Training material and methodology

Deliverable D4.1

Editors
Efrosini Siougle (HDPA)
Kyriaki Karakasi (HDPA)
Contributors
Simos Retalis (UPRC)
Maria Alikakou (HDPA)
Katerina Chatzidiakou (HDPA)
Eleni Kapralou (HDPA)
Amalia Logiaki (HDPA)
Reviewers
Costas Lambrinoudakis (UPRC)
Vasilios Zorkadis (HDPA)
Date
31st May 2023

Classification
Public

Funded by the European Union

The byDefault project is funded by the Citizens, Equality, Rights and Values Programme (CERV) of the European Union under grant agreement No. 101074939. Views and opinions expressed are however those of the project partners only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

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, 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 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.
4. Development of an electronic collaboration space open to DPOs and privacy professionals, fostering the exchange of general and, especially, specialized knowledge, such as information that is sector-specific or concerns on the practical applicability of technologies.
5. Launch of the platform, creation of a critical mass of content and users (DPOs and privacy professionals), monitoring and assessment of its operation till the end of the project and beyond.
6. Maximization of byDefault impact, through dissemination, networking and sustainability of project results; byDefault aims at being a project of high impact in the Greek society, with a European dimension.

This work package, WP4, is linked to the strategic goal of raising data protection and privacy awareness among children. During this WP an online in-service teacher professional development program will be designed, deployed and evaluated. Thus, it aims at the following objectives:

- To set up a training strategy and methodology for teachers
- To prepare appropriate training material for teachers
- To develop and operate a teachers' training platform
- To provide training to several elementary and secondary school teachers

The WP4 deliverables will be:

- D4.1 – Training material and methodology
- D4.2 – Training platform
- D4.3 – Teachers' training activities

This deliverable for an online in-service teachers' professional development program on personal data protection and privacy will provide a comprehensive overview of the program's philosophy and structure. In addition to outlining the program's philosophy and structure, the document will also provide information about the current state of in-service teachers' professional development in Greece. By including this information, the document will provide a broader context for the development of the online in-service teachers' professional development program on personal data protection and privacy, as well as help readers understand how it fits into the larger landscape of professional development for teachers in Greece.

The document is intended for educators, educational administrators, and policymakers who are interested in implementing this program as well as designing similar programs in their schools or regions.

The philosophy of the program will be based on the principles of self-directed learning, experiential learning, recognition of prior knowledge and experience, and addressing the hierarchy of needs. These principles will guide the development of the program and its delivery to participants. The document will provide a clear description of how these principles will be applied and how they will help in-service teachers develop their skills and knowledge related to personal data protection and privacy.

The structure of the program will be detailed in the deliverable, including the specific topics and skills covered, the duration of the program, and the methods of delivery, such as online courses, webinars, and interactive activities. It will also outline the requirements for participation, and the criteria for successful completion of the program.

2 In-service teachers' professional development in Greece

In-service teachers' professional development in Greece is primarily organized and provided by the Ministry of Education, Research and Religious Affairs. The Ministry has established various programs and initiatives to support teachers' ongoing professional development and to ensure that they remain up to date with the latest research and best practices in their field.

One of the main programs offered by the Ministry is the Continuing Professional Development (CPD) programme[1], which is designed to provide teachers with ongoing training and support throughout their careers. The CPD program includes a range of activities, such as seminars, workshops, online courses, and conferences, covering a wide range of topics related to teaching and learning.

In addition to the CPD program, the Ministry has also established a network of Teacher Training Centres (TTCs)[2] throughout the country. These centres offer a variety of professional development opportunities for teachers, including training courses, workshops, and conferences on a range of topics related to teaching and learning. The TTCs also provide access to educational resources and support services, such as mentoring and coaching, to help teachers improve their practice.

Furthermore, various universities and educational organizations in Greece offer postgraduate programs and courses for teachers who wish to specialize in a particular area of teaching or to advance their professional qualifications. These programs are usually offered in the form of master's or doctoral degrees, and they provide teachers with the opportunity to deepen their knowledge and skills in a particular field of education.

Recently, the Ministry has also established the Digital Skills for Teachers (Di.S.T.E.) program[3], which aims to provide teachers with the necessary digital skills and competencies to effectively integrate technology into their teaching practice. The program offers a range of training courses and resources for teachers on topics such as online safety, digital citizenship, and the use of educational technology in the classroom.

In Greece, in-service teachers' professional development programs are offered by universities and other institutions to help teachers improve their teaching skills and knowledge in specific subjects. These programs are generally voluntary and conducted outside regular school hours.

The professional development programs offered by Greek universities are diverse and cover a broad range of topics such as teaching methodology, subject-specific pedagogy, educational technology, and classroom management. The programs are designed to provide teachers with the knowledge and skills necessary to adapt to the changing needs of students and to keep up with advances in teaching practices.

Greek universities, via their Lifelong Learning Centres, also offer long-term professional development programs that provide teachers with the opportunity to gain in-depth knowledge and skills in specific subject areas. These programs are usually short-term, lasting from a few days to several weeks, and are focused on specific topics. They may be delivered in-person or online, and include lectures, group discussions, and practical workshops. They often feature experts in the field who share their knowledge and experience with participants. These programs enable teachers to learn from experts, collaborate with peers, and stay up to date with advances in teaching practices, all while improving their knowledge and skills in specific areas of education.

To participate in in-service teachers' professional development programs offered by Greek universities Lifelong Learning Centres, teachers must meet specific requirements such as holding a bachelor's degree or having a certain amount of teaching experience. In some cases, participants are required to pass an entrance exam or demonstrate their language proficiency.

Overall, in-service teachers' professional development in Greece is designed to provide teachers with ongoing training and support to help them improve their teaching practice and remain up to date with the latest developments in their field. By participating in these programs and initiatives, teachers can continue to develop their knowledge and skills, ultimately benefiting their students and the wider educational community in Greece.

2.1 Theoretical principles of the in-service teachers' professional development program

The theory of Maslow, Kolb, and other adult education theorists can be applied to an online in-service teachers' professional development program on personal data protection and privacy, as follows:

- Emphasize self-directed learning: Maslow's theory [6]emphasizes that individuals have a natural drive to learn and develop. In an online in-service teachers' professional development program, this can be supported by providing opportunities for self-directed learning, such as allowing teachers to choose topics of interest or offering personalized learning paths. This can help to increase motivation and engagement.
- Incorporate experiential learning: Kolb's experiential learning theory[4] emphasizes the importance of hands-on, practical experience. In an online environment, this can be facilitated through virtual simulations, case studies, or interactive activities. This can provide opportunities for teachers to apply new concepts and skills in a safe and supportive environment.
- Recognize prior knowledge and experience: Other adult education theorists, such as Malcolm Knowles[5], emphasize the importance of recognizing and building upon adult learners' prior experiences and knowledge. In an online in-service teachers' professional development program, this can be facilitated through opportunities for reflection, peer-to-peer learning, and collaborative activities.
- Address the hierarchy of needs: Maslow's hierarchy of needs emphasizes the importance of meeting physiological, safety, love and belonging, esteem, and self-actualization needs. In an online in-service teachers' professional development program, this can be supported by ensuring that the program is accessible and easy to use, providing a safe and supportive learning environment, and recognizing teachers' achievements and contributions.

Moreover, self-directed learning is an important aspect of an effective in-service teachers' professional development program. It involves the learner taking responsibility for their own learning, including setting goals, identifying resources, and evaluating their own progress. This approach acknowledges that adults have different learning needs and preferences and are more motivated when they have control over their learning process.

In the context of in-service teachers' professional development, self-directed learning has several advantages. Firstly, it enables teachers to tailor their learning experiences to their individual interests and needs. This personalized approach ensures that teachers receive relevant and meaningful training that can enhance their teaching practice.

Secondly, self-directed learning is more motivating for teachers than traditional professional development programs because it allows them to take ownership of their learning. When teachers have a say in what they learn and how they learn it, they are more invested in the process and more likely to apply what they have learned in their classrooms.

Thirdly, self-directed learning promotes lifelong learning skills that are essential for ongoing professional growth and development. By developing self-directed learning skills, in-service teachers become more confident and effective lifelong learners who can adapt to new developments in their field.

To support self-directed learning, in-service teachers' professional development programs can offer flexible learning options, such as online courses or self-paced modules. By empowering teachers to take ownership of

their own learning, programs can foster a culture of ongoing professional growth and development in the education sector. They can also provide coaching and mentoring to help teachers set goals, identify resources, and evaluate their own learning progress. Additionally, programs can facilitate peer collaboration and knowledge sharing.

In summary, an online in-service teachers' professional development program should apply the theory of Maslow, Kolb, and other adult education theorists by emphasizing self-directed learning, incorporating experiential learning, recognizing prior knowledge and experience, and addressing the hierarchy of needs. By doing so, the specific program can support the ongoing growth and development of teachers as professionals.

2.2 Overall instructional and learning objectives of an online teacher training course on personal data protection and privacy

2.2.1 Instructional Goal

To enable teachers to understand the importance of personal data protection and privacy and develop strategies for protecting their own and their students' personal data online.

2.2.2 Learning Objectives

By the end of the course, participants will be able to:

- Define personal data protection and privacy and explain why it is important in the context of education.
- Identify common types of personal data that are collected and stored online in educational settings.
- Understand legal and ethical obligations for protecting personal data in school environment.
- Evaluate the risks associated with personal data breaches and develop strategies for mitigating those risks.
- Implement best practices for protecting personal data, including creating strong passwords, using secure networks, and avoiding sharing personal data with third-party apps and services.
- Explain the importance of educating students on personal data protection and privacy and develop strategies for teaching students about safe online behavior.
- Conduct an audit of their own personal data practices and make changes to ensure compliance with legal and ethical obligations for personal data protection and privacy.

By achieving these learning objectives, participants in the course should be better equipped to protect personal data and educate students on personal data protection and privacy in online educational settings.

2.2.3 Principles

The principles for the online teachers' professional development program on personal data protection and privacy will be:

- *Student-Centered Approach*: The course should focus on protecting students' personal data and empowering teachers to help students protect their own data.
- *Practical and Relevant*: The course should provide practical strategies that teachers can apply in their own classrooms and relevant to the specific context of their teaching.
- *Interactive and Engaging*: The course should use a variety of interactive and engaging activities to help teachers stay motivated and interested, such as case studies, role-playing exercises, quizzes, and group discussions.

- *Ongoing Support*: The course should provide ongoing support to teachers, including resources, online communities, and coaching, to help them implement what they have learned and stay up-to-date on the latest developments in personal data protection and privacy.
- *Collaborative*: The course should encourage collaboration and networking among teachers to share best practices, learn from each other, and build a community of practice around personal data protection and privacy.
- *Customizable*: The course should allow for customization to meet the specific needs and goals of individual teachers, including providing opportunities for teachers to pursue areas of interest or specialization within the broader topic of personal data protection and privacy.

By following these principles, an online professional development program can help ensure that teachers are equipped to protect their students' personal data and empower students to protect their own data online.

3 Description of the professional development program

3.1 Program's general objectives

The training 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 teachers in order to understand the importance of students' 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 through Webinars and messages or comments in the Forum provide a safe environment and enhance incentives to achieve the expected learning outcomes.

3.2 Detailed learning objectives per module

The modules of the training program share common structure. They are structured in sub-modules, in particular when it is necessary to better organise and present relevant educational material and learning activities. Initially, in-service teachers will have the opportunity to participate in a Webinar, organized by each specialist, in order to analyse through discussions the themes of the modules, to answer questions and to carry out micro-activities (tasks). Online meetings will be recorded so that all participants can attend the lectures at any time. Then, asynchronously, teachers will study the educational material and participate in learning activities, which will be a kind of formative assessment, thus ensuring the achievement of the learning outcomes per module (written deliverables, quizzes, etc.).

3.2.1 Module 1: Introduction to personal data protection - Competent bodies - Definitions and Terms

The first module is structured into three sub-modules.

Sub-module 1A: The protection of personal data as an individual right: Introduction and historical retrospective.

Upon completion of this sub-module, the participants will:

- know that personal data are protected as a human right,
- understand who are entitled to this right,
- be able to distinguish it from the right to the protection of privacy,
- have a general knowledge of the legal texts in which this right is provided for,
- recognize the importance of data protection as a right through protection from the competent authority and courts in the event of an infringement and
- be aware of the right to data protection.

Sub-module 1B: Presentation of the role of the competent bodies: Data Protection Authority (DPA) and European Data Protection Board (EDPB)

Upon completion of this sub-module, the participants will:

- know which is the competent supervisory authority for the enforcement of the data protection legal framework in Greece (Hellenic DPA),
- know the organization, operation, tasks and powers of the HDPA,
- know the European Data Protection Board, its role and responsibilities,
- be informed about the role of the European Data Protection Supervisor,
- be familiar with and able to exercise their rights in relation to these entities.

Sub-module 1C: Explanation and understanding of the basic definitions and concepts of the General Data Protection Regulation (EU) 2016/679 (GDPR).

Upon completion of this sub-module, the participants will:

- know what personal data means and when does processing take place,
- distinguish the difference between “simple” personal data and special categories of data and its practical significance,
- recognize the role of key stakeholders in the processing of personal data (role of data subject, controller, processor, third party, etc.),
- understand the concept of basic data protection terms.

3.2.2 Module 2: Data protection principles – Lawful processing

The second module is structured into two sub-modules.

Sub-module 2A: Principles governing the processing of personal data.

Upon completion of this sub-module, the participants will:

- be familiar with the principles underlying data processing and be able to give examples,
- recognize in practice which principles apply to the different kinds of data processing,
- assess and document through hypothetical scenarios whether a processing principle is violated,
- be able to make sound decisions on personal data management issues based on the application of the data processing principles.

Sub-module 2B: Lawfulness of the processing of personal data.

