Co-funded by the
Erasmus+ Programme
of the European Union

DiSCVET
TOOLBOX for VET teachers / trainers

Development of the Digital Sovereignty
Competences of VET teachers and trainers

DiSCVET

BBB Bundesverband der Träger beruflicher Bildung (Bildungsverband) e. V.
Germany

MUNDUS Bulgaria
Bulgaria

Greece

VERNIAN rti
Cyprus

MIITR
Slovenia

BK·CON
Germany

petit pas
Italy

Created by MIITR
• May 2023

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
[Projektnummer: 2020-3-BE05-KA205-003110]

1 Contents

DiSCVET **TOOLBOX**

DiSCVET

PROJECT: Development of the Digital Sovereignty Competences of VET teachers and trainers

Available in BG, DE, EN, GR, IT, SI!

WHY?

Digital sovereignty is a new concept in the digital era suggesting that parties should have sovereignty over their digital data. On an individual level, digital sovereignty demonstrates the capacity of individuals to own their data and control its use. People often struggle to appreciate the importance of privacy since the consequences of privacy violations are hard to gauge due to their elusive nature.

WHAT

A new innovative form of training content along with an online simulation platform

FOR WHO

VET teachers/trainers, VET organizations, education providers, authorities, experts/decision makers

WHERE

discvet-hub.eu
discvet.eu
facebook.com/discvet

Includes material on:

- Managing Digital resources
- Personal data and Privacy
- Information Security Management
- Risk Management
- Information and Knowledge Management

IO2 Online platform & training material

A creative training material that aims to equip VET teachers/trainers with the necessary competences to increase their digital sovereignty and enable them to train others. The training material comprises a bundle of digital learning resources using the micro-learning concept. These digital learning nuggets feature various resources such as interactive games, e-learning videos, interactive case studies, infographic resources, and more.

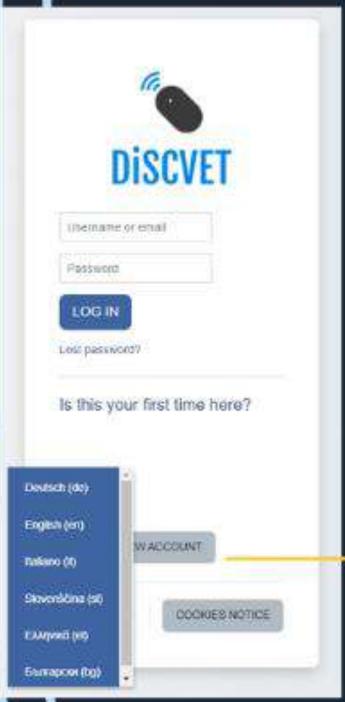
IO3 Simulation exercises

A transition to a practical setting is made via simulation exercises mimicking real-life use, introducing new apps, methods and tools, and allowing users to gain hands-on experience. The exercises enhance knowledge retention, as users will be able to apply the principles of digital sovereignty and digital security to practical situations, such as cyber-attacks, security breaches, phishing, malware and others.

Learn more about the results, how to use them, pilot testing and national initiatives regarding digital security education! ⟶

How to use the platform?

(discvet-hub.eu/)



DiSCVET

Username or email

Password

LOG IN

Lost password?

Is this your first time here?

Deutsch (de)

English (en)

Italiano (it)

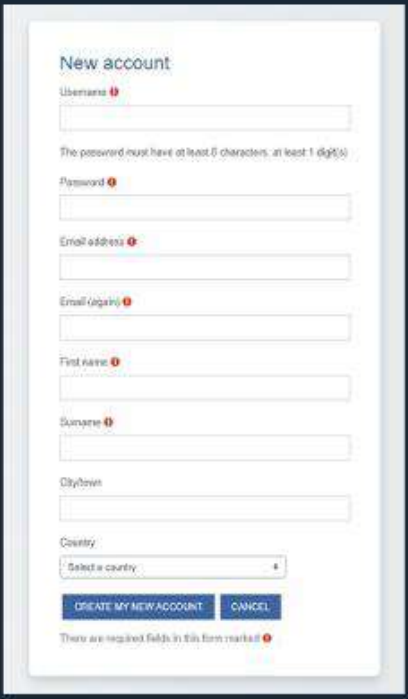
Slovenščina (sl)

Ελληνικά (el)

Български (bg)

W ACCOUNT

COOKIES NOTICE



New account

Username ❗

The password must have at least 8 characters, at least 1 digit(s)

