personal data that may be granted to you.*

d. None of the above.

This answer is correct. None of the above answers are correct for the reasons stated in each of them separately.

2.4.10 Learning Topic 10: Children and parents legal responsibility

2.4.10.1 Background

In cases where minors, through the use of personal data of third parties, even those of their relatives (e.g. their parents), cause damage to the aforementioned persons, their liability is formulated as follows (see also relevant national provisions in particular of the Civil and Criminal Code) :

Criminal responsibility, as long as the use of a given third party's personal information constitutes a criminal offense (e.g. public posting on Facebook of a video with pornographic material in the context of which the minor himself videotaped his classmate – revenge porn), the minor is criminally liable if he has completed the 15th year of his age. In this case, therapeutic or reformative measures can be imposed on him, while restriction to a special youth detention center can also be imposed. If the minor is between 12 and 15 years old, the act is not attributed to him/her, but there is a possibility of imposing therapeutic or reformative measures (Article 126 of the Greek Penal Code).

A minor is liable for damages he causes if he has completed his 10th but not 14th year of age (see Greek Civil Code). In this case, the guardians of the minor (e.g., his parents) are sued. The damage compensation claim may concern both the material damage that may occur and the moral damage that may be caused. It is noted that those exercising parental care of the minor (regardless of the age of the minor) or whoever exercises the supervision of the minor even on the basis of a contract, are responsible according to article 923 of the Civil Code as having their supervision. In particular, they are responsible for the damage that these persons, the minors, illegally cause to a third party, unless they prove that they exercised proper supervision or that the damage could not have been prevented.

In addition, there is a risk that minors, when processing personal data, either of their own or of third parties, may cause financial and/or moral damage both to themselves and to their parents or to third parties, as mentioned above.

2.4.10.2 Learning objective

There are specific parent/child responsibilities for children's online activities, depending on age. The children should be aware of the legal responsibility that their guardians bear for any act or omission of the children in the field of personal data processing (with all the possible ramifications that such processing may involve).

2.4.10.3 Learning resources

2.4.10.3.1 Material in the form of scenarios regarding children obligations

2.4.10.3.1.1 *A high school student receives a bullying email from a classmate, making fun of his new haircut (e.g. calling him "nerd"). Navigating the internet, the student finds the saferinternet platform that allows him to chat online with a representative, in order to provide him with instructions on how to manage the situation (there is a related screenshot). He does not have to ask his parents' consent to continue the conversation.* RIGHT/WRONG.

RIGHT, because it is a service that is specifically aimed at children.

2.4.10.3.1.2 *An elementary school student wants to buy a popular game online that will allow him to play alongside with other classmates of him who already have it. Following the navigation indications, he fills in his name, address and date of birth, at which point automatically and before proceeding to the registration of the payment details of the application of the game in question, he is asked for his parent's consent for the processing of the personal data that already registered as well as for the acceptance of the other conditions of the application's acquisition. 2 sketches are given below: in the first, the student fills in a false age to overcome the parental consent 'hurdle', while in the second, he is seen informing his mother to give her consent and make a secure online payment. The student will be asked to choose the correct behavior.*

By choosing the wrong first option, it will appear as feedback that this is an action contrary to Article 8 of the GDPR and in addition there is a risk of causing financial damage to his parents, if he proceeds with an unsecured payment using the information of their credit/debit cards without their knowledge, without excluding any other parental responsibilities depending on the means of age verification that the provider of the game platform in question may have (the last possibility presupposes the interconnection of more files which, logically, will not be possible for the controller to have. Therefore it is better not to make any reference to "other potential responsibilities").

Feedback for the second answer, which is the correct one: The child's mother, as the one who exercises the parental care, clearly needs to be informed so that the online payment can be made safely under her supervision

2.4.10.3.1.3 *I need to get my classmate's consent before I publicly post a photo or video that includes him RIGHT/ WRONG.*

«RIGHT» is the correct answer: If I post in public a photo or video that includes the image, thus personal data, of a third party, the consent of the above third person depicted must be secured beforehand

2.4.10.3.1.4 *When a classmate asks me to take down from a social media platform a photo of him that I have posted making it visible to everyone, I ignore him and continue to keep it publicly posted. RIGHT/WRONG.*

The correct answer is «WRONG»: since the classmate has. expressed his desire to delete a photo of him that his classmate has posted on a social networking platform in a way that is publicly visible, the classmate must in principle respect the protection of his privacy and immediately proceed to unpost/delete the said photo.

2.4.10.3.2 Material in the form of real life cases regarding legal responsibility

2.4.10.3.2.1 *A high school student posts on a social networking platform, so that it is publicly visible by all users of the platform, a photo of his classmate that depicts her injured in the school yard, without obtaining her consent. When the person pictured asks him to unpost the photo in question, he: 1st scenario unposts it immediately, 2nd scenario keeps the photo posted.*

The first scenario is the correct one. Since there is no consent of the depicted student and the latter expresses her desire to have the photo in question removed from her classmate's profile, he must immediately remove it in order to protect the legal right to the privacy of the depicted student. In case where someone chooses the second scenario as an answer, sketches pop up (or bubbles depending on the available technical possibilities) through which we see the consequences (a lawsuit filed against the student who made the post, as represented by those who exercise parental care, for payment of compensation in the context of moral damage due to insulting the personality of the depicted injured student as well as a lawsuit for payment of compensation due to violation of personal data legislation as it is illegal processing. Furthermore, the student receives (via those who exercise parental care) a complaint to provide clarifications to the Data Protection Authority for illegal processing of personal data. His parents are also sued for compensation due to negligent supervision of their child who made the controversial post, which he kept publicly despite the objection of the pictured person. (It is noted that the above actionable claims could be accumulated in the same case file, but they are simply presented separately for reasons of emphasis.)

2.4.10.3.2.2 *A high school student purchases a tracksuit online and proceeds to the payment by giving his mother's debit card details without informing her beforehand. 2 days later, it is found that the balance of the account, from which the debit card was serviced and with which (card) the student made the payment, has been zeroed, so it is notified after contacting the Electronic Crime Prosecution that the transaction took place on an unsecured website and therefore it was fraud that caused financial loss to the student's parent. What would be the correct behavior for the student to follow so as to reduce the risk of harm?*

Feedback: The parent's information and consent is necessary to make any online purchase using the latter's payment card.

2.4.10.3.2.3 *In the event that a 17-year-old High School student posts an abusive comment on a social networking platform against a classmate of him, whom he mentions by name, he is criminally liable. RIGHT/WRONG.*

«RIGHT» is the correct answer: since the use of personal data of a third party constitutes a criminal offense, such as the insult in this case, the minor is criminally liable if he has reached the age of 15. In this case, therapeutic or reformative measures can be imposed on him, while restriction to a special youth detention center can also be imposed.

2.4.10.3.2.4 *In the event that a 15-year-old student sends an intimidating email to a classmate of him, sharing it with the email addresses of third parties - the sender's contacts, his guardians are at risk of paying compensation if illegal processing of personal data is found in the context of a related lawsuit. RIGHT/ WRONG.*

The correct answer is «RIGHT»: It is noted that those exercising parental care of the minor (regardless of the age of the minor) or whoever exercises the supervision of the minor even on the basis of a contract, are responsible according to article 923 of the (Hellenic) Civil Code as having their supervision. In particular, they are responsible for the damage that these persons, i.e. minors, illegally cause to a third party, unless they prove that they exercised proper supervision or that the damage could not have been prevented.

3 Description of the learning scenarios

Learning scenarios used in the educational program aim to use the various learning resources in a way to maximize the awareness and learning results for the children. Considering pedagogical methods appropriate for the children age, the learning scenarios are presented through a variety of methods and tools aimed to maximize the level of interest and active participation of the children. Overall, the progression of topics follows a logical sequence via learning scenarios in the format of 21st century Skills Labs (Ergastiria Dexiotiton) starting with foundational concepts and gradually delving into more complex aspects. The program's design ensures that students develop a comprehensive understanding of personal data privacy and are equipped with the knowledge to navigate the digital landscape responsibly.