Upon completion of this sub-module, the participants will:

- understand the importance of the lawfulness of the processing of personal data,
- be able to recognize when a processing is legal and when it is not,
- know the legal bases for lawful processing, including the legal basis of consent,
- be familiar with issues related to the legal basis of consent (e.g.: informed consent, age limits for consent, withdrawal of consent, etc.),
- be able to guide their students to identify the legal basis for data processing,
- be able to guide their students whether to give or not their consent for the processing of their personal data.

3.2.3 Module 3: Transparency – Data subjects’ rights

Upon completion of the third module, the participants will:

- understand the principle of transparency in the processing of students’ personal data,
- understand the content of each of the rights under the GDPR concerning students as data subjects,
- learn how and to whom they may exercise their rights,
- solve practical problems and/or provide solutions to complex situations in the contemporary digital landscape (related, indicatively, to the use of social media networks),
- guide their students to choose the appropriate right for the effective protection of their personal data depending on the circumstances,
- evaluate the knowledge and opinion of their peers.

3.2.4 Module 4: Cyber-Threats against personal data – data security

The fourth module is structured into two sub-modules.

Sub-module 4A: Cyber-Threats against Personal Data

Upon completion of this sub-module, the participants will:

- recognize the different categories of risk regarding data protection (identity theft, phishing, cyberbullying) the students face in the modern digital environment (social networks, video sharing platforms, online gaming platforms),
- understand the consequences of each category of risks for the protection of students' personal data,
- learn best practices for the protection of personal data depending on the risk category.

Sub-module 4B: Personal data security

Upon completion of this sub-module, the participants will:

- be able to advise children on the security of their personal data and on applying appropriate protection measures,
- use an open tool for encrypting personal data,
- access through hypothetical scenarios the consequences of a personal data breach,
- assess the ways of appropriate data management according to the relevant circumstance.

3.2.5 Module 5: Profiling – Tracking technologies

The fifth module is structured into two sub-modules.

Sub-module 5A: Profiling

Upon completion of this sub-module, the participants will:

- know basic technical concepts (artificial intelligence, chat box, machine learning),
- understand the concept of targeted advertising on the internet for the creation of consumer profiles,
- apply practical ways of protections when surfing the internet,
- be able to explain to students how targeted advertising works and how they can be protected.

Sub-module 5B: Tracking technologies

Upon completion of this sub-module, the participants will:

- know key features and concepts of these technologies (face recognition technologies, tracking pixels, cookies),
- identify tracking technologies and consider risks,
- be able to propose appropriate protection measures in relation to these technologies,
- use simple tools to control cookies.

3.2.6 Module 6: Privacy settings – Personal data management

The sixth module is structured into two sub-modules.

Sub-module 6A: Privacy settings

Upon completion of this sub-module, the participants will:

- understand key concepts of privacy and privacy settings,
- understand the practical importance of privacy settings, especially on smartphones and social media,
- be able to explain to students how they can look up and adjust privacy settings through examples
- familiarize themselves with the concept and management of the privacy or data protection policy of an online application/website.

Sub-module 6B: Personal data management

Upon completion of this sub-module, the participants will:

- understand the importance of proper data management,
- be aware of cases where students should retreat on privacy issues
- analyze how someone can indirectly and unconsciously give their own or other persons' personal data online,
- guide students to respect and protect the personal data of other people (e.g. posting on social networks audiovisual material related to their friends or family),
- explain to students the risks of sharing their personal data with strangers, especially on social media.

3.2.7 Module 7: Dark patterns in social networks

Upon completion of the seventh module, the participants will:

- learn about dark patterns and why they are illegal practices,
- know practices that constitute a dark pattern,
- recognize forms of black patterns when surfing the internet,
- provide examples of black patterns,
- use their knowledge to avoid websites that use dark patterns,
- make sound decisions about the management of students' personal data online.

3.3 Performance evaluation

To obtain the certificate of attendance, in-service teachers should participate in the final evaluation and ensure a promotional score. After the completion of the activities of all modules in Moodle (see section 5 below), the quiz, which is the cumulative assessment, becomes apparent to all participants. The performance of the trainees must be equal to or greater than 75 % in order for the participation in the seminar to be considered successful.

3.4 Communication - Interaction

The online training program will take place synchronously and asynchronously with the trainees communicating all the time with each other and with the instructor. The tools to be used in Learning Management System are the Forum and the Chat, while in synchronous teaching participants will use the Zoom platform tools, such as live chat and Breakout Rooms, to exchange views and experiences in a group or classroom.

4 Training platform

For the needs of the training program, the flexible learning management platform Moodle will be used, which:

- will support both different forms of learning depending on how the learning content is presented, the organization of educational activities and the type of interaction between trainer-trainee-learning resources: Asynchronous and synchronous distance digital learning,
- will support, with the right tools, all those involved in the digital learning process — administrators, trainers and trainees — in successfully performing their role.

The main features of the platform are the following:

- It will support multiple/distinct roles in the training process (trainer, trainees, course creator, administrator, assistant instructor, etc.).
- It should be easy to use and functional on different kinds of digital devices. However, the basic training function will be performed on devices that have a sufficiently large screen. Mobile functionality will be limited to access to basic data and communication between users.
- It will be compatible with GDPR policy.
- It should provide linear and non-linear use of educational content, i.e. include research and thematic classification of the learning material offered.
- It will support the posting and distribution to trainees of learning resources of various formats such as text files, presentations, pdf, video and sound, SCORM assets, etc.
- It will provide full support for both Greek and English languages.
- It will provide space for synchronous and asynchronous debates organized in thematic areas per module between trainees and trainers as well as between trainees.
- It will be based on sound and robust open-source technologies to be easily customizable, depending on teaching needs and to provide an economically viable solution.
- It will support open interface protocols with third-party applications that can be used either as educational material creation tools or as services that enhance the education process.
- It will have high standards of digital security.
- It will follow the international standards and international good practices developed in the field of digital learning.

5 Training Material

The modules of the training program will include the basic and complementary material, which will be as follows:

- presentation files
- videos
- scientific articles
- case law of the Data Protection Authority
- guidelines of the European Data Protection Board
- provisions and legal texts
- press releases
- links (e.g. link to access the cookie control tool and encryption tool as well as instructions for use, link to Instagram platform policy)
- images (e.g. screenshots)

In addition, trainees will be invited to carry out interactive evaluation and practice activities. In particular:

1. complete closed-type activities (multiple choice, True/False).
2. answer in writing questions of reflection.
3. participate in discussions in the forum.
4. encrypt data files using an open tool.
5. produce a report using an automated cookie control tool.

5.1 Organization of training flow per module – Correlation with the training material

The educational material and activities per module are detailed in the following tables. The organization of the learning flow per module has been designed with the goal that the learners need about 5-6 hours of work per week.

1st Week — Module 1 Sub-module 1A: Introduction to personal data protection Sub-module 2A: Competent bodies Sub-module 3A: Definitions and Terms			
Sub-module No.	**Activity**	**Material**	**Time (minutes)**
1A.1	Participation in the webinar (1st part)	Webinar	40
1A.2	Study of material	Presentations, articles of legal texts, article from Journal, decision of criminal court, decision of the Hellenic DPA	50
1A.3	Fill in quiz	Quiz with right/wrong questions	20
1A.4	Watch video	Video	5
1A.5	Short commentary of a specific excerpt from video 1A.4	Short answer to forum	10
1A.6	Personal opinion on the above extract of video 1A.4	Forum	10

1B.1	Participation in the webinar (2nd part)	Webinar	30
1B.2	Study of material	Presentations, selected texts on DPA website, EDPB website, EDPS website	25
1B.3	Watch video	Video	5
1B.4	Fill in quiz	Multiple choice Quiz	20
1C.1	Participation in the webinar (3rd part)	Webinar	60
1C.2	Study of material	Presentations, extracts of guidelines referring to basic concepts (such as: Article 29 WP for DPOs, EDPB 7/2020 for controllers — processors, definition of personal data, etc.), decisions of the Hellenic DPA	30
1C.3	Fill in quiz	Quiz with right/wrong questions	20
1C.4	A scenario study	Description of the scenario	15
1C.5	Fill in quiz	Quiz with questions on scenario 1C.4	20

2nd Week — Module 2 Sub-module 2A: Data protection principles Sub-module 2B: Lawful Processing			
Sub-module No.	**Activity**	**Material**	**Time (minutes)**
2A.1	Participation in the Webinar (1st part)	Webinar	60
2A.2	Study of material	Presentations, decisions of the Hellenic DPA	60
2A.3	Fill in quiz	Quiz with right/wrong questions	20
2A.4	Study of scenarios	Description of two scenarios	20
2A.5	Fill in quiz on the two scenarios — checking the correct decision	Quiz with right/wrong questions on scenarios 2A.4	20
2B.1	Participation in the webinar (2nd part)	Webinar	60
2B.2	Study of material	Presentations, publications, extracts of the Hellenic DPA's decisions	40
2B.3	Fill in quiz	Quiz with right/wrong questions	20
2B.4	Explanation of the role of parents/guardians in the consent of minors	Text with word limit	20
2B.5	Study and reflection on the responses of other participants	Explanations, comments in the forum	10

3rd Week — Module 3 Transparency — Data subjects' rights			
Module No.	**Activity**	**Material**	**Time (minutes)**
3.1	Participation in the webinar (1st part)	Webinar, presentation on transparency	50
3.2	Participation in the webinar (2nd part)	Webinar, presentation on the right of access	50
3.3	Study of material	Extract from the EDPB's Guidelines on Transparency	15
3.4	List the 2 characteristics which should govern the information provided in particular to children under the principle of transparency	Forum	15
3.5	Study and reflection on the responses of other participants	Explanations, comments in the forum	10
3.6	Fill in quiz	Quiz on the right of access	20
3.7	Participation in the webinar (3rd part)	Webinar, presentation of rectification and erasure rights	50
3.8	Participation in the webinar (4th part)	Webinar, presentation of rights of processing restriction, portability, objection	55
3.9	Participation in the webinar (5th part)	Webinar, right to human intervention	15
3.10	Study of material	Extract from the Hellenic HDPA's decision	20
3.11	Selection of 2 criteria from the HDPA's decision that are considered by the learner to be the most important for the "right to be forgotten"	List	10
3.12	A scenario study	Description of a scenario on data subjects' rights	10
3.13	Fill in quiz	Quiz with multiple choice questions on scenario 3.12	15
3.14	A scenario study	Description of a scenario on data subjects' rights	10
3.15	Fill in quiz	Quiz with multiple choice questions on scenario 3.14	15
Optional activities			
3.16	Study of scenario and material	Scenario on rights and link to Instagram platform policy	30
3.17	Answer to the question of scenario 3.16	Structured reply form	10
3.18	Study and reflection on the responses of other participants	Explanations, comments in the forum	20

4th Week — Module 4 Sub-module 4A: Cyber-Threats Against Personal Data Sub-module 4B: Data security

Sub-module No.	Activity	Material	Time (minutes)
4A.1	Participation in the webinar (1st part)	Webinar	40
4A.2	Study of material	Presentations, publications, articles	50
4A.3	Fill in quiz	Quiz with multiple choice questions on scenario 4A.2	20
4A.4	A scenario study	Description of the scenario	20
4A.5	Recording of responses of comprehension	Structured reply form for scenario 4A.4	20
4A.6	Study and reflection on other participants' responses	Explanations, comments in the forum	20
4B.1	Participation in the webinar (2nd part)	Webinar	40
4B.2	Study of material	Presentations, Guidelines 1/2021 with appropriate examples of personal data breaches, press releases, articles, Hellenic DPA's decisions	50
4B.3	Fill in quiz	Quiz with multiple choice questions	20
4B.4	Encrypt data file	Instructions for the use of an open tool	40
4B.5	Complete the required information on the encrypted file	Structured reply form	20
4B.6	Study and reflection on other participants' responses	Explanations, comments in the forum	20

5th Week — Module 5 Sub-module 5A: Profiling Sub-module 5B: Tracking technologies			
Sub-module No.	**Activity**	**Material**	**Time (minutes)**
5A.1	Participation in the webinar (1st part)	Webinar	30
5A.2	Study of material	Presentations, publications, articles, videos	50
5A.3	Fill in quiz	Quiz with multiple choice questions	20
5A.4	Study 3 specific examples from websites and/or applications of everyday life	Internet	20
5A.5	Answer brief questions about the above 3 examples	Structured reply form	15
5A.6	Study and reflection on other participants' posts	Explanations, comments in the forum	15
5B.1	Participation in the webinar (2nd part)	Webinar	40
5B.2	Study of material	Presentations, press releases	30
5B.3	Fill in quiz	Quiz with multiple choice and right/wrong questions	20
5B.4	Observation of images	Screenshots of web cookie banners	15
5B.5	Fill in quiz	Quiz with multiple choice and right/wrong questions for activity 5B.4	20

5B.6	Visit 3 websites and accept cookies	Internet	15
5B.7	Use of an automated cookie control tool to gather information on the above 3 websites	Tool and instructions for use	40
5B.8	Create a report for the cookie tool	Report	10
5B.9	Study and reflection on other participants' responses	Explanations, comments in the forum	20

6th Week — Module 6 Sub-module 6A: Privacy settings Sub-module 6B: Personal data management			
Sub-module No.	**Activity**	**Material**	**Time (minutes)**
6A.1	Participation in webinar (1st part)	Webinar	30
6A.2	Study of material	Presentations, links to press release, articles	40
6A.3	Fill in quiz	Quiz with multiple choice questions	20
6A.4	Study of the privacy policy of a specific video sharing application	Internet	30
6A.5	Answer brief questions about the above policy	Structured reply form	30
6A.6	Study and reflect on the responses of other participants in three activities	Explanations, comments in the forum	15
6B.1	Participation in the webinar (2nd part)	Webinar	60
6B.2	Study of material	Presentation	15
6B.3	Fill in quiz	Quiz with multiple choice questions	20
6B.4	Observation of images	Photos/screenshots of posts on social networks	15
6B.5	Answer brief questions about personal data in photos/screenshots	Structured reply form	15
6B.6	Study and reflection on other participants' responses on for activity 6B.5	Explanations, comments in the forum	15
6B.7	A scenario study	Description of the scenario	20
6B.8	Answer brief questions for scenario 6B.7	Structured reply form	20
6B.9	Study and reflection on other participants' responses for activity 6B.8	Explanations, comments in the forum	15

7th Week — Module 7 Dark patterns in social networks			
Module No.	**Activity**	**Material**	**Time (minutes)**
7.1	Participation in webinar	Webinar	80
7.2	Study of material	Presentations, press releases, articles	60

7.3	Fill in quiz	Quiz with right/wrong questions	20
7.4	Study of 3 scenarios	Description of 3 scenarios	30
7.5	Fill in quiz	Quiz with right/wrong questions for the 3 scenarios	20
7.6	Complete matching exercise for the 3 scenarios	Matching columns	20
7.7	Identify dark patterns in 3 scenarios	Multiple choice quiz between four options	20
7.8	Identify the reasons for the specific dark pattern	Multiple choice quiz between three options	20

6 Conclusions

In conclusion, the design of this online seminar on personal data privacy awareness among the critical social group of children for in-service teachers aims to provide a comprehensive and engaging learning experience. By incorporating key principles of adult learning theory, interactive content, and practical examples, we will be creating a learning environment that will foster active participation and deep understanding. Throughout the seminar, participants will be equipped with essential knowledge, strategies, and resources to safeguard personal data and promote digital privacy in their classrooms.

Moreover, this online seminar by its design serves as a crucial step towards empowering in-service teachers to become advocates for personal data privacy. By raising awareness about the potential risks and ethical considerations surrounding data collection and use, we have enabled teachers to make informed decisions in their instructional practices. They are provided with comprehensive and well-structured material which covers the major topics related to crucial data protection issues especially in the challenging data-driven digital environment that children and teachers engage in. By emphasizing the importance of key elements on data protection such as transparency, consent, the exercise of data subject's rights and security measures, we encourage teachers to cultivate a culture of digital responsibility and respect for privacy among their students.

Furthermore, the collaborative and interactive elements of this online seminar will foster a strong sense of community among participants. By providing opportunities for networking, discussion, and sharing of best practices, teachers will be able to learn from one another and build a support network for ongoing professional development. The knowledge and skills that will be gained from this seminar will undoubtedly have a ripple effect, as teachers bring their newfound expertise back to their schools and share it with their colleagues.

Moving forward, the development of this online seminar should focus on continuous improvement and expansion. To ensure its effectiveness and relevance, ongoing evaluation and feedback mechanisms should be implemented. This includes soliciting input from participants through surveys, conducting follow-up assessments, and seeking input from subject matter experts to enhance the content and delivery. Additionally, the seminar should be regularly updated to reflect the evolving landscape of personal data privacy. Technology and legislation related to data protection are continuously evolving, making it essential to keep the seminar up to date with the latest information and best practices. This can be achieved by establishing a dedicated team or committee responsible for monitoring developments and making necessary updates to the content and resources provided.

Furthermore, to effectively integrate the proposed online seminar into existing in-service teachers' professional development, several recommendations can be made. Firstly, collaboration and coordination with educational authorities and institutions should be prioritized. By aligning the seminar with established professional development frameworks and guidelines, it can be seamlessly integrated into existing programs and initiatives.

One approach is to offer the online seminar as a modular or elective component within a broader professional development curriculum. This allows teachers to select topics and self-paced training opportunities that are most relevant to their needs and interests. By offering flexibility in scheduling and delivery formats, such as asynchronous learning modules or live webinars, the seminar can accommodate teachers' busy schedules and varying preferences.

Encouraging teachers to apply what they have learned in their daily practices and providing opportunities for reflection and feedback can further deepen their understanding and integration of personal data privacy principles.

Closing, this online seminar has been meticulously designed to provide a transformative learning experience on a sensitive topic. By addressing the unique needs and challenges faced by educators in an increasingly digital world, we will equip teachers with the strategies and tools necessary to navigate the complex landscape of personal data privacy. Through their enhanced understanding and commitment to digital responsibility, these teachers will play a vital role in shaping a future where privacy is valued and protected in educational settings.

7 Appendix A: Sample Training material

The training material comprises a variety of informative, collaborative and interactive elements in an attempt to provide a comprehensive and engaging learning experience to in-service teachers with the aim to cultivate and strengthen the data protection awareness culture and philosophy. The training material includes the following major elements:

a) the basic and supplementary material from various sources comprising the presentation upon which the webinars are based, scientific articles, summaries and essential parts from decisions, acts and guidelines issued by competent bodies such as the European Data Protection Board and the Hellenic Data Protection Authority and
b) the interactive assessment and practice activities comprising multiple choice and/or True/False questions, written answers, discussions in the forum, use of simple tools for encryption and management of cookies.

The training material is organized into seven (7) modules providing a thorough and comprehensive educational program to educators. The organization of the learning flow per module is designed to include webinars with the use of PowerPoint presentations and activities based on the study of the corresponding material. The full training material per module will be structurally depicted and provided to the in-service teachers through the training platform. The content and flow of the educational material and the activities for the module on "Transparency - Data Subjects Rights" are detailed below.

Module: Transparency - Data Subjects Rights

Activity 3.1: Presentation on transparency for the 1st part of the webinar

Contents

- Conceptual delimitation of transparency in the field of the processing of children's personal data
- Description of the actions of the controller regarding the information provided to children — Reference to the criteria for appropriate information
- Description of the controller's actions in responding to rights enshrined in the GDPR for children — Content of the principle of transparency
- Specification of information to be provided by the controller on the processing of personal data (Articles 13 and 14 GDPR)

Funded by the European Union

Contents

- Time delimitation for providing information to data subjects
- Conditions for further processing in the context of the application of the principle of transparency
- Exemptions from the obligation of controllers to provide information in application of the principle of transparency

Funded by the European Union

The concept of transparency

- Each controller must inform children of any processing of their personal data, of their rights and of incidents of data breaches. They must at all times be able to demonstrate that they adhere to GDPR (principle of accountability).
- Information is provided before any processing takes place and upon special request.

Funded by the European Union

Characteristics of information in the context of transparency

The controller must provide the information mentioned above

- ✓In plain and understandable language, especially when children are addressed
- ✓Briefly
- ✓In such a way that it is immediately and easily visible
- ✓In a single text (the privacy policy)
- ✓Free of charge

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Transparency in the field of children's rights as data subjects

- The controller is obliged to facilitate the exercise of the rights and to act (i.e. to either fulfill the rights or justify the failure to fulfill them entirely or partially) provided that there is no doubt as to the identity of the child.
- The controller must respond to the rights exercised within 30 days of the exercise (unless, within the month, it informs for an extension of up to 2 months). In case of failure to respond, it must again within the month justify the non-response by informing the subject of the possibility to lodge a complaint with the Data Protection Authority.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

6
31/5/2023

Transparency — Articles 13 & 14 GDPR

- The information shall include in particular the following information:

✓ Controller details

✓ Data subject rights

✓ Exercise of data subject rights

✓ Data protection officer's details

✓ Purposes, legal basis for processing

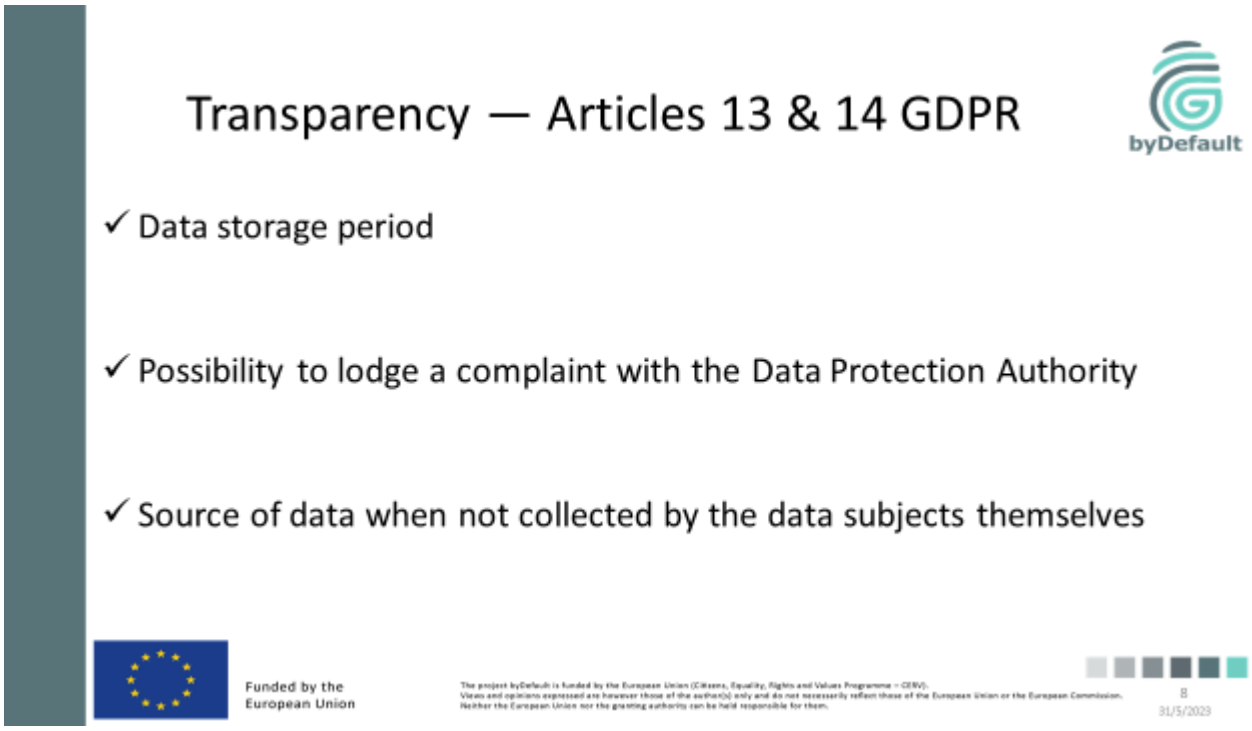
✓ Recipients of data

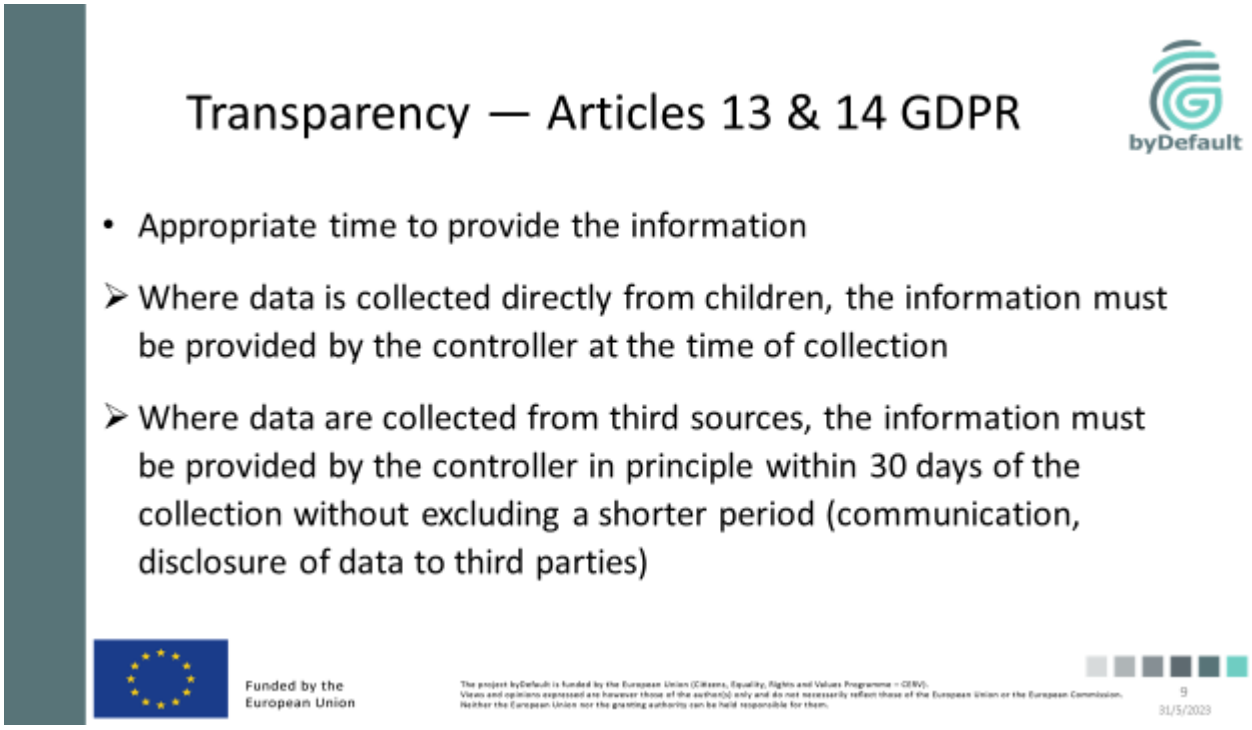
✓ Possibility of withdrawing consent

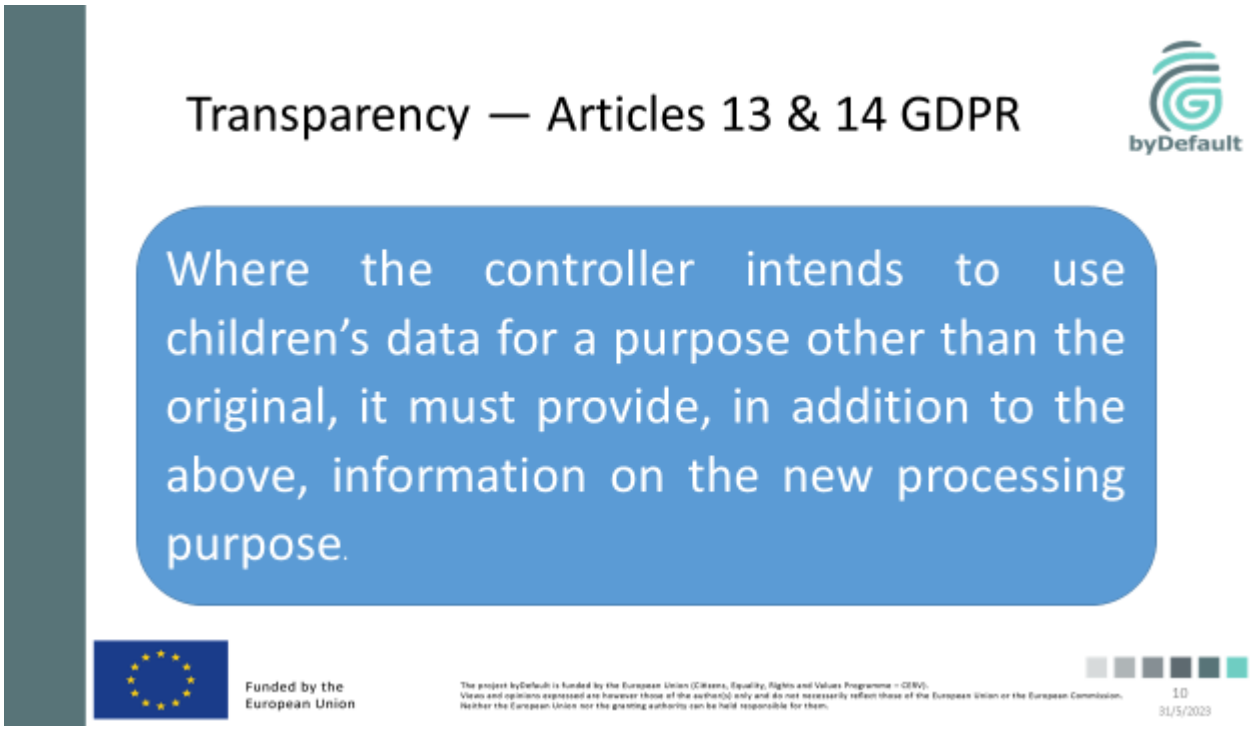
Funded by the European Union

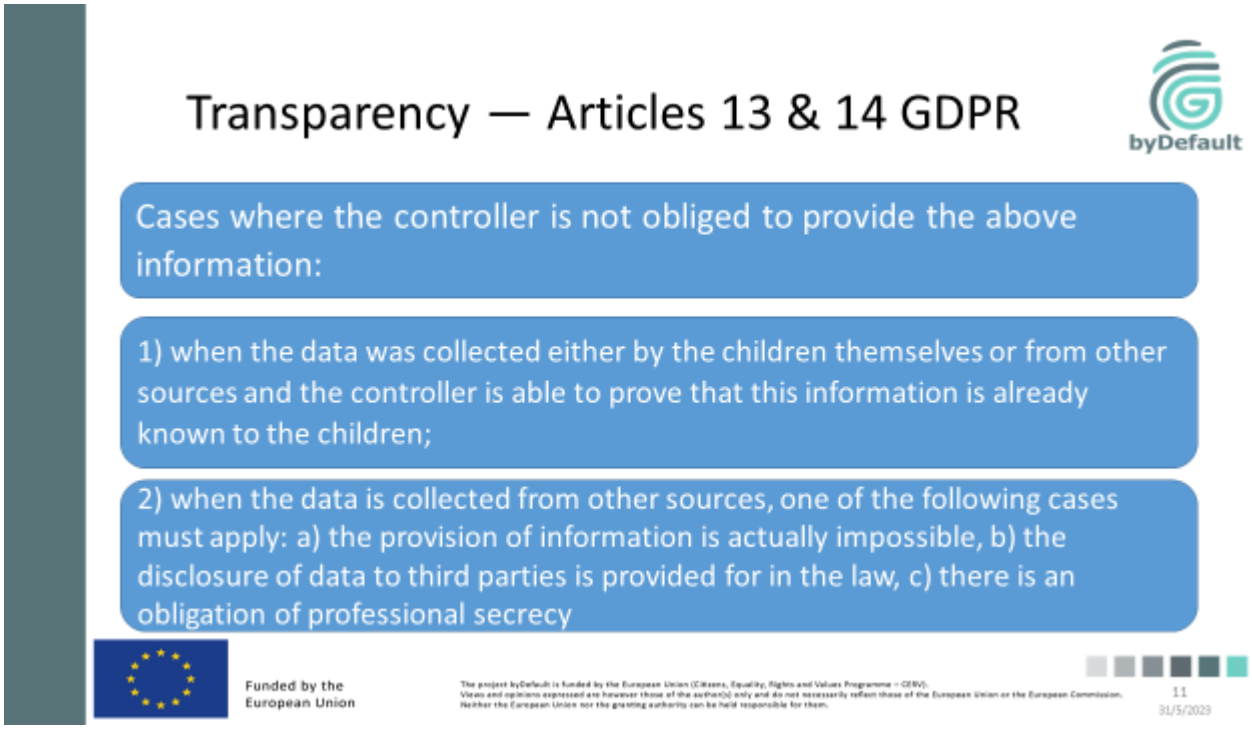
The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

7
31/5/2023


Transparency — Articles 13 & 14 GDPR
byDefault
✓ Data storage period
✓ Possibility to lodge a complaint with the Data Protection Authority
✓ Source of data when not collected by the data subjects themselves
Funded by the European Union
8
31/5/2023

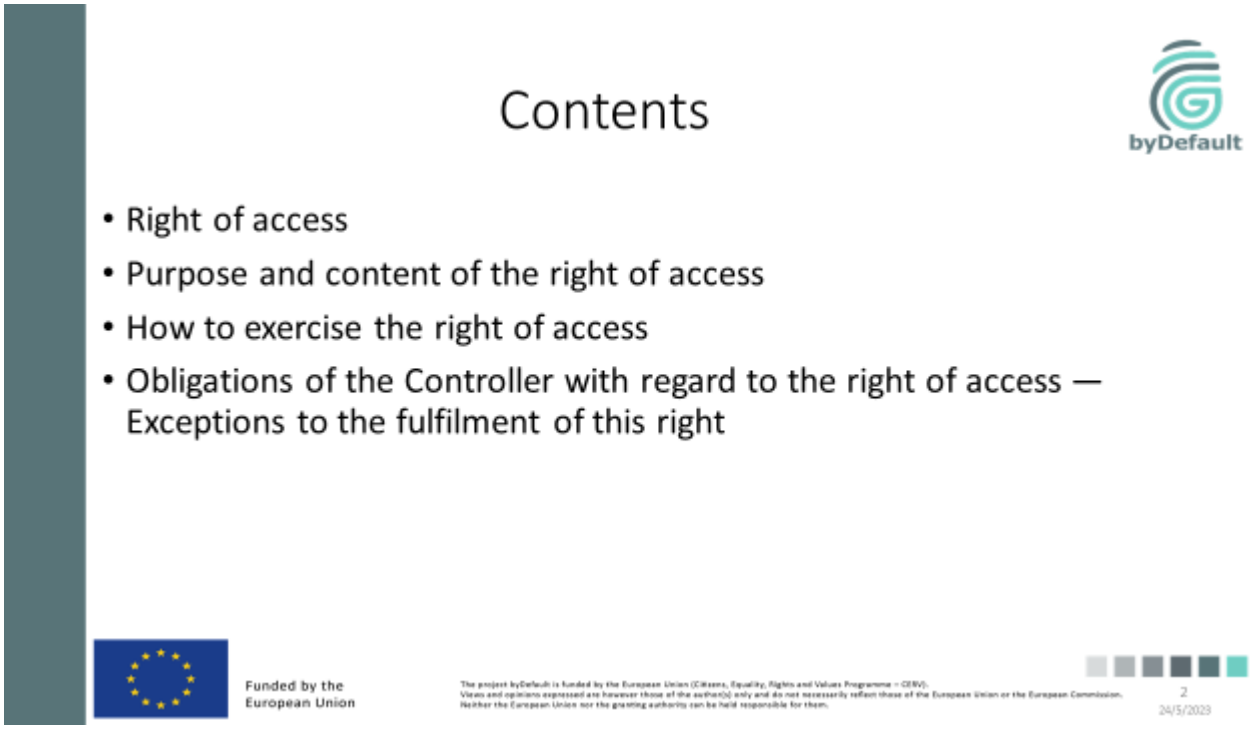

Transparency — Articles 13 & 14 GDPR
byDefault
• Appropriate time to provide the information
➢ Where data is collected directly from children, the information must be provided by the controller at the time of collection
➢ Where data are collected from third sources, the information must be provided by the controller in principle within 30 days of the collection without excluding a shorter period (communication, disclosure of data to third parties)
Funded by the European Union
9
31/5/2023


Transparency — Articles 13 & 14 GDPR
byDefault
Where the controller intends to use children's data for a purpose other than the original, it must provide, in addition to the above, information on the new processing purpose.
Funded by the European Union
10
31/5/2023


Transparency — Articles 13 & 14 GDPR
byDefault
Cases where the controller is not obliged to provide the above information:
1) when the data was collected either by the children themselves or from other sources and the controller is able to prove that this information is already known to the children;
2) when the data is collected from other sources, one of the following cases must apply: a) the provision of information is actually impossible, b) the disclosure of data to third parties is provided for in the law, c) there is an obligation of professional secrecy
Funded by the European Union
11
31/5/2023


byDefault
Thank you for your attention
Funded by the European Union

Activity 3.2: Presentation on the right of access for the 2nd part of the webinar



Right of access — Purpose and content

- In exercising the right of access, the data subject may request a copy of his or her data held by the Controller, information about the processing, while at the same time it is necessarily confirmed whether the subject's data are actually processed.
- The right of access shall ensure:

✓The awareness of the child's data being processed at all times (accuracy, lawfulness)

✓The effective exercise of other rights of the child (e.g. correction, erasure)

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right of access — Purpose and content

In cases where the child exercises the right of access to his/her personal data without further specializing them, the Controller is obliged to provide the whole set of data that is kept and concern the child who exercised the said right.

Only in cases where a very large amount of the child's data is kept, may the Controler ask for further specification.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right of access — How to exercise the right

- The Controller usually provides specific communication channels and standard forms for exercising the right of access.

✓However, if the right of access is exercised through another communication channel indicated by the Controller as a regular contact point, the Controller should make all reasonable efforts to handle such a request.

✓In any case, it is recommended, as good practice, that controllers introduce appropriate mechanisms for the redirection of access requests to the competent department.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right of access — Obligations of the Controller

- The Controller must satisfy within the deadline (see Article 12(3) GDPR) any right of access and is not entitled to ask the data subject the reasons for exercising it. It is far less legitimate to satisfy (or not) the right of access based on the reasons why it is exercised.
- In addition, the Controller must:

✓Carefully evaluate every right of access

✓Inform about the inability to locate the requested personal data

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right of access — Obligations of the Controller

- ✓extend his search for the personal data of the applicant-child to all his information systems and archiving systems in general
- ✓provide the identified personal data in easily accessible form and in clear and easily understandable language
- ✓provide a copy of the requested data either electronically or by other automatic means, and alternative means may be foreseen if requested by the subject (such as on-site access)

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right of access — Obligations of the Controller

The Controller shall ask for additional information about the identity of the data subject when they have doubts about it.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right of access — Exceptions from the obligation to satisfy the right

- The Controller shall not be required to provide children's data that have already been deleted, but he has to provide a relative negative answer.
- Where the Controller demonstrates that the fulfilment of the right of access adversely affects the rights or freedoms of others, the right of access exercised by the child to his or her personal data may be restricted on that basis. It is sufficient, of course, even in these marginal cases to omit only those personal data, the granting of which would have a negative impact on the rights and freedoms of third parties.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

9
26/5/2023

Right of access — The example of Instagram

- Steps to access the user/account holder's data on Instagram:
- 1. In the account profile options, the user selects "Receive data".
- 2. Fill in the e-mail address of the account holder and the password to that account.
- 3. The user then receives an email with a link that leads them to a file to be downloaded.
- This file includes the user's photos and videos, the private messages they have exchanged in the context of conversations on that platform, the likes they have made, their comments on various videos, the people they follow and those they have been blocked. The collection and dispatch of such data, to which the user has requested access in the above manner, may take place within 48 hours of the request.
- For more information on other platforms, see Social media: download everything you've published in one click! | CNIL

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

10
24/5/2023

Right of access — Activity

Study the activity and indicate the correct answer:

The wording in a request for the exercise of the right of access *'I wish to have access to the personal data you keep about me'* means that the controller must provide, if easily possible, all the personal data of the applicant-child, through his or her legal representative.