The Skills Labs' main goal is the cultivation of skills necessary for a rapidly changing world. Particular emphasis is placed on the 4Cs of 21st century skills – communication, collaboration, critical thinking, and creativity – along with digital skills. It was awarded the Global Education Network Europe (GENE) Global Education Award (2020/2021). Kindergartens and elementary schools dedicate 3 hours per week (10% of total teaching time) and lower secondary schools dedicate 1 hour per week (to be expanded soon).

Thus, the pedagogical principles of the learning scenarios are:

- Active Learning: Focusing on student engagement through interactive activities that encourage critical thinking, problem-solving, and hands-on exploration.
- Collaborative Learning: Emphasizing teamwork and communication skills by promoting group projects, discussions, and peer-to-peer learning.
- Inquiry-Based Learning: Encouraging students to ask questions, seek solutions, and explore topics in-depth, fostering a sense of curiosity and autonomy.
- Technology Integration: Leveraging technology to enhance learning experiences, promote digital literacy, and provide access to a wider range of resources.
- Differentiated Instruction: Recognizing diverse learning needs and tailoring instruction to accommodate various learning styles and paces.
- Real-World Relevance: Connecting classroom learning to real-life situations to make concepts more meaningful and applicable.

Students will use a variety of learning resources that have the following characteristics:

- They are interactive, putting the children in a position to actively select plots/answers/paths in the scenarios. Interactive videos are used in this context, giving children the opportunity to interact with a popular tool which they are so very much used to interact with in the online world.
- They are in the form to raise the interest and attention of children according to their age, such as in the form of a comic, either presented either being created or edited by the children themselves.
- They include additional material included in a Web site, in a modern and attractive format.

Group discussions and comic creation urge children to actively think about the learning materials in real cases, use their imagination and creativity and interact in groups, exchanging ideas and feelings.

In addition, an educational game as the "means of transport" for the personal data protection awareness "journey", plays an important role in these scenarios as an engaging educational tool making use both of traditional flat board game and of technology to keep children interest and maximize the learning results.

3.1 Educational Game

3.1.1 The purpose of the game

The purpose of this educational game is to help students become aware of the dangers lurking on the internet and acquire the necessary knowledge to safeguard their personal information and protect their online reputation. Additionally, the aim is to learn how to reject inappropriate behaviors on the Internet and seek help from a trusted adult when they have doubts or when something or someone online makes them feel uncomfortable, anxious, or fearful.

3.1.2 The target group, the players and the goal of the game

This game is designed for students in the last grades of elementary school and middle school, as well as high school students. Prior knowledge on Data Protection is not necessary. Students should be familiar with mobile devices or tablets. Specifically, they need to be able to search for and open applications and use the device's camera to scan symbols on the game board and cards. Moreover, they should be able to navigate the application environment following on-screen instructions.

The game is played by two (2) to six (6) players or by two (2) to six (6) teams of players.

The goal of each player is to move their pawn through the eight stations of the game, answer the questions correctly, and collect as many diamonds as possible (they must collect at least 1 diamond of each color). The player who has gathered the most diamonds is the winner. It is necessary for them to have collected at least 1 diamond from each station.

The equipment used and the rules of the game can be found in Appendix A: Educational Game Equipment, Rules and Presentation Modes of the Learning Resources, sections 5.1 and 5.2 respectively.

3.1.3 Digital Learning Resources

The learning material of the game is digitized and appears on the player's screen when he/she scans the symbol on a card (the different presentation modes of the learning resources can be found in Appendix A: Educational Game Equipment, Rules and Presentation Modes of the Learning Resources, section 5.3). The material is categorized into units. Each station of the game corresponds to a thematic unit. The thematic units are independent, allowing players to move from one station to another as many times as they wish and in any order they prefer. The units of the learning material are listed in Table 1.

UNIT	LEARNING OBJECTIVES
CONCEPTUAL DEFINITION OF PERSONAL DATA	• Understanding the concept of personal data and how it relates to their privacy in daily life. • Understanding when and how they may disclose their personal data in their social life or on the internet, primarily through online games, social networking services, and content sharing.
RISKS OF DISSEMINATING/SHARING CHILDREN'S PERSONAL DATA	• Understanding the potential risks of sharing their personal data on social networks. • Learning ways to protect their personal data on the Internet and social networks. • Recognizing the characteristics of malicious individuals on the Internet.
PROFILING - TARGETING – ADVERTISING	• Realizing how browsing works as a means of leaving digital traces. • Understanding the risks arising from forming an image of their preferences. • Learning protective measures such as refusing cookies or configuring settings for private browsing.

UNIT	LEARNING OBJECTIVES
	• Understanding the risks of using applications on smartphones, with a special focus on electronic applications of mobile phones regarding tracking capabilities through the permission model on Android.
PRIVACY CHOICES - MANAGEMENT	• Being able to adjust their privacy settings on social networks and electronic services. • Understanding that without activating privacy settings on the social networks they use, anyone can access their personal data. • Realizing the importance of prevention, meaning thinking seriously before posting or disclosing their data on the internet.
RIGHTS CONCERNING THE PROCESSING OF PERSONAL DATA	• Understanding their rights as autonomous data subjects. • Distinguishing the types of each right (access, deletion, objection, and correction). • Understanding when they can exercise each right. • Understanding that they should address their parents/teachers. • Learning about the role of the Data Protection Authority.

Table 1: Learning Material Units

3.2 Learning Scenarios in the format of Skills Lab

3.2.1 The Goals of the Lab

A lab entitled "*Think of your data more... 'personal'*" has been designed for the students of Primary Education (5th and 6th grade) and Secondary Education (Middle School and High School). The purpose of this skills lab is to help students via a series of learning activities understand the risks that exist on the internet and acquire the necessary knowledge to safeguard their personal information and protect their online reputation. Additionally, the goal is to help students learn how to reject inappropriate behaviors on the internet and seek help from a trusted adult when they have doubts or when something or someone online makes them feel uncomfortable, anxious, or fearful.

The Lab's target skills are the following:

- Life skills
  - Responsibility
  - Empathy
  - Online privacy
- Learning skills
  - Collaboration
  - Critical thinking
  - Communication
  - Digital critical thinking
  - Integrated digital technology, communication, and collaboration skills

3.2.2 Structure of the Lab

The duration of the lab will be seven weeks consisting of the following seven sessions (each one can be considered a learning scenario with specific activities to address particular learning objectives per topic). A more detailed description of the activities involved in each session can be found in Appendix B: Skills Lab Activities.

3.2.2.1 Session 1: "Think before you share"

In the first session of the lab, students ponder the issue of personal data protection and privacy, as well as the importance of others' privacy. They watch a video to raise awareness and connect the topic with their own personal experiences. The students are expected to:

- Reflect on the risks involved when posting something on the Internet.
- Express their opinions and feelings regarding social media posts.
- Understand the issue of personal data security and recognize its global dimension.
- Listen carefully to their peers.
- Use dialogue tools to articulate their opinions with respect to their classmates.

3.2.2.2 Session 2: "Authentic stories"

In the second session, students are divided into groups and study authentic scenarios involving other children. They are asked to carefully examine each scenario, identify the problem of each scenario, express their questions, and suggest what additional information they would like to know about the specific topic. At the end of this session, students consult the workshop's supplementary materials to find solutions or good practices for each scenario. The students are expected to:

- Make connections with their previous knowledge and experiences.
- Interpret in-depth the subject of personal data security.
- Justify the change in their views regarding the issue of personal data.
- Give space to others to express themselves.