Please select:

1. Right
2. Wrong

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

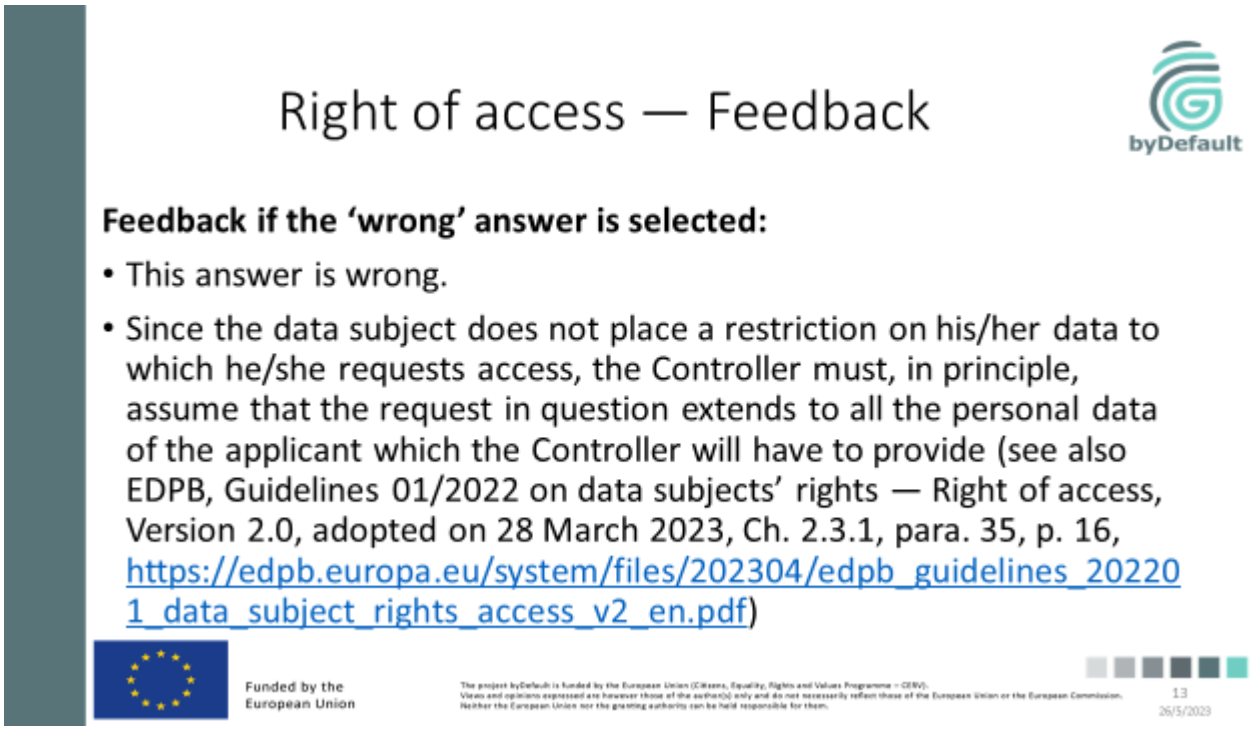
Right of access — Feedback

Feedback if the 'right' answer is selected:

- This answer is correct.
- 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)

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.


Right of access — Feedback
byDefault
Feedback if the 'wrong' answer is selected:
• This answer is wrong.
• 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)
Funded by the European Union
13
26/5/2023


byDefault
Thank you for your attention
Funded by the European Union

Activity 3.3: Please study the paragraphs 12-13 and 14-15 of the "Guidelines on transparency under Regulation 2016/679" of the European Data Protection Board (EDPB) which are available (in the pdf file) below (as well as in the link https://ec.europa.eu/newsroom/article29/items/622227/en).

Paragraphs 12-13 and 14-15 of the EDPB's "Guidelines on transparency under Regulation 2016/679"

"Clear and plain language"

12. With written information (and where written information is delivered orally, or by audio/ audiovisual methods, including for vision-impaired data subjects), best practices for clear writing should be followed. A similar language requirement (for "plain, intelligible language") has previously been used by the EU legislator and is also explicitly referred to in the context of consent in Recital 42 of the GDPR. The requirement for clear and plain language means that information should be provided in as simple a manner as possible, avoiding complex sentence and language structures. The information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations. In particular the purposes of, and legal basis for, processing the personal data should be clear.

Poor Practice Examples

The following phrases are not sufficiently clear as to the purposes of processing:

- *"We may use your personal data to develop new services" (as it is unclear what the "services" are or how the data will help develop them);*

- *"We may use your personal data for research purposes (as it is unclear what kind of "research" this refers to); and*

- *"We may use your personal data to offer personalised services" (as it is unclear what the "personalisation" entails).*

Good Practice Examples

- *"We will retain your shopping history and use details of the products you have previously purchased to make suggestions to you for other products which we believe you will also be interested in" (it is clear what types of data will be processed, that the data subject will be subject to targeted advertisements for products and that their data will be used to enable this);*

- *"We will retain and evaluate information on your recent visits to our website and how you move around different sections of our website for analytics purposes to understand how people use our website so that we can make it more intuitive" (it is clear what type of data will be processed and the type of analysis which the controller is going to undertake); and*

- *"We will keep a record of the articles on our website that you have clicked on and use that information to target advertising on this website to you that is relevant to your interests, which we have identified based on articles you have read" (it is clear what the personalisation entails and how the interests attributed to the data subject have been identified).*

13. Language qualifiers such as "may", "might", "some", "often" and "possible" should also be avoided. Where data controllers opt to use indefinite language, they should be able, in accordance with the principle of accountability, to demonstrate why the use of such language could not be avoided and how it does not

undermine the fairness of processing. Paragraphs and sentences should be well structured, utilising bullets and indents to signal hierarchical relationships. Writing should be in the active instead of the passive form and excess nouns should be avoided. The information provided to a data subject should not contain overly legalistic, technical or specialist language or terminology. Where the information is translated into one or more other languages, the data controller should ensure that all the translations are accurate and that the phraseology and syntax makes sense in the second language(s) so that the translated text does not have to be deciphered or re-interpreted. (A translation in one or more other languages should be provided where the controller targets data subjects speaking those languages.)

Providing information to children and other vulnerable people

14. Where a data controller is targeting children or is, or should be, aware that their goods/ services are particularly utilised by children (including where the controller is relying on the consent of the child), it should ensure that the vocabulary, tone and style of the language used is appropriate to and resonates with children so that the child addressee of the information recognises that the message/ information is being directed at them. A useful example of child-centred language used as an alternative to the original legal language can be found in the "UN Convention on the Rights of the Child in Child Friendly Language".

15. WP29's position is that transparency is a free-standing right which applies as much to children as it does to adults. WP29 emphasises in particular that children do not lose their rights as data subjects to transparency simply because consent has been given/ authorised by the holder of parental responsibility in a situation to which Article 8 of the GDPR applies. While such consent will, in many cases, be given or authorised on a once-off basis by the holder of parental responsibility, a child (like any other data subject) has an ongoing right to transparency throughout the continuum of their engagement with a data controller. This is consistent with Article 13 of the UN Convention on the Rights of the Child which states that a child has a right to freedom of expression which includes the right to seek, receive and impart information and ideas of all kinds. It is important to point out that, while providing for consent to be given on behalf of a child when under a particular age, Article 8 does not provide for transparency measures to be directed at the holder of parental responsibility who gives such consent. Therefore, data controllers have an obligation in accordance with the specific mentions of transparency measures addressed to children in Article 12.1 (supported by Recitals 38 and 58) to ensure that where they target children or are aware that their goods or services are particularly utilised by children of a literate age, that any information and communication should be conveyed in clear and plain language or in a medium that children can easily understand. For the avoidance of doubt however, WP29 recognises that with very young or pre-literate children, transparency measures may also be addressed to holders of parental responsibility given that such children will, in most cases, be unlikely to understand even the most basic written or non-written messages concerning transparency

Activity 3.4: Then identify, based on the paragraphs mentioned in activity 3.3, the two (2) characteristics that the information provided to data subjects should meet in order to satisfy the principle of transparency, especially when the latter are children.

Feedback to Activity 3.4:

According to paragraphs 12-15 of the "Guidelines on transparency under Regulation 2016/679" of the EDPB, the information provided to data subjects by data controllers regarding the processing of their personal data must meet the following two (2) characteristics in order to be consistent with the principle of transparency:

(1) the clarity and

(2) the accuracy

of the statements contained on the data protection policy.

These characteristics, which shall be met in the statements of data controller's privacy policy, become even more important when the information is provided to children, in order to remove any doubts or ambiguity regarding the processing of their personal data.

Activity 3.5: Please study and reflect on the responses of the other participants in the forum.

Activity 3.6: Please fill in the following quiz: study he multiple choice questions and indicate the correct answers.

Question 1: Which of the following cannot be the content of a right of access? Select the correct answer.

1.1. copies of the applicant's recorded calls;

1.2. information on the recipients of the applicant's data;

1.3. copies of data concerning the applicant's spouse;

1.4. information on the time of storage of the applicant's data

Question 2: The child sends, through their legal representative, a request for access to their personal data 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. The child does not 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 do you advise the child, through their legal representative, to do? Select one or more correct answers.

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

2.2. 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;

2.3. to contact the Data Protection Authority;

2.4. to contact the Controller by phone.

Feedback on activity 3.6 for question (1):

Feedback if option is (1.1) is selected: This answer is wrong. 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.

Feedback if option (1.2) is selected: This answer is wrong. 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'.

Feedback if option (1.3) is selected: This answer is correct. A data subject's right of access cannot, in principle, cover data relating to third parties.

Feedback if option (1.4) is selected: This answer is wrong. 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".

Feedback on activity 3.6 for question (2):

Feedback if answer (2.1) is selected: 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, 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 not mandatory for the child to resubmit the request by sending it to another address of the same controller.

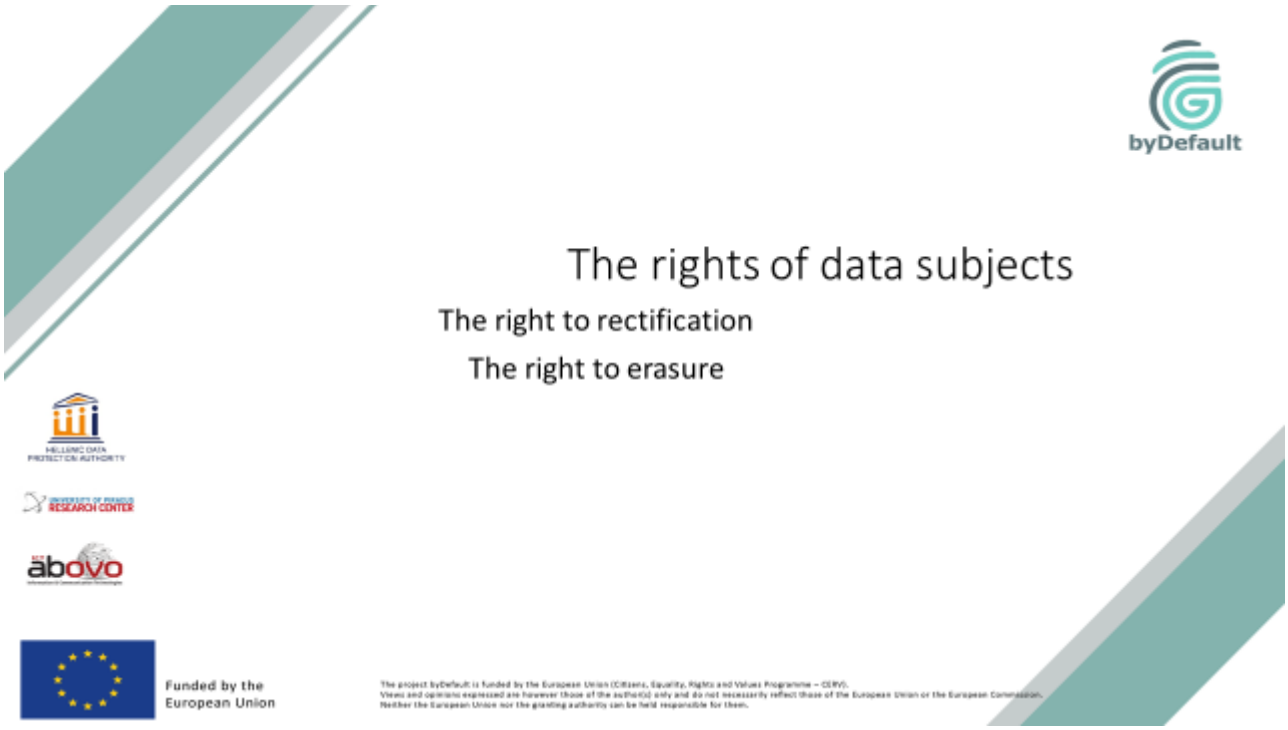
Feedback if answer (2.2) is selected: This answer is correct. If a right of access is clearly and explicitly formulated and is brought to the attention of the controller through a communication channel provide by the controller, and even addressed to an e-mail address indicated for regular customer communication with the company, the controller must examine it even if 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.

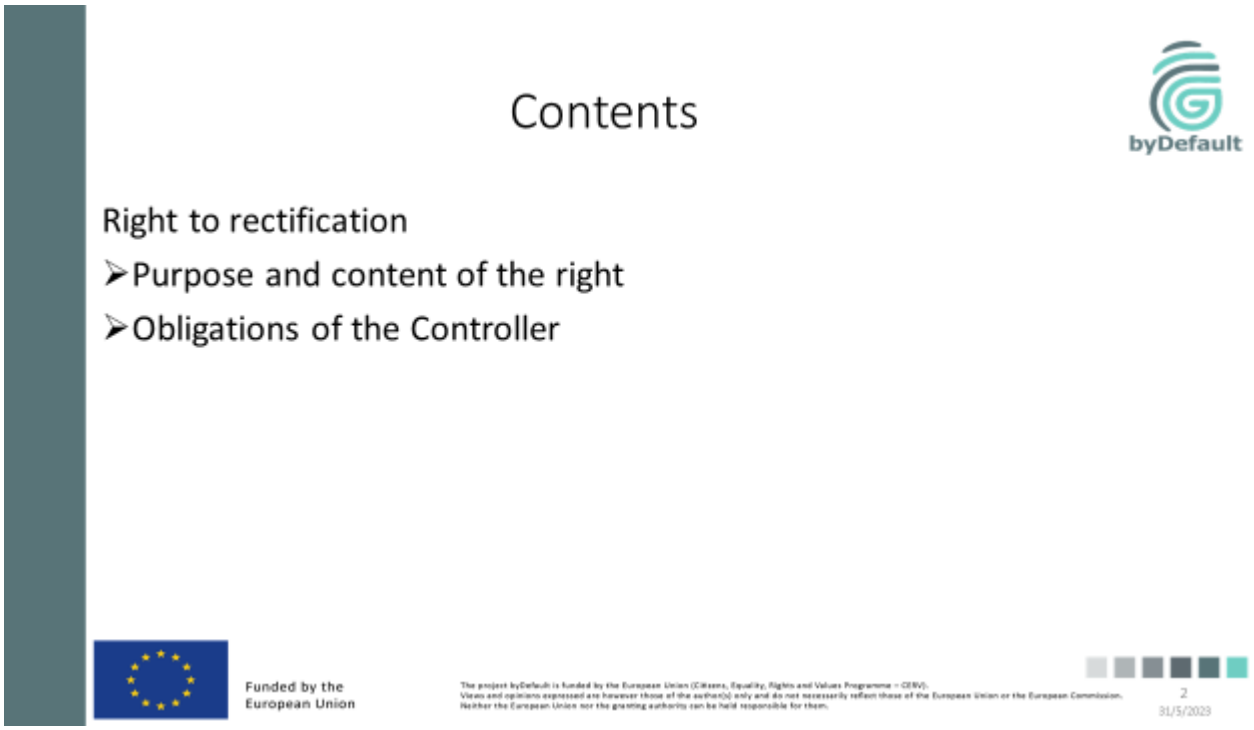
Feedback if answer (2.3) is selected: This answer is wrong. The child is not recommended to lodge a complaint with the Authority, through their representatives, before 30 days have elapsed since the exercise of the right of access and provided that no reply has been received from the controller. This 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.

Feedback if answer (2.4) is selected: 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 — 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).

Activity 3.7: Presentation of rectification and erasure rights for the 3nd part of the webinar





Contents

Right to erasure

- Purpose and content of the right
- Obligations of the Controller
- Exemptions from the obligation to fulfill the right
- "Right to be forgotten" — deletion of results in search engines

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right to rectification — Purpose and content

In exercising the right to rectification, the child may request, through his or her legal representatives,

- ✓that inaccurate information concerning him or her be rectified in particular where an incorrect impression may emerge from the data already existing,
- ✓or that his/her data be supplemented, if this, in particular, serves the purpose of the processing.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right to rectification — Obligations of the controller

The controller must respond within the deadline (Article 12(3) GDPR) to the right to rectification

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right to erasure

- In the context of the right to erasure, the erasure of personal data of the child processed by a Controller may be requested.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right to erasure— Obligations of the controller

- The controller shall erase the child's personal data when:

✓they are no longer necessary in relation to the purposes for which they were collected or otherwise processed

✓the data subject (DS) withdraws the consent on which the processing is solely based

✓the data subject objects to the processing (article 21(1) GDPR) and there are no compelling legitimate grounds for the processing or objects to the processing in accordance with Article 21(2) GDPR

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right to erasure

➢In the context of the right to erasure, the erasure of personal data of the child processed by a Controller may be requested.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right to erasure— Obligations of the controller

- The controller shall erase the child's personal data when:

✓they are no longer necessary in relation to the purposes for which they were collected or otherwise processed

✓the data subject (DS) withdraws the consent on which the processing is solely based

✓the data subject objects to the processing (article 21(1) GDPR) and there are no compelling legitimate grounds for the processing or objects to the processing in accordance with Article 21(2) GDPR

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

7
31/5/2023

Right of erasure — Obligations of the controller

✓the data have been unlawfully processed

✓the erasure is provided by Union or Member State law

✓the data have been collected with the consent of the child in relation to the provision of information society services referred in Article 8(1) GDPR and the child then exercises the right to erasure.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

8
31/5/2023

Right to erasure — Obligations of the controller

- The controller shall inform accordingly all other controllers who have received or republished the deleted data, so that they also refrain from any processing thereof
- This obligation of the controller is automatic and therefore there is no need for the child to ask for this
- Exemption from the above obligation: if the provision of information is proved unfeasible or involves a disproportionate effort. The Controller shall inform the data subject about those recipients, if so requested by the data subject.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right of erasure — Exceptions from the obligation to fulfill the right

- The right to erasure does not apply when processing is necessary

✓for the exercise of the right to freedom of expression and the right to information

✓to comply with a legal obligation requiring the Controller to process or perform a task carried out in the public interest or in the exercise of official authority vested in the Controller (therefore, in this case, the need to keep the data stems from a provision of law)

✓for reasons of public interest in the field of public health (see Article 9(2)(h) and (i) as well as Article 9(3) GDPR)

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right of erasure — Exceptions from the obligation to satisfy the right

- ✓for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89(1), where the right to erasure is likely to render impossible or seriously impair the achievement of the purposes of such processing
- ✓for the establishment, exercise or defense of legal claims
- See Art. 17(3) GDPR.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

"Right to be forgotten" — erasure of results in search engines

- When the child's details appear on a publicly accessible website as a result of a search on relevant search engines (e.g. Google), he or she has the right to request from the search engine, through his or her legal representatives, that the website in question does not appear in the search results based on his/her data. If the search engine refuses to comply with such requests, it is obliged to substantiate the reasons on the basis of specific criteria (see EDPB Guidelines 5/2019)

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

"Right to be forgotten" — erasure of results in search engines

- The "right to be forgotten" does not lead to the erasure of the children's data from the original websites. To achieve this, children should, at all times through their legal representatives, address independently to the Controllers who operate each website.
- Through the "right to be forgotten" only the non-appearance of specific results (websites) from a search engine based on the child's data may be achieved.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

"Right to be forgotten" — erasure of results in search engines

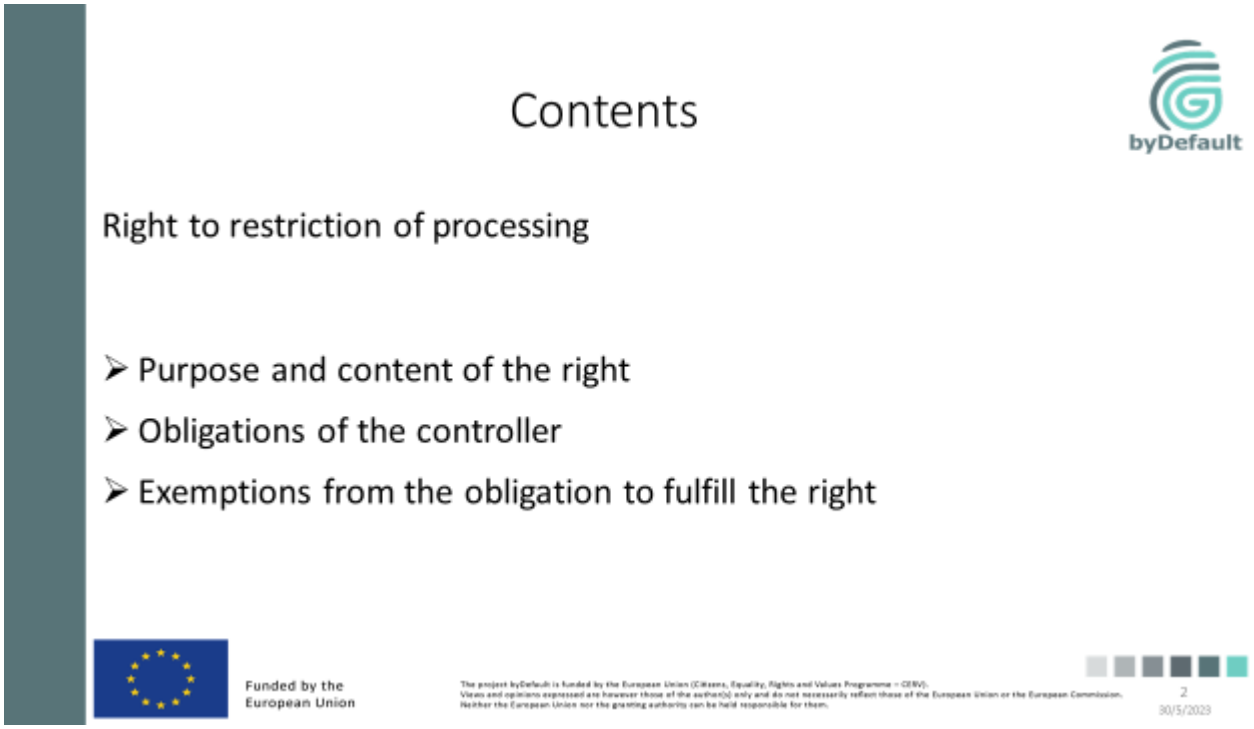
- For the form to be submitted for google search engine, see https://reportcontent.google.com/forms/rtbf

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.


byDefault
Thank you for your attention
Funded by the European Union

Activity 3.8: Presentation of rights of restriction of processing, portability, objection for the 4th part of the webinar



Contents

- Right to data portability
  - Purpose and content of the right — Ways of fulfilling the right
  - Conditions for establishing the possibility of exercising the right
  - Obligations of the controller
  - Exceptions to the obligation to fulfil the right
  - Question — example (tik tok platform)

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Contents

Right to object

- Purpose and content of the right
- Obligations of the controller
- Exceptions to the obligation to fulfil the right

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right to restriction of processing — Purpose and content

- With the right to restrict processing, the child may request that any specific processing of his or her data be stopped as long as it is still kept by the controller.
- This is the fundamental difference between this right and the right to erasure, where the controller ceases to keep the deleted data.

Funded by the European Union

Right to restriction of processing — Purpose and content

- In order to be entitled to request the restriction of the processing of his or her data:
  - the child must question the accuracy of the personal data. In this case the restriction of processing lasts for a period of time sufficient to allow the controller to verify the accuracy of the data; or
  - the processing is unlawful and the child objects to the erasure of such data and requests instead the restriction of their use; or
  - the controller no longer needs the child's data for the purposes of processing, but such data are required by the child him/herself for the establishment, exercise or defense of legal claims; or
  - the child must object to the processing in accordance with Article 21(1) of the GDPR (which will be analyzed below), in which case the restriction of the processing of the data in question is requested, while verification of whether the legitimate grounds of the controller prevail over the grounds of the child is pending.
- See Art. 18(1) GDPR

Funded by the European Union

Right to restriction of processing — Obligations of the controller

byDefault

- The controller must comply with the right to restrict processing within the time limit laid down in Article 12(3) of the GDPR.
- The controller shall inform the child when the restriction of the processing requested is lifted.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right to restriction of processing — Exceptions from the obligation to satisfy the right

byDefault

- Where processing has been restricted following the exercise of the child's right, such data shall be processed — apart from being kept —

✓ only with the consent of the child; or

✓ for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person; or

✓ for reasons of important public interest of the Union or of a Member State.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right to data portability — Purpose and content — Ways of fulfilling the right

With this right, the child is entitled to request from the controller — through their legal representative — the data they have already provided.

The child is entitled to receive the data in question in an appropriate format so as to be able to transfer it easily to another controller.

This right ensures

✓ more control over children's data

✓ ability to move, copy or transfer their data from one computer system to any other

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right to data portability — Conditions for exercising the right

- In order for the right to data portability to be exercised:

➢ the processing must be based on consent (see Article 6(1)(a) or 9(2)(a) GDPR) or on a contract (see Article 6(1)(b)); or

➢ the processing must be carried out by automated means

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right to data portability — Obligations of the Controller

- The controller must comply with the right to data portability within the time limit laid down in Article 12(3) of the GDPR.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right to data portability — Exceptions from the obligation to fulfill the right

Controllers shall not be obliged to fulfil the right to data portability where:

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in the exercise of public functions or in compliance with a legal obligation of the controller

However, even in these cases, the controller must provide

- ✓ negative reply to the relevant requests
- ✓ information on this matter (see Art. 13 and 14 GDPR).

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right to object — Purpose and content of the right

- By exercising the right to object (Article 21 GDPR), the child may object to the processing of their data by the controller
- concerning their particular situation (special family situations, any legal needs, etc.),
- for the performance of a task carried out in the public interest or in the exercise of official authority entrusted to the controller
- or for reasons of legitimate interests of the same or a third party.

Funded by the European Union

Right to object — Obligations of the controller

- The controller shall provide children as data subjects with explicit, clear and independent information on the right to object. This information shall take place at the latest on the first contact with them. In other words, the controller must inform the children explicitly of the existence of the right to object and of the way in which they can exercise it before them.
- The controller must comply with the right to object in principle within the time limit laid down in Article 12(3) of the GDPR.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right to object — Obligations of the Controller

- The controller shall be obliged to stop processing if the right to object is exercised, unless is proved that there are compelling legitimate grounds for continuing the processing of the child's data in question, as those grounds override the fundamental rights and freedoms of the child who has exercised that right.
- When the controller processes children's data for direct marketing, it must always fulfill the relevant right to object which may be exercised and immediately cease processing for the purposes of marketing.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Right to object — Exceptions from the obligation to fulfill the right

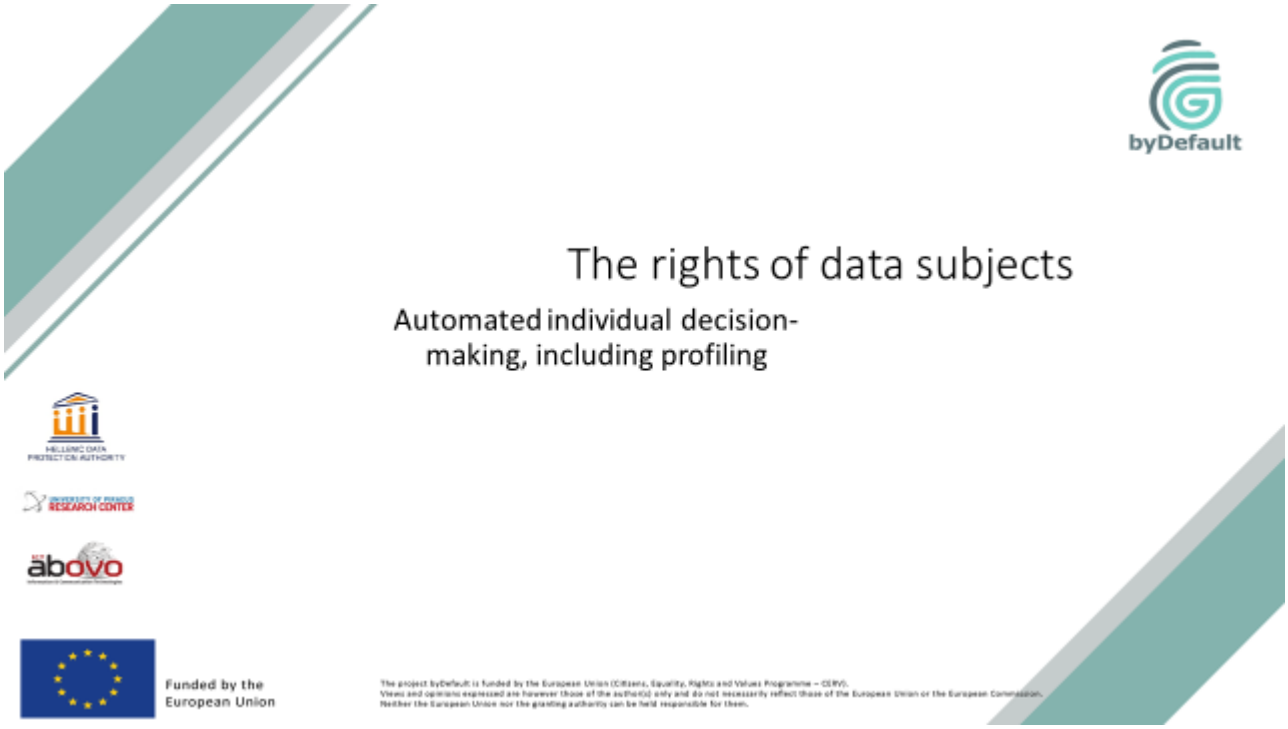
- Where the data of the child are processed for statistical or scientific or historical research purposes, even if a right of objection has been exercised on grounds relating to the particular situation of the child, this cannot be fulfilled if the processing in question is necessary for the performance of a task carried out for reasons of public interest.