3.2.2.3 Sessions 3 and 4: "The Game"

In these two sessions, students, still in groups, participate in an augmented reality tabletop game (see section 3.1). They encounter various scenarios where they need to recognize risks to personal data that are being processed and the possible consequences for the individuals involved. The goal of the game is for students to acquire the necessary knowledge to protect their own personal data. Additionally, they learn how to reject inappropriate online behaviors and seek help from a trusted adult if they have doubts or feel uncomfortable, anxious, or fearful about something or someone in the Web. The students are expected to:

- Understand the concept of personal data and how it relates to their daily private life.
- Comprehend when and how they may disclose their personal data in their social life or on the internet, primarily through online games, social media services, and content sharing.
- Be aware of the potential risks of sharing their personal data on social networks.
- Learn ways to protect their personal data on the Internet and on social networks.
- Recognize the characteristics of malicious individuals on the Internet.
- Understand how navigation leaves digital traces.
- Comprehend the risks of forming an image based on their preferences.
- Learn about self-protection methods, such as denying cookies or configuring settings for private browsing.
- Understand the risks of using smartphone applications, particularly electronic applications with tracking capabilities via permission models on Android.
- Be able to adjust their privacy settings on social networks and electronic services.
- Realize that when privacy settings are not enabled on social networks they use, anyone can access their personal data.
- Understand the importance of prevention, meaning they should think seriously before posting or sharing their data on the internet.

- Understand their rights as autonomous data subjects.
- Distinguish between different types of rights (access, deletion, objection, and correction).
- Understand when they can exercise each right.
- Know when to address their parents/teachers.
- Learn about the role of the Data Protection Authority

3.2.2.4 Sessions 5 and 6: "Become a comic creator"

In sessions five and six, the students take on the active role of comic creators. They are asked to imagine, design, and digitize their own comic scenarios on the theme of "Personal Data Protection." Students will present their comics to the class and evaluate their peers' comics. The purpose of these sessions is to reinforce the knowledge about the security protection of their personal data, which they have built in the previous sessions, and enhance their collaborative skills. The students are expected to:

- Reinforce their knowledge about the topic of personal data security that they have built in previous workshops.
- Enhance their collaborative skills.
- Develop skills in:
    - collaborative writing,
    - designing and producing narrative content, and
    - problem-management and problem-solving (critical thinking, Creative imagination, analysis, synthesis, organization, interaction, self-reliance, responsibility).

3.2.2.5 Session 7: "Knowledge is turned into action"

Finally, the lab concludes with the creation of a poster containing tips for protecting personal data for peers, followed by a discussion about a future action aimed at informing and raising awareness among other students. The students are expected to:

- Reflect on what they have learned and draw inspiration from it.
- Express their opinions on the usefulness of future actions to their peers.
- Realize that new knowledge, both theoretical and practical, can redefine our thoughts and emotions.
- Adjust their behavior based on new knowledge, especially if it may pose risks to their own personal data or others'.
- Evaluate what they gained from participating in this workshop by completing self-assessment forms

4 Conclusions

In conclusion, the objective of raising data protection and privacy awareness among the critical social group of children will be reached by the development of an educational program, which does comprise adequate and suitable learning resources, adapted accordingly taking into consideration pedagogical issues so that selected learning scenarios are presented to children via education forms and tools aiming to achieve the best awareness and learning results.

The learning resources cover selected topics (Personal data and special categories of personal data; Processing of personal data; Data Controller and Data Subject; Lawfulness of the processing; Consent of the data subject; rights of data subjects; Online personal data commercialization; Personal data protection risks and measures). The chosen topics effectively cover the essentials of personal data privacy for children. Beginning with defining personal data and its sensitivity, the seminar progresses to clarify roles like data controller and data subject. It educates on legal processing, the importance of consent, and data subjects' rights. The discussion extends to commercial use of personal data, raising awareness about risks and promoting protective measures. This well-rounded approach equips children with fundamental knowledge, empowering them to make informed decisions while navigating the digital landscape and fostering responsible online behavior.

Furthermore, we have designed engaging learning scenarios within a 7-week skills lab that could immerse students in active learning and critical thinking. Each week, distinct themes should be tackled through real-world challenges, case studies, interactive content, every day cases and material for further study and group projects. Role-playing exercises and discussions encourage diverse perspectives, fostering analytical skills. Diverse learning styles have been accommodated through textual resources, multimedia like videos, interactive game, visual aids like comics, and practical tools. These scenarios aim to make learning dynamic and relatable, promoting engagement and deep understanding.

By providing a variety of learning resources and interactive approaches, the learning scenarios, along with their accompanying materials, cater to diverse preferences and ensure an enriching educational experience.

5 Appendix A: Educational Game Equipment, Rules and Presentation Modes of the Learning Resources

5.1 Game Equipment

The game includes:

1. A game board depicting the 8 stations, the starting positions, the places where players position their pawns at the beginning and during the game, the mystery symbols, and a QR code in the center.

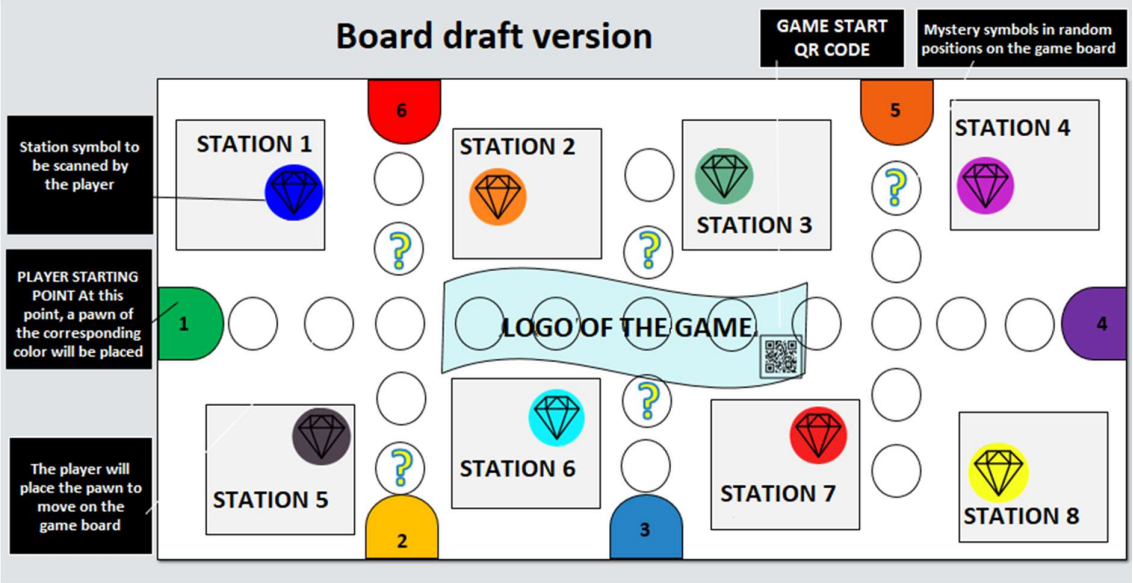


Figure 1: Game Board

2. One numeric die.
3. Six (6) pawns of different colors.
4. Six cards in newspaper format for the start of the game.

Figure 2: Card in Newspaper Format

5. Six (6) cards with diamonds for the end of the game

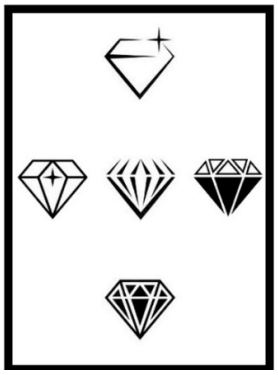


Figure 3: Card that Players will Scan at the end of the Game

6. 10 mystery cards
7. Paper cards with diamonds. There are diamonds in 8 different colors (blue, purple, gray, green, yellow, orange, blue, and red) that correspond to the different stations. Additionally, there are white diamonds that are given as a bonus to the players.