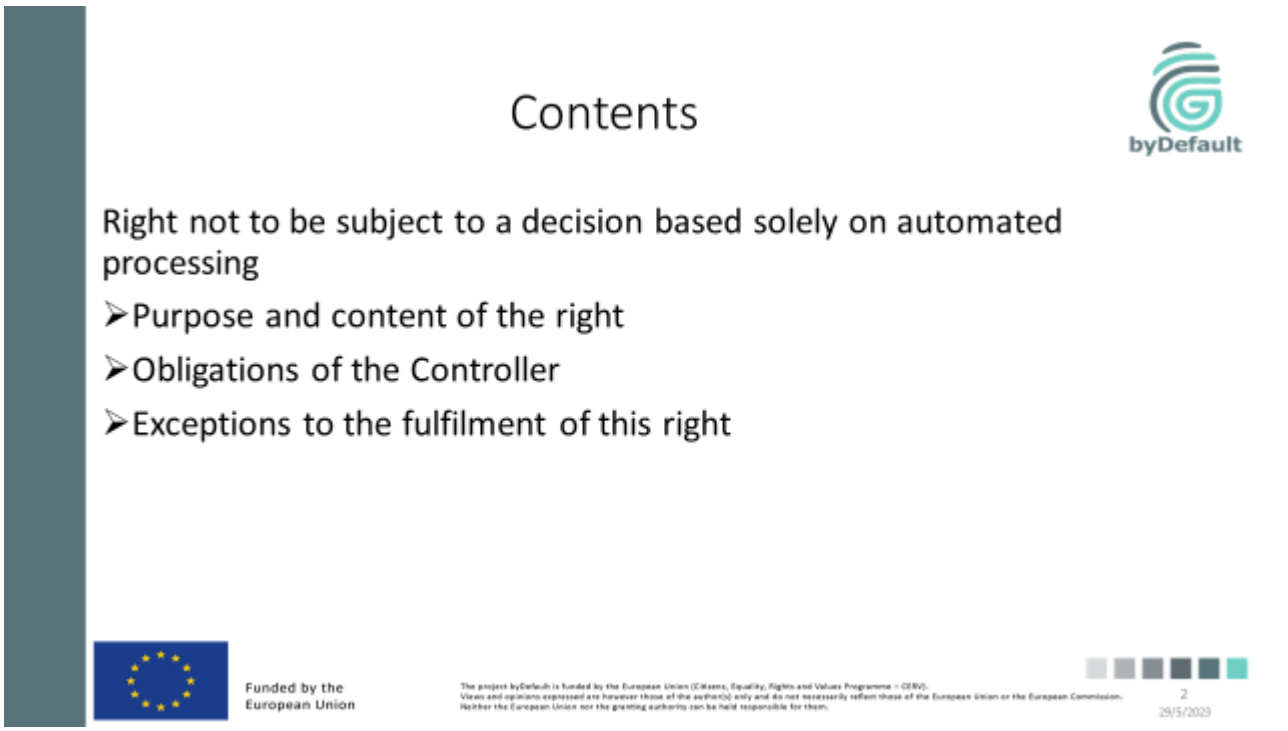
Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.


byDefault
Thank you for your attention
Funded by the European Union

Activity 3.9: Presentation on automated individual decision-making, including profiling for the 5th part of the webinar





Purpose and content

In the context of this right

- the data subject (DS) is given the possibility not to be subject to a decision reached without human intervention and which significantly affects its legal situation, including the creation of a profile (for the definition of a profile, see article 4 (4) of the GDPR)
- a general prohibition is established to decisions entailing serious consequences for the legal status of a DS on the basis of processing without human intervention

Funded by the European Union

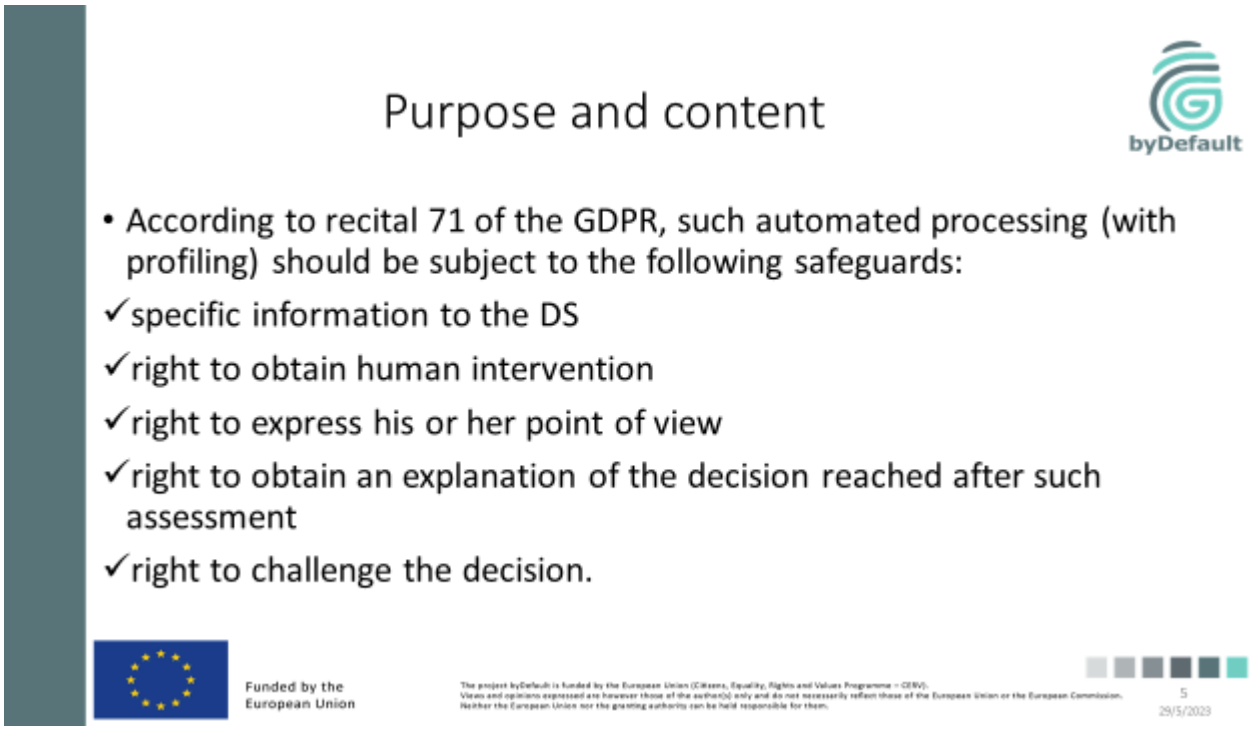
Purpose and content

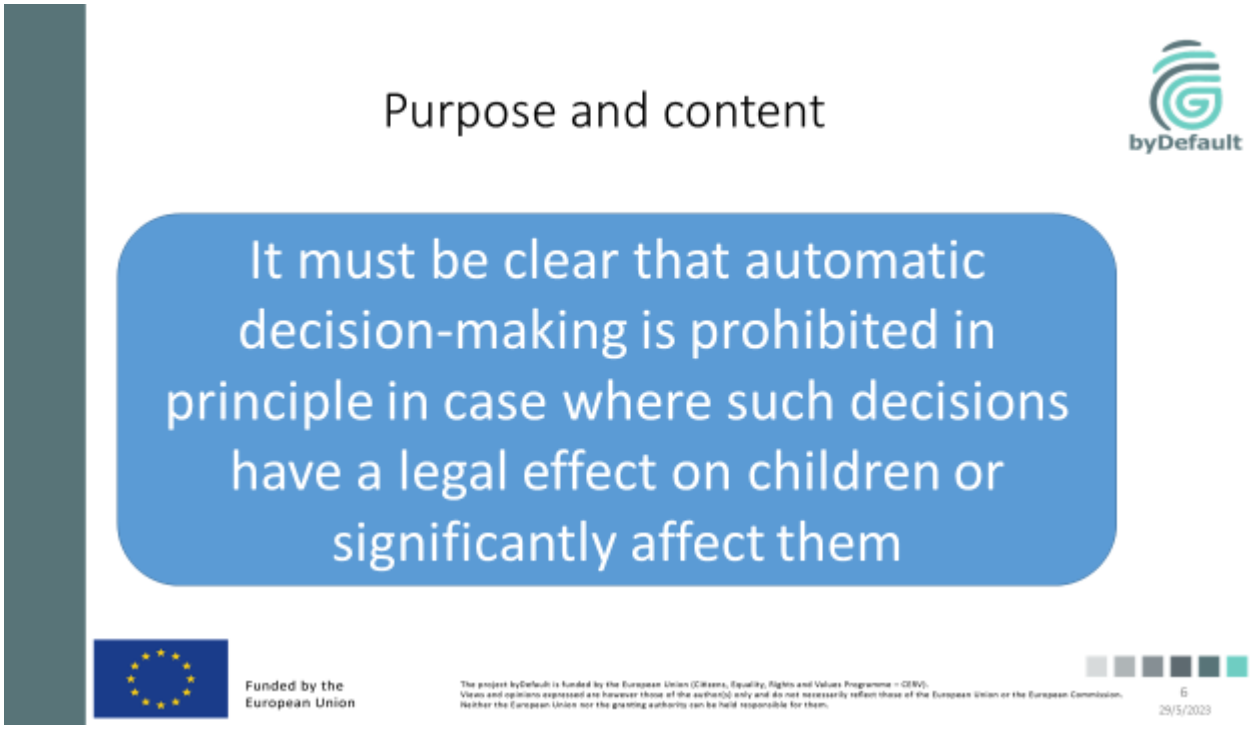
- The GDPR provided for this right due to the ever-increasing use of artificial intelligence in many areas of public and private life (e.g. commercial promotion and advertising) which allow decision-making and accurate profiling without human intervention therefore posing serious risks to DS:

➢ they may be unaware of the existence of profiling or the data processed for its creation and/or

➢ they may be unaware of the logic by which an algorithm makes decisions about them.

Funded by the European Union


Purpose and content
byDefault
• According to recital 71 of the GDPR, such automated processing (with profiling) should be subject to the following safeguards:
✓specific information to the DS
✓right to obtain human intervention
✓right to express his or her point of view
✓right to obtain an explanation of the decision reached after such assessment
✓right to challenge the decision.
Funded by the European Union
5
29/5/2023


Purpose and content
byDefault
It must be clear that automatic decision-making is prohibited in principle in case where such decisions have a legal effect on children or significantly affect them
Funded by the European Union
6
29/5/2023

Obligations of the controller

- In case of profiling of children, the Controller shall provide clear information regarding the processing of their data. Under no circumstances should the Controller take advantage of their inability to understand or the weak position of children in general.
- In addition, **profiling of children for marketing purposes is prohibited**.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Obligations of the controller

- In cases of automated individual decision-making, the Controller must make it clear to the DS through relevant information, which will be provided to them whether the data is collected by them or not.
- The controller should include information on the logic used to reach the automated decision as well as explanations on the consequences of the processing each time for the DS.

Funded by the European Union

The project byDefault is funded by the European Union (Citizens, Equality, Rights and Values Programme – CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Obligations of the controller

- ✓To ensure fair and transparent processing in respect of the DS, the Controller should, as the case may be,
- ➢use appropriate mathematical or statistical procedures for the profiling,
- ➢implement technical and organizational measures to correct the factors which result in inaccuracies in personal data and to minimize the risk of errors
- ➢secure the data by taking into account the potential risks involved with the interests and rights of the DS and preventing, inter alia, discriminatory effects on the basis of racial or ethnic origin, political opinions, etc. (recital 71 of the GDPR).

Funded by the European Union

The project byDefault is funded by the European Union (CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Exceptions to the fulfilment of this right

- There are cases where the right not to take automated decisions does not apply (see article 22 par. 2 GDPR):
- ✓the decision is authorized by Union or Member State law to which the Controller is subject and which also lays down suitable measures to protect the rights, freedoms and legitimate interests of the DS, or
- ✓the decision reached is necessary for entering into or performance of a contract between the DS and the Controller or
- ✓the decision is based on the explicit consent of the DS.
- In the last two exceptions, the Controller must apply appropriate measures to protect the rights, freedoms and legitimate interests of the DS

Funded by the European Union

The project byDefault is funded by the European Union (CERV).
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission.
Neither the European Union nor the granting authority can be held responsible for them.