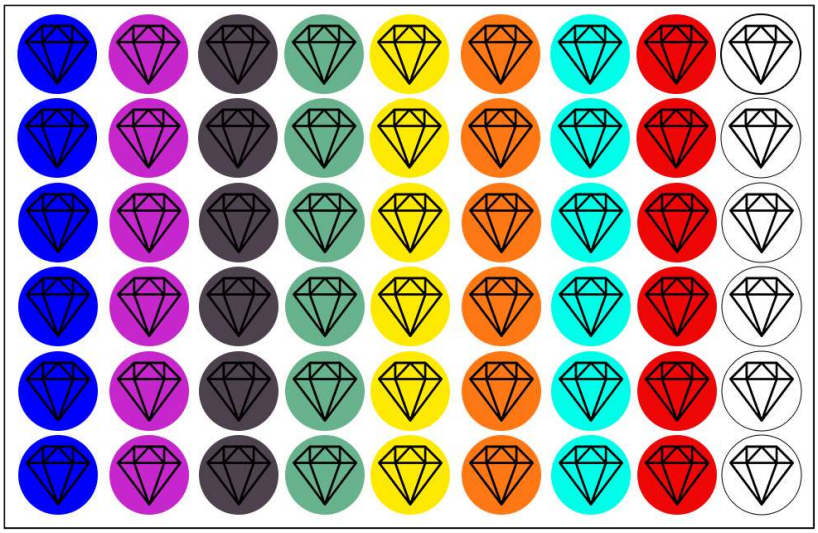


Figure 4: The paper diamonds that players will win at the stations and mystery cards

8. Eight cards for each station of the corresponding color (Total of 64 cards).
9. Each player or team of players needs a smartphone or tablet with the ARTutor application installed.

5.2 Game Rules

5.2.1 Preparation

1. The cards with the diamonds, the mystery cards, and the station cards are placed stacked by color in the center or next to the game board.
2. Before starting the game, players open the ARTutor application on their smartphones or tablets and scan the QR code located on the game board.
3. On their device's screen, they will be presented with a quiz containing questions related to the topics covered in previous sessions. When a player scores above 70%, they can choose a pawn and start the game. They can repeat the quiz as many times as needed.

5.2.2 Game start

1. The player places their pawn on the corresponding starting square of the game board, based on its color.
2. He/She draws a card with the newspaper graphic and a card with 5 diamonds.
3. He/She scans the card with the newspaper, and the game begins.
4. The player with the highest roll of the die goes first, followed by the player to his/her right.
5. The first player rolls the die and moves his/her pawn in any direction on the board as many spaces as the number rolled on the die.

5.2.3 Gameplay

If a player places his/her pawn on a station, he/she draws a card from the corresponding station's stack and scans the symbol on it using his/her device. Following the steps shown in the form of a story on his/her screen, he/she answers some questions. If he/she answers correctly, the player earns the paper diamond with the color matching the station and keeps the card he/she drew. If the player answers incorrectly, he/she does not get the diamond and leaves the card at the bottom of the stack. The turn ends, and the next player takes his/her turn.

If a player places his/her pawn on a mystery circle  (a circle with the English question mark "?"), he/she draws a mystery card and scans it. Then, the following scenarios can occur:

- He/she may be asked to go directly to any station he/she desires and draw a card from the corresponding stack.
- He/she wins a bonus white diamond.
- He/she is asked to give one of his/her diamonds to a teammate.
- He/she is asked to give/share some personal information in exchange for a diamond (trap - violation of Personal Data Protection principles).

Once one of the above actions is completed, the player's turn ends, and the next player takes his/her turn.

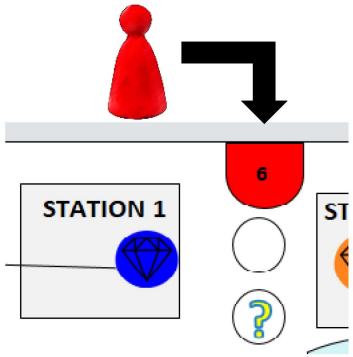
The player who has collected diamonds from all stations (at least one diamond of each color) can scan the card he/she was given at the beginning of the game. If he/she answers all the questions correctly, he/she earns 5 white diamonds. He/she has 3 attempts.

The game ends when all available diamonds are collected.

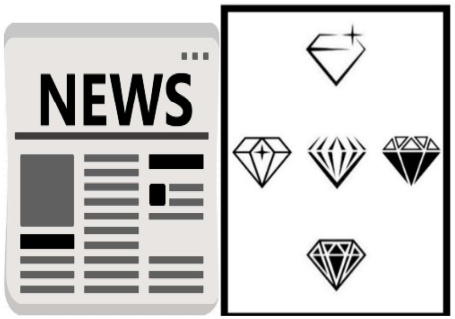
A visualization of the game steps / rules is depicted next:

Game preparation

The player places his/her pawn at the starting position based on its color.

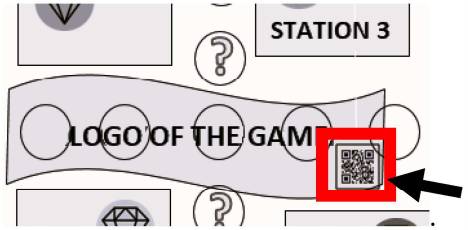


Each player receives 2 cards. One card in the form of a newspaper and one card with diamonds.



Game start

Players open the ARTutor application on their device and scan the barcode, which is located at the center of the game board

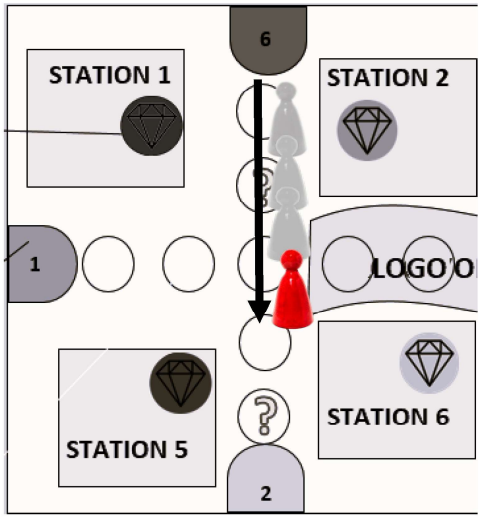


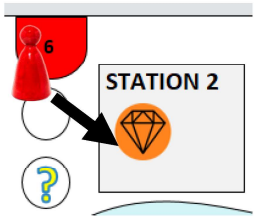
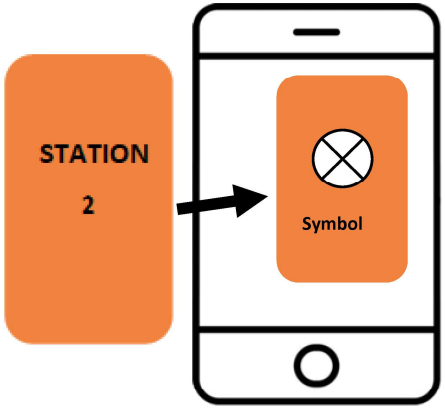
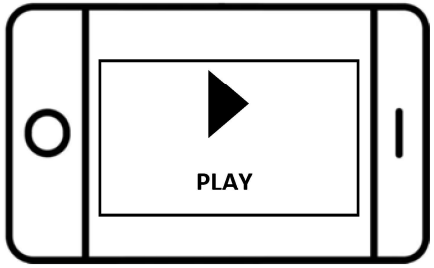
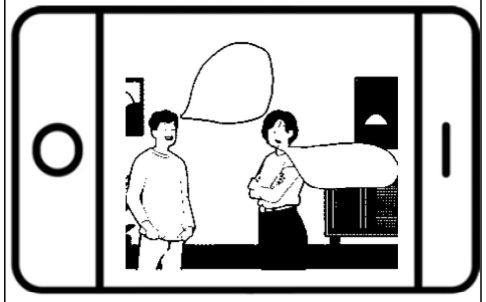
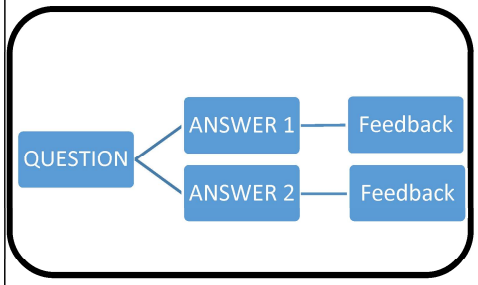
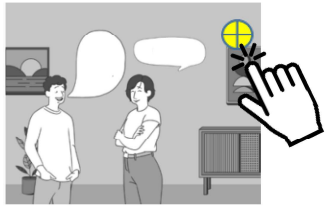
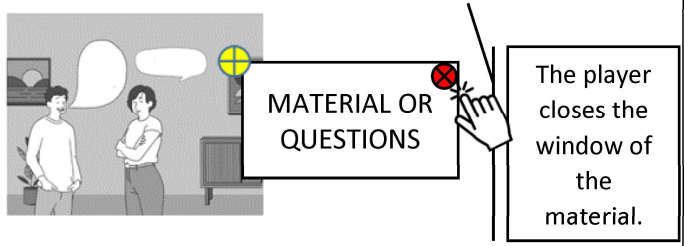
Players scan the newspaper card. Research data appear on their screens.

The player's turn

The player rolls the dice.

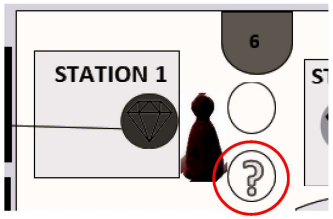
The player moves his/her pawn within the board, as many positions as the number shown on the dice.



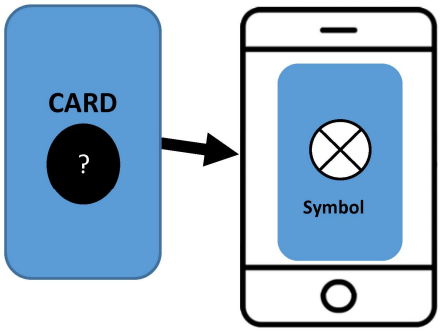
Displaying educational material	Presenting educational material in video format	"Presenting educational material in interactive image (hotspot) format
When the player places their pawn inside a station:  He/she draws a card corresponding to the station and scans its symbol.  Then, the educational material appears on the screen.	The player presses the PLAY button on the screen.  The educational scenario appears on the screen in the form of a comic.  Once the video is completed, comprehension questions are displayed.  	The educational scenario appears on the player's screen in the form of a comic.  The player navigates through the material by clicking on buttons.  By clicking on the buttons, the educational material and comprehension questions are displayed. 

Presentation of mystery card material

If the player places thei pawn on a mystery circle:



He/she draws a mystery card and scans its symbol.



Then, a clue for the continuation of the game is displayed to the player in the form of an image.

End of player's turn

If the player answered correctly:

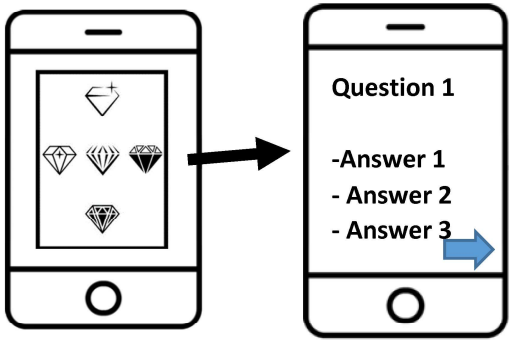
He/she keeps the card he/she played and earns a diamond with the same color as the station.

If the player answered incorrectly, he/she does not win the diamond and leaves the card at the bottom of the stack.

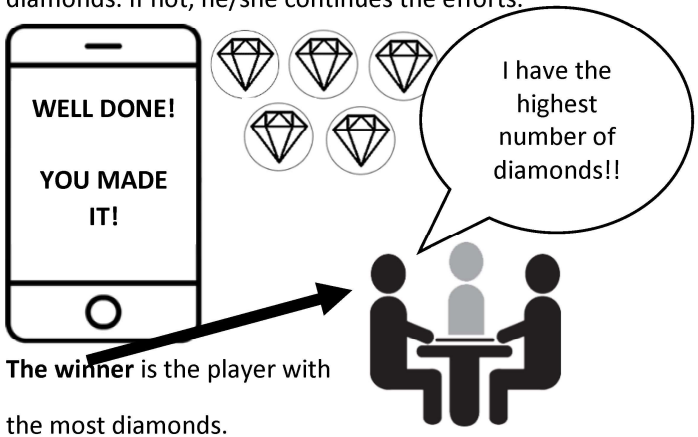
End of the game

The player who has collected the diamonds from all the stations,

can scan the card with the diamonds. Then, a quiz appears on their screen.



If the player answers all the questions correctly, he/she wins 5 diamonds. If not, he/she continues the efforts.



The winner is the player with the most diamonds.

5.3 Presentation Modes of the Learning Resources

When the player scans the card symbol, the learning material will appear on the screen in the following formats:

1. **Interactive image (Hotspot)**

More specifically, on the user's screen, a learning scenario in the form of a comic will appear. The player will be able to click on various points of the image (buttons). As soon as he/she clicks with his/her mouse, additional learning material will appear on the screen in the form of text and comprehension questions, for which he/she will receive positive and negative feedback. For example:

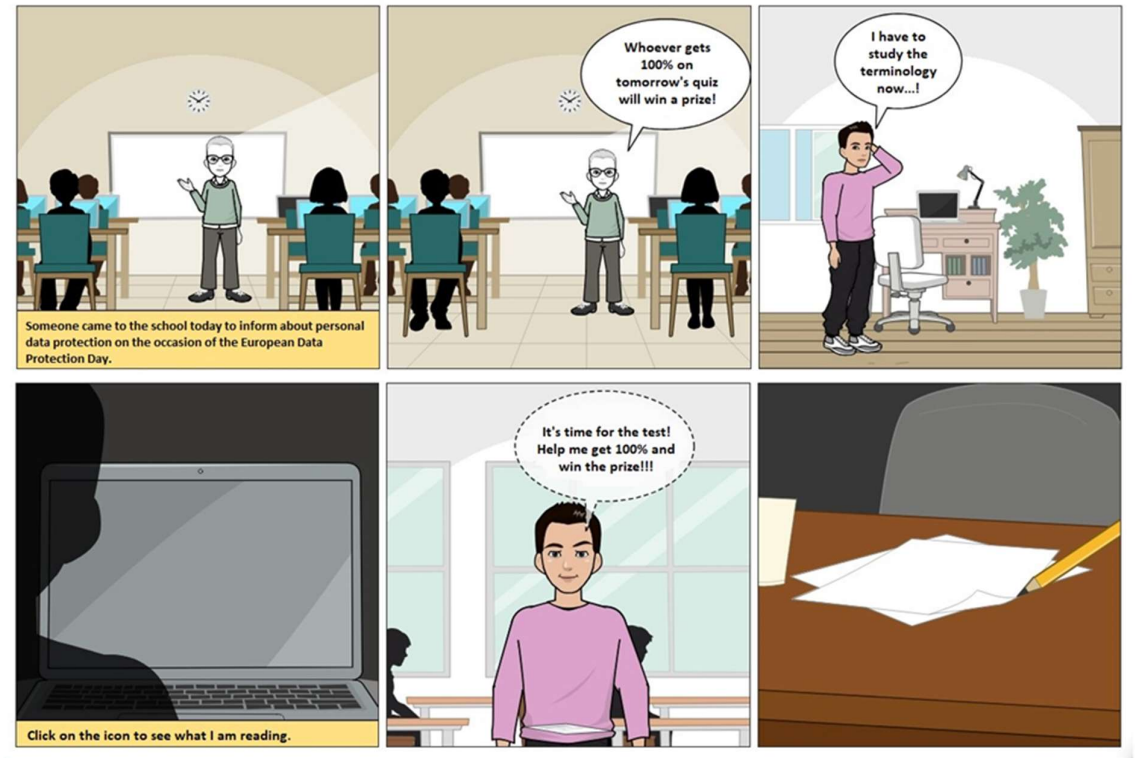


Figure 5: Comics with hotspots

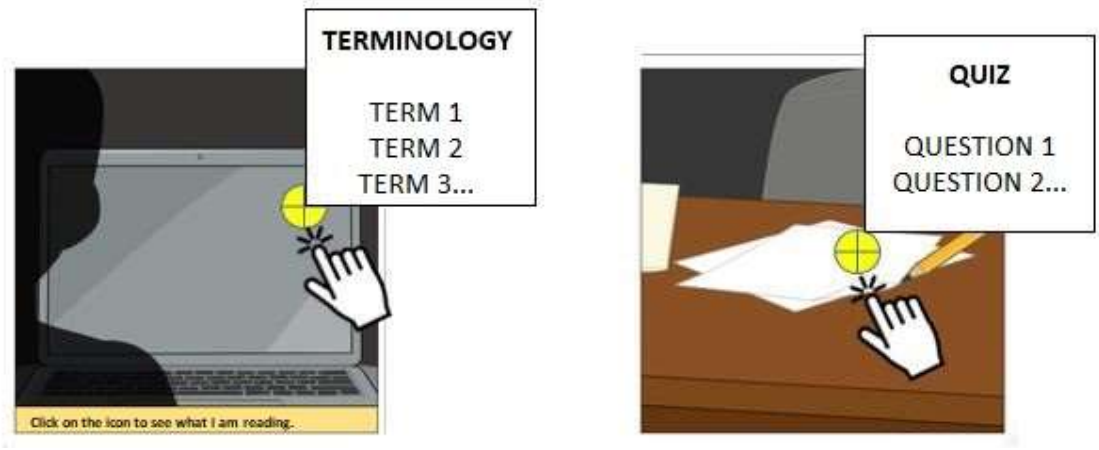
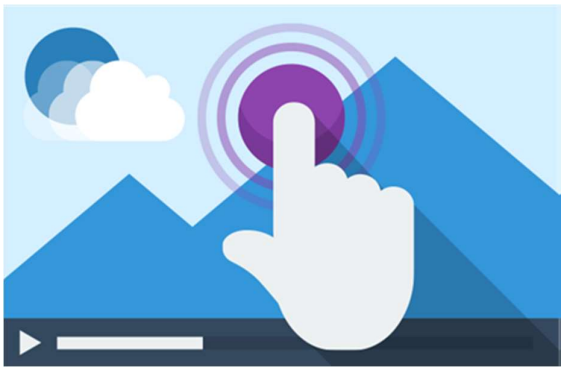


Figure 6: The player clicks on the hotspots, and additional material or comprehension questions appear

2. Interactive video



Once the player scans the symbol of a card, a video appears on his/her screen. The player clicks the start button of the video. While the player is watching the video, interactions are displayed on the screen. For example, buttons that the player can click to access additional learning material or questions he/she must answer. For example:

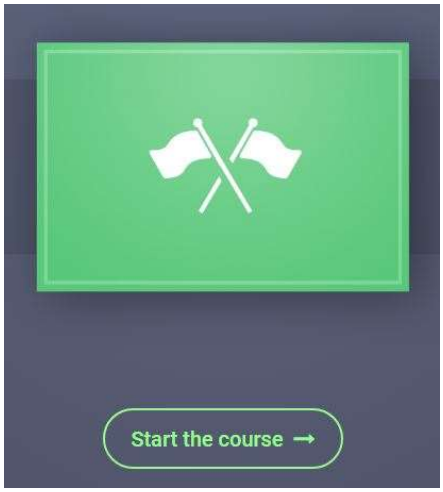


Figure 7: Video start screen

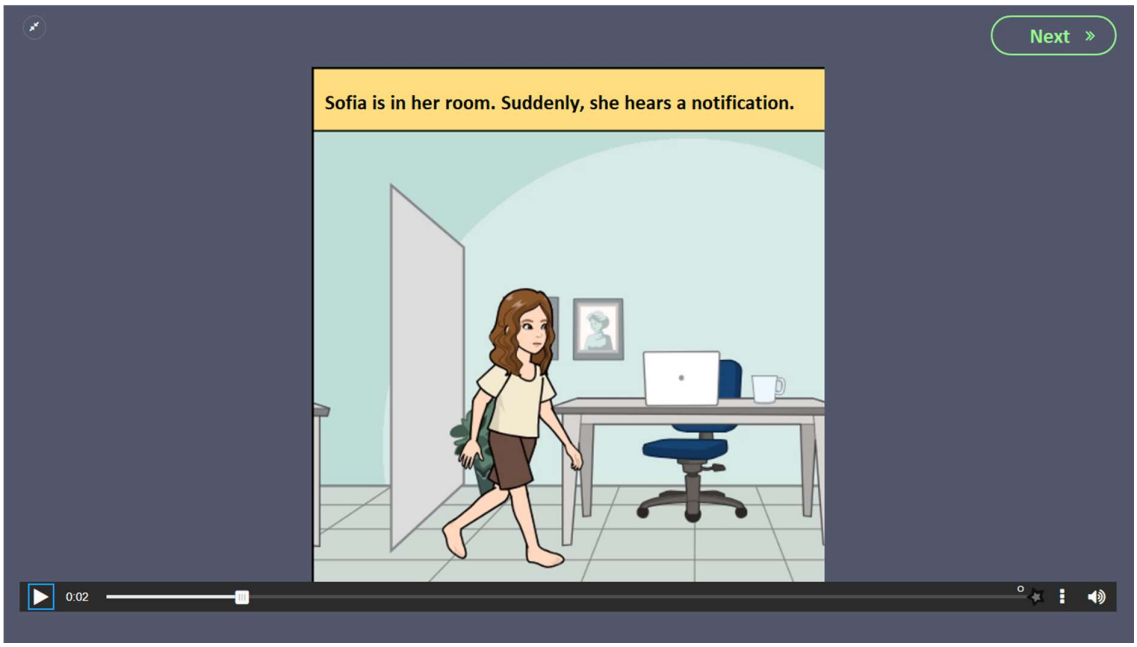


Figure 8: The player watches the video

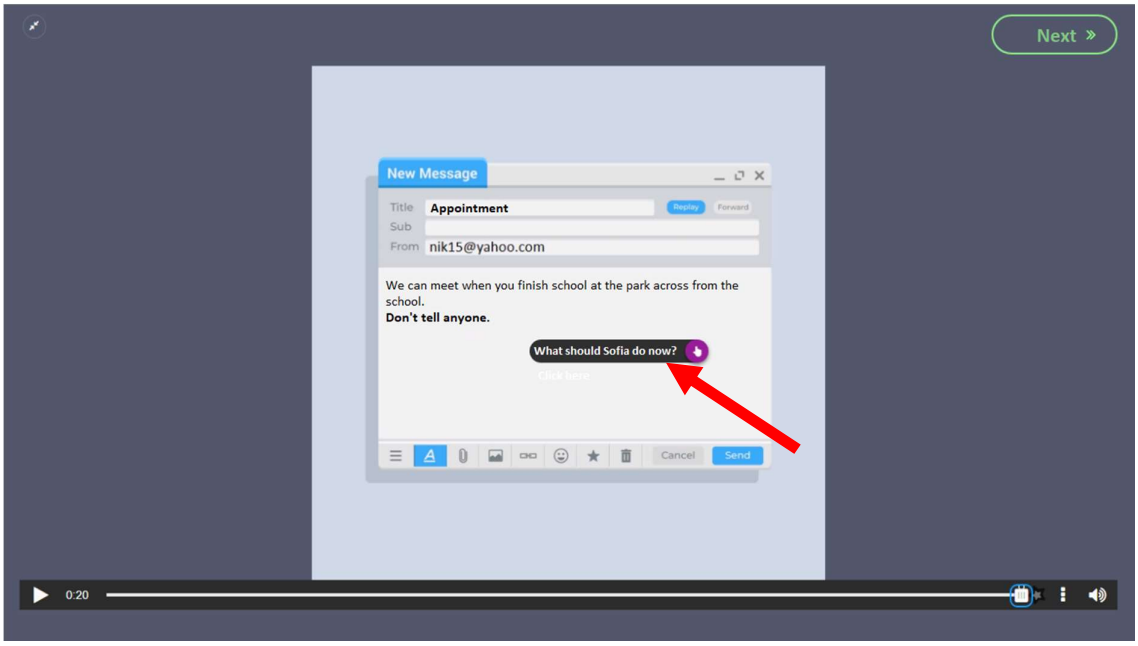


Figure 9: Displaying an interaction

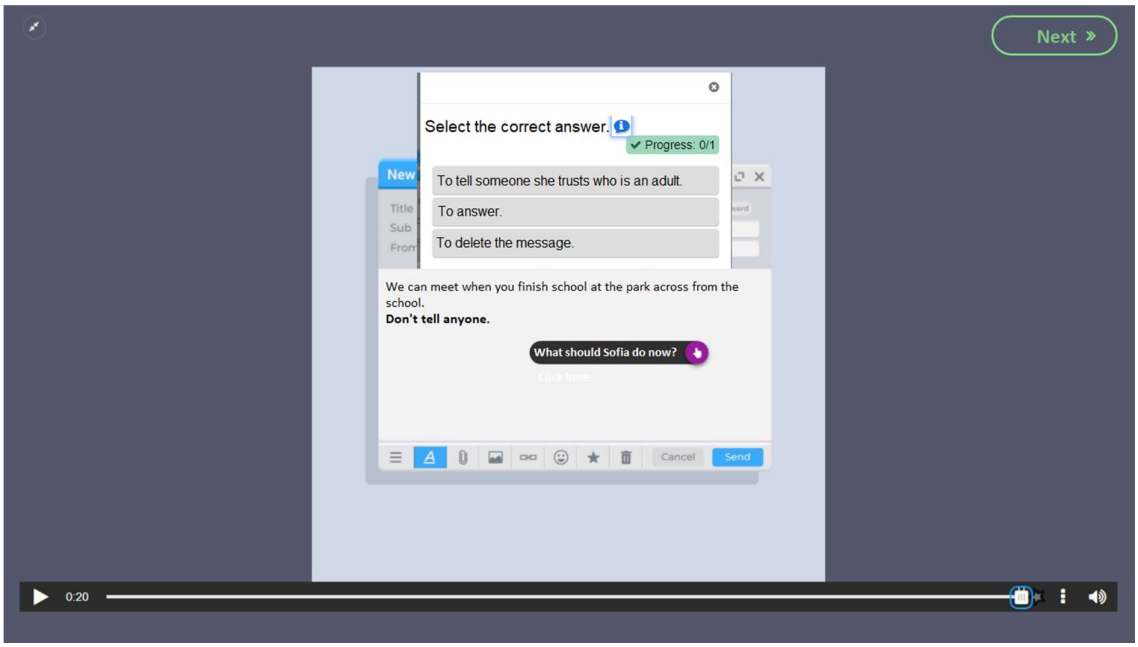


Figure 10: The player clicks on an interaction element

3. Website

As soon as the player scans the card's code, the default web browser opens, and the learning material appears on his/her screen in the form of a webpage. The player navigates through the material using the menu and navigation buttons. By selecting various buttons and menu items, the learning material appears in the form of a comic and comprehension questions. For example:

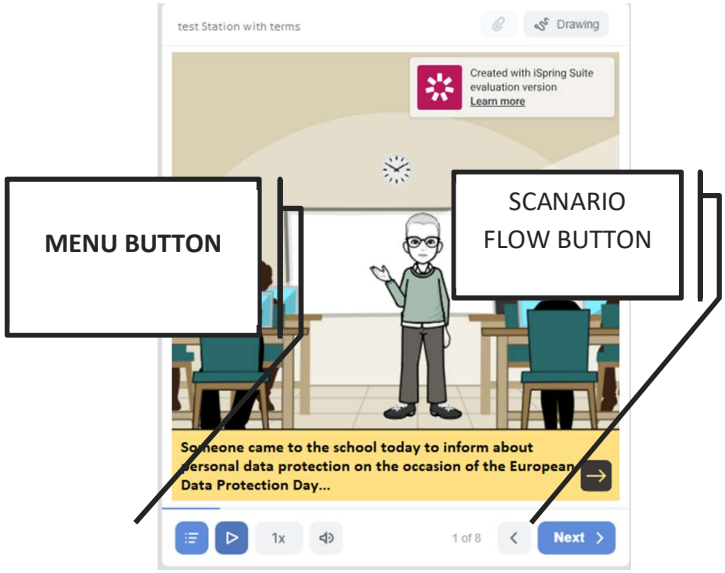


Figure 11: Material webpage screen

Figure 12: The player has opened the menu

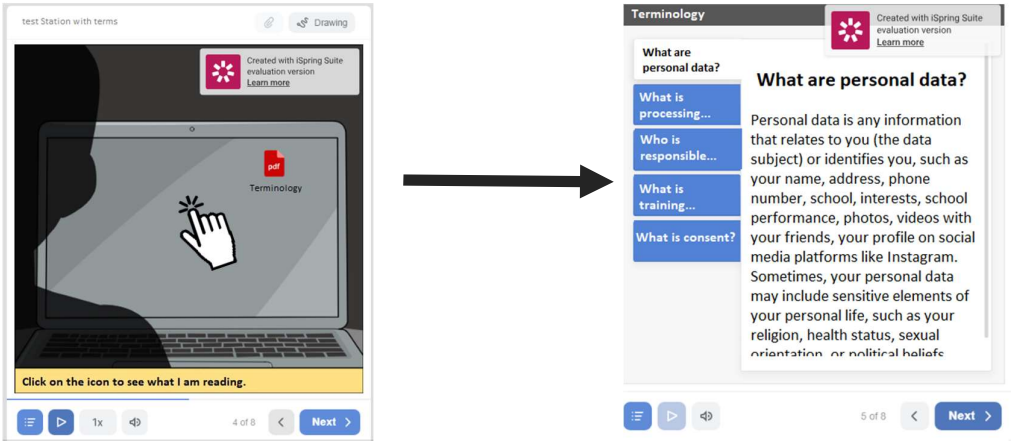


Figure 13: The player clicks on a button, and additional learning material appears

6 Appendix B: Skills Lab Activities

1st Session (Title): "Think before you share"

Activities

Watch with your peers the suggested video "Σκέψου πριν κοινοποιήσεις" ("Think Before You Share") from the Greek Safer Internet Centre (https://www.youtube.com/watch?v=DOe5fxaSW7s).