Activity 3.10: Please study the following Decision (with number 25/2019) of the Hellenic Data Protection Authority available below and on its website (https://www.dpa.gr/el/enimerwtiko/prakseisArxis/prosfygi-kata-tis-arnisis-toy-forea-ekmetalleysis-tis-mihanis-anazitisis), with emphasis on point (e) (page 33-34 of the Decision). Point (e) specifies the criteria that the Authority weighs, in order to assess the refusal by the search engine to remove specific links that appear in the search results on the basis of the name of the data subject.

Start of the extract from the HDPA's decision 25/2019

THE HELLENIC REPUBLIC

DATA PROTECTION AUTHORITY

Athens, 25-07-2019

Ref. No: G/EX/5225/25-07-2019

DECISION No. 25/2019

(Chamber)

The Data Protection Authority met at the invitation of its President to a Chamber meeting at its headquarters on 17 July 2019, following its ordinary meeting of 13 March 2019 and the postponement of its meeting of 30-01-2019 in order to examine the case referred to in the case history of this Decision.

(...)

The Authority took into account the following:

'A' submitted to the Authority the appeal with Ref. No. … (as supplemented by Ref. No. … document) concerning the refusal of Google LLC (hereinafter, Google) to remove/delete the links mentioned in the complaint, which appear in the search results of the company's relevant search engine on the basis of the complainant's name, both in Greek characters ("...") and in English characters ("...").

(...)

e. The Article 29 Working Party, in its Opinion of WP 225, 26-11-2014, developed a list of common assessment criteria for the European data protection authorities' handling of relevant appeals lodged at their national offices following the refusal to delete/remove links by search engines. This list of common evaluation criteria is the framework that National Data Protection Authorities apply in their decision-making processes, but also which they can jointly enrich by building on the experience they will gain over time. The common assessment criteria are as follows:

i. Does the search result relate to a natural person, i.e. an individual? And does the search result appear based on the name of the data subject?

ii. Does the data subject play a role in public life? Is he/she a public figure?

iii. Is the data subject a minor?

iv. Is the data accurate?

v. Is the data relevant and not more than needed?

vi. Is it about the subject's professional life?

vii. Is the search result linked to information allegedly constituting hate speech/slander/defamation or similar offences in the area of expression against the applicant?

viii. Does the data reflect a personal opinion or does it appear to be a confirmed fact?

ix. Is it sensitive personal data?

x. Is the data up-to-date? Is the data available for longer than necessary for the intended purpose?

xi. Does the disclosure of the data have a disproportionate negative impact on the privacy of the data subject?

xii. Is the result of the search linked to information that puts the data subject at risk?

xiii. What are the general circumstances in which the data were published? Has this data been made public by the subject him/herself? Could there be a reasonable expectation from the subject that the data will be made public?

xiv. Has the original text been published in the context of journalistic purposes?

xv. Does the data publisher have the legal power or legal obligation to make the data available to the public?

xvi. Does the data relate to a criminal offence?

In accordance with the above Opinion/Guidelines, these criteria should be applied in accordance with the relevant national legislation and no single criterion alone is decisive. Similar assessment criteria have also been developed by a number of data protection authorities, such as the UK Authority (I.C.O.).[1]

(...)

FOR THESE REASONS

The Data Protection Authority,

1) unanimously rules that Google Inc's response to the present request by Applicant 'A' is not legally justified in the cases of links 7, 10 and 15, on the basis of the legitimate assessment criteria set out in the grounds hereof.

2) orders, pursuant to Article 58(2)(c) of Regulation (EU) 2016/679, Google LLC, as controller, to immediately remove the above-mentioned links and the link numbered 37 above.

(3) addresses a reprimand to GOOGLE LLC based on Article 58(2)(b) of Regulation (EU) 2016/679 for the above mentioned violation of the provisions of Art. 12 of Regulation (EU) 2016/679.

The Deputy President **The Secretary**

Giorgos Batzalexis Irini Papageorgopoulou

End of the extract from the HDPA's decision 25/2019

Activity 3.11: Then indicate which two (2) of the criteria from Decision 25/2019 you consider to be most important at your discretion.

Select from the list:

i. Does the search result relate to a natural person, i.e. an individual? And does the search result appear based on the name of the data subject?

ii. Does the data subject play a role in public life? Is he/she a public figure?

iii. Is the data subject a minor?

iv. Is the data accurate?

[1] HTTPS://ico.org.uk/for-organisations/search-result- delisting-criteria/

v. Is the data relevant and not more than needed?
vi. Is it about the subject's professional life?
vii. Is the search result linked to information allegedly constituting hate speech/slander/defamation or similar offences in the area of expression against the applicant?
viii. Does the data reflect a personal opinion or does it appear to be a confirmed fact?
ix. Is it sensitive personal data?
x. Is the data up-to-date? Is the data available for longer than necessary for the intended purpose?
xi. Does the disclosure of the data have a disproportionate negative impact on the privacy of the data subject?
xii. Is the result of the search linked to information that puts the data subject at risk?
xiii. What are the general circumstances in which the data were published? Has this data been made public by the subject him/herself? Could there be a reasonable expectation from the subject that the data will be made public?
xiv. Has the original text been published in the context of journalistic purposes?
xv. Does the data publisher have the legal power or legal obligation to make the data available to the public?
xvi. Does the data relate to a criminal offence?

Feedback on activity 3.11:

Please navigate by clicking on the following link: https://support.google.com/legal/answer/10769224?hl=en, in order to establish the similarities between the above criteria mentioned in Decision 25/2019 of the Authority and those weighted by the Google search engine when it receives those requests to delete specific links that appear in the search results by the name of the applicant-data subject.

Activity 3.12: Please study the following scenario and indicate the correct answer:

A 5th grade student submits to the Secretariat of his/her school, through his/her legal representative (his/her mother), a court decision for the recognition of a child. By virtue of this decision the surname of the student has been altered.

What GDPR right will you direct the student to exercise (through his/her mother) before his/her Primary School, so that the corresponding modification of his surname in the records kept at the school takes place?

1. right to rectification

2. right of access

3. right to restriction of processing

4. right to data portability.

Feedback on activity 3.12:

Feedback if answer (1) is selected: This answer is correct. This right to rectification is exactly the one that satisfies the student's request. Through the exercise of this right the accuracy of the student's personal data in the school records will be restored as the correct family name will be recorded from now on.

Feedback if answer (2) is selected: This answer is wrong. The access right does not satisfy the student's request. The student is not requesting access to his/her data.

Feedback if answer (3) is selected: This answer is wrong. The right to restrict the processing is not suitable to satisfy the student's specific request. The issue at stake here is not to suspend the processing of the students' data and retain his/her old surname, as it is already listed in the school records, instead of his new surname after the recognition that took place.

Feedback if answer (4) is selected: This answer is wrong. The right to portability is not appropriate to satisfy the student's request in this case. The student is not requesting to receive from the controller the data that he/she (the student) made available to the former, in an appropriate format, so that the student can make them available to another controller.

Activity 3.13: After reflecting the correct answers on the scenario described in activity 3.12 please study the following additional scenario and indicate the correct answer:

Immediately afterwards, the student, again through his/her mother in this case, wishes until the already exercised right to modify the student's data in the school records is examined and satisfied accordingly, to delay as much as possible the publication of the electronic school newspaper, which has a great impact as it is posted on the school's website, so that the student is listed with his new surname as member of the editorial team of this newspaper.

What right will you direct the student to exercise, through his/her mother before the Primary School, in order to satisfy this request and to prevent the publication of the electronic newspaper so that he is included in it with his new surname?

1. right to erasure

2. right to rectification

3. right to restriction of processing

4. right of data portability.

Feedback on activity 3.13:

Feedback if answer (1) is selected. This answer is wrong. The right to erasure is not suitable to satisfy the student's request for the correct inclusion of his new surname in the electronic school newspaper. The issue at stake here isn't the deletion of his surname. The student essentially requests that no processing takes place (that his old surname is not reproduced in the school newspaper) until the request for the modification of the student's data in the school records is examined and satisfied, so that his new surname is written in the editorial team.

Feedback if answer (2) is selected. This answer is wrong. The right to rectification is not appropriate to satisfy the student's request for the correct inclusion of his new surname in the school newspaper. And this because the issue is not to correct his name and indeed at a time when the online newspaper has not yet been published and posted on the school website. Besides, the right to rectification cannot prevent the school from reproducing

the old surname in the newspaper until the examination and (accordingly) satisfaction of the request to change the student's surname in the school records takes place.

Feedback if answer (3) is selected. This answer is correct. The right to limit the processing is exactly what serves the student at the present time that his request for modification of his personal data (of his surname on the basis of the court decision submitted) in the school records has not yet been considered. This right will allow the student to "freeze", to suspend any processing of his data, i.e. the reproduction of his name in the electronic school newspaper as it is before the recognition, until the request regarding the modification of his surname, as it is kept in the school records, is examined and accordingly satisfied in order to subsequently take place the proper processing regarding the correct inclusion of the student's new surname as a member of the editorial team in the electronic school newspaper

Feedback if answer (4) is selected. This answer is wrong. The right to portability is not objectively adequate to satisfy the student's request. In this case, the student is not requesting to receive from the controller the data that he/she (the student) made available to the former, in an appropriate format, so that the student can make them available to another controller.

Activity 3.14: Please study the following scenario and indicate one or more correct answers:

Suppose a child is staring into a shop window in a busy shopping mall. Someone steals his/her backpack just outside the shop. For the protection of persons and goods, a camera had been installed capturing the shop's entrance. The data controller has the obligation delete the data captured by the camera every 15 days, at the latest, if they do not need them for their own purposes. The child is entitled to obtain a copy of the visual material at issue showing that he/she was the victim of the attack.

In view of the above, which of the following rights would you advise the child to exercise –through his/her legal representatives– in order to obtain the material in question which will help identify and arrest the offender?

1. Right to object

2. Right to erasure

3. Right to restriction of processing

4. Right of access

Feedback on activity 3.14:

Feedback if option (1) is selected: This answer is wrong. The right to object in the present case cannot de facto satisfy the child's request, as the child does not object to the processing of their data, that is to say, to the fact that they were filmed as they gazed at the shop window in the shopping mall. On the contrary, in the present case, the processing of their data through the camera is desirable, in order to assist the authorities in the arrest of the offender.

Feedback if option (2) is selected. This answer is wrong. The right to erasure in this case cannot de facto satisfy the child's request, as the deletion of the video depicting the moment of the theft of the backpack by the offender contradicts the child's request.

Feedback if option (3) is selected: This answer is the correct. By exercising the right to restrict processing, the child will be able to satisfy his/her request because the controller will be prevented from erasing the video in

question, which the controller would otherwise erase since its retention time is very limited and the latter does not need it; this video, however, is necessary for the child to establish a legal claim against the offender.

Feedback if option (4) is selected: This answer is the correct. The right of access clearly satisfies the child's request; by exercising it the child will be able to receive from the controller the video footage concerning him/her and help him/her establish their legal claims.

Activity 3.15: After reflecting the correct answers on the scenario described in activity 3.14 please study the following additional scenario and indicate the correct answer:

Who will you direct the child to contact, through his or her legal representatives, in order to exercise his/her rights as specified in the scenario described in activity 3.14? Select one or more correct answers.

1. To the shop outside of which the child was robbed.
2. To the police.
3. To anyone indicated in the relevant policy (of the website) of the shopping mall as being the controller with regard to the data collected through the video surveillance system.
4. To anyone indicated as being the controller on the information sign of the video surveillance system.

Feedback on activity 3.15:

Feedback if option (1) is selected: This answer is wrong. In so far as it is a shop in a shopping mall, it is not absolutely certain that the controller, before which the relevant rights of the child may be exercised, would be that shop, although the video at issue depicts the window of the specific shop.

Feedback if option (2) is selected: This answer is wrong. The police is in no way the controller as far as video surveillance in private places –such as the shop within the shopping mall– is concerned.

Feedback if option (3) is selected: This answer is correct. The correct course of action of each data subject in such cases is in principle to consult the policy and/or the sign in the place where it is located (in this case the shopping mall). Furthermore, each controller must have a relevant sign (with or without QR code) with its details and how to exercise the rights of the GDPR. In fact, each controller must provide appropriate information, both electronically and manually, by supplying, for example, relevant information leaflets on the above topics in a counter. In addition, the company operating the shopping mall must have a privacy policy on its website, which the child, via his/her legal representatives, must consult before exercising the above rights.

Feedback if option (4) is selected: This answer is correct. The correct course of action of each data subject in such cases is in principle to consult the policy and/or the sign in the place where it is located (in this case the shopping mall). Furthermore, each controller must have a relevant sign (with or without QR code) so data subjects can easily determine the controller responsible for any existing cameras in the mall and how they may exercise their rights. In fact, each controller must provide appropriate information, both electronically and manually, by supplying, for example, relevant information leaflets on the above topics in a counter. Furthermore, the company operating the shopping mall must have a privacy policy on its website, which the child, via its legal representatives, must consult before exercising the above rights.

8 References

[1] Ministry of Education, Research and Religious Affairs (2019). Continuing Professional Development Program for Teachers. Retrieved from http://www.minedu.gov.gr/publications/docs2019/CPD_teachers_2019.pdf

[2] Teacher Training Centers (n.d.). About TTCs. Retrieved from https://www.iep.edu.gr/en/teacher-training-centers/about-ttcs

[3] Digital Skills for Teachers (n.d.). About Di.S.T.E. Retrieved from https://diste.edu.gr/en/about-digital-skills-for-teachers-diste/

[4] Kolb, D. A. (1984). Experiential learning: Experience as the source of learning and development. Prentice-Hall.

[5] Knowles, M. S. (1975). Self-directed learning: A guide for learners and teachers. Association Press.

[6] Maslow, A. H. (1943). A theory of human motivation. Psychological Review, 50(4), 370-396.

[7] Mezirow, J. (1991). Transformative dimensions of adult learning. Jossey-Bass.

[8] Brookfield, S. D. (2017). Becoming a critically reflective teacher. Jossey-Bass.