Engage in a class discussion, using the "What makes you say that?" routine, to comment on the video and its content.

Students answer to the following questions:

- What did you see happening in the video?
- Who are the main characters?
- What is the topic they are dealing with?
- What makes you say that?
- What did you see that led you to that conclusion?
- How did you understand it?
- Has something similar happened to you or someone you know?

During the interaction, encourage the use of dialogue tools:

- ***"Share your opinion":*** *Students express their opinions boldly, using phrases like "From my perspective, I believe...", "In my opinion...", "Some argue that... Others say... In my opinion, however..."*
- **"Ask":** Ask for more details to better understand the other person's opinion.
- **"Connect":** Explain how your perspective or personal experience connects with what your conversation partner said.

Ask the students to play the game "2 truths and 1 lie".

Specifically, provide the students with 3 statements containing research data related to personal data.

Ask the students to vote on which statement they think is false.

Reveal the false statement and present other statistics and research data. Discuss the global dimension of personal data protection.

2nd Session (Title): "Authentic stories"

Activities

Divide the students into groups and distribute 2 scenarios in text format to each group. These scenarios are authentic short stories related to security and personal data. You can either have the scenarios printed or ask the students to open them on their computers.

Create a table with 7 columns, one for each topic to be discussed, or create a padlet.

The topics are as follows:

- Risks of spreading/sharing personal data.
- Security and Privacy settings on social networks.
- Rights regarding the processing of personal data.
- Legal responsibility of children and parents.
- Communication with third parties - Appropriate ways of reacting.
- Online advertisement, manipulation and Deceptive Patterns.
- Secure passwords.

Ask the students to:

- Collaborate and carefully read the 2 scenarios.
- Think and discuss the following topics using the " Think-Puzzle- Explore" Routine :

- What do you believe about this topic?
- What is the problem?
- What questions or doubts do you have?
- What do you want to explore further or learn about this?

Encourage the groups to present their scenarios in class, mentioning their thoughts, sharing and discussing their doubts in the plenary session. Finally, have them place their scenarios under the correct column/category in the table or write the titles of the scenarios in the correct section of the padlet.
Discuss the problem of each scenario and ask the students to consult the workshop's supplementary material to find a solution or best practice.

Discuss whether their way of thinking about the topic of personal data protection has changed using the thinking routine "I used to think..., but now I think...".
Possible questions to be asked are:

- *- What did you used to believe about this topic? (before the workshop started)*
- *- What do you believe now? (at the end of the second session)*

3rd and 4th Session (Title): "The game"

Activities

Discuss the necessity of personal data protection by evaluating the "Three Whys" thinking routine.

- Why does the topic of personal data protection matter to me?
- Why does it concern people around me?
- Why does it matter to the entire world?

Explain the rules of the game and divide the students into six groups.

Game preparation

1. Place the cards with diamonds, mystery cards, and station cards stacked by color at the center or next to the board.
2. Before starting the game, players open the ARTutor application on their mobile or tablet and scan the QR code displayed on the board.
3. On their device screen, a quiz with questions related to the topics covered in the previous sessions will appear. When a player scores above 70%, they can choose a game piece and start the game. They can retake the quiz as many times as needed.

Game start

1. Each player places their game piece on the corresponding starting square on the board based on its color.
2. Draws one newspaper card and one card with five diamonds.
3. Scans the newspaper card to initiate the game.
4. The player who rolls the highest number on the dice goes first. The player to their right follows.

Gameplay

1. The first player rolls the dice and moves the game piece in any direction on the board as many spaces as the number rolled.
   a. If he/she lands on a station square, he/she draws a card from the corresponding station's stack and scans the symbol on it using his/her device. Following the steps presented on the screen in the form of a story, he/she answers some questions. If he/she answers correctly, the player earns the paper diamond

with the color matching the station and keeps the drawn card. If he/she answers incorrectly, he/she does not receive the diamond and places the card at the bottom of the stack. Then, it's the next player's turn.

b. If a player lands on a mystery circle (a circle with a question mark symbol "?"), he/she draws a mystery card and scans it. The following scenarios may occur:

i. He/She will be asked to go directly to any station and choose and draw a card from the respective stack.
ii. He/she will win a bonus of five white diamonds.
iii. He/she will be asked to give one of his/her diamonds to a fellow player.
iv. He/she will be asked to provide/share some personal information in exchange for a diamond (trap - violating Personal Data Protection Principles).

When a player completes one of the actions above, his/her turn ends, and the next player takes their turn.

2. The player who has collected diamonds from all the stations (has collected at least 1 diamond of each color) can scan the card given to the players at the beginning of the game. Once he/she answers all the questions correctly, he/she wins 5 white-colored diamonds. The player has 3 attempts to do so.

Game end

The game ends when all available diamonds are collected.

Game winner

The player who has collected the most diamonds is the winner. A prerequisite is that he/she has collected at least one diamond from each station.

5th and 6th Session (Title): "Become a comic creator"

Activities

Explain to the students their role: "Students will be divided into groups and become creators of their own scenarios in the form of digital comics. *Their scenarios could provide ideas to the creators of the game, and why not? They could be incorporated into it!*" They will implement their own scenario on the theme of Personal Data Protection, inspired by the game they played in the previous two workshops.

Divide the students into groups of 3 people.
Students will open the 1st worksheet (a Microsoft Word document) and organize the story of their comic by answering the following questions:

- What is the title?
- What is the theme? Which social network or online application/page does it concern?
- Who are the characters?
- What personal data will be published?
- What is the problem? (what risks will arise from publishing/sharing)
- How will the problem be solved?

Students will be given printed copies of the second worksheet. Each group will design the cover, the frames of their comic, and fill in the captions and dialogues.

Students will bring their comic to life using the application StoryboardThat and save it on their computer.

7th Session (Title): "Knowledge is turned into action"
Activities
The students will present their comics. You will ask each group to provide feedback and request further details from another specific group. Encourage the students to interact in the discussion using dialogue tools: **Ask**: Request more details to understand your conversation partner's perspective. **Connect**: Comment on a part of the comic that relates to your personal experience or emotion. Afterwards, they will discuss what they learned in this workshop and talk about what impressed them the most. Together, they will create a poster with advice they would give to their peers. Using the "Headlines" thinking routine, each student will write a headline on the poster that summarizes the most important topic discussed in this section. You can create a flipping book with the comics of the groups or print them and create a book. Furthermore, you can discuss the organization of an event with the purpose of raising awareness and informing other students.

7 References

[1] Daskalaki, E., Psaroudaki, K., Karkanaki, M., Fragopoulou, P. (2020). Understanding the online behavior and risks of children: results of a large-scale national survey on 10-18 year old. arXiv:2008.10274v1 [cs.CY]. Available in https://arxiv.org/abs/2008.10274

[2] Schneier, B. (2014). Choosing secure passwords. Available in https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Available in https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

[4] EDPB, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2018. Available in https://edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en

[5] EDPB, Guidelines 01/2022 on data subjects' rights – Right of access, 2022. Available in https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en

[6] Article 29 Working Party, Opinion 2/2010 on online behavioural advertising, 2010. Available in https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

[7] EDPB, Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognize and avoid them. 2022. Available in https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en

[8] Hellenic Data Protection Authority Web site https://www.dpa.gr/

[9] The Australian Parenting Website (https://raisingchildren.net.au/)

[10] EU Kids Online, "Survey results from 19 countries", 2020. Available in https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf

[11] Greek Safer Internet Center, "Online behavior of students aged 10-17 years old in Greece", 2018. Available in https://saferinternet4kids.gr/wp-content/uploads/2019/06/2019-%CE%B5%CF%81%CE%B5%CF%85%CE%BD%CE%B1-%CE%B3%CE%B5%CE%BD%CE%B9%CE%BA%CE%BF-EN.pdf