Password ❗

Email address ❗

Email (again) ❗

First name ❗

Surname ❗

City/town

Country

Select a country

CREATE MY NEW ACCOUNT

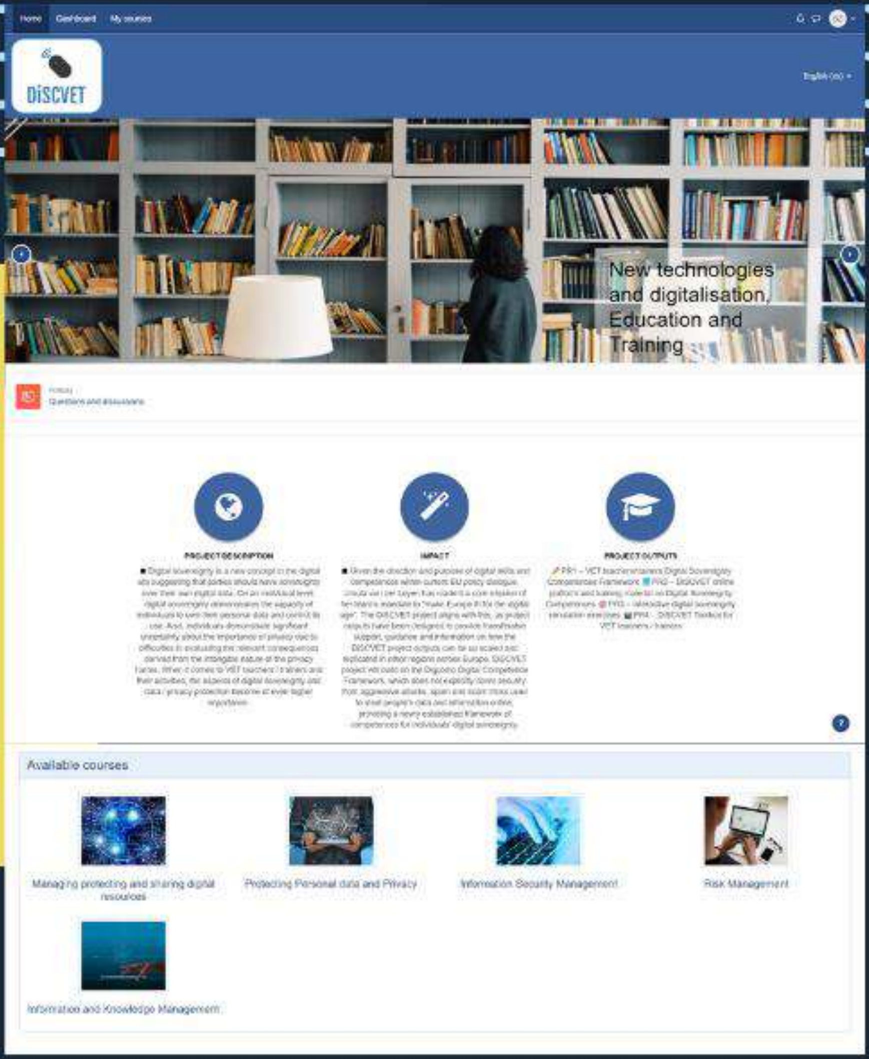
CANCEL

There are required fields in this form marked ❗

To access the materials, users need to sign up on the platform. After providing all the necessary information for creating an account, you will receive a confirmation e-mail (check your spam folder!), which will include a link to activate your account.

On the home page, you can find information about the project and 5 available courses. To access the learning material, click on a course and press the enrol button.

No qualification needed!



Home
Dashboard
My courses
DiSCVET
English (en)
New technologies and digitalisation, Education and Training
Forum
Questions and discussions

PROJECT DESCRIPTION

■ Digital sovereignty is a new concept in the digital era suggesting that parties should have sovereignty over their own digital data. On an individual level, digital sovereignty demonstrates the capacity of individuals to own their personal data and control its use. And, individuals demonstrate significant uncertainty about the importance of privacy due to difficulties in evaluating the relevant consequences derived from the intangible nature of the privacy harms. When it comes to VET teachers / trainers and their activities, the aspects of digital sovereignty and data / privacy protection become of even higher importance.

IMPACT

■ Given the direction and purpose of digital skills and competences within current EU policy dialogue, Ursula von der Leyen has made it a core mission of her team's mandate to "make Europe fit for the digital age". The DISCVET project aligns with this, as project outputs have been designed to provide transferable support, guidance and information on how the DISCVET project outputs can be up scaled and replicated in other regions across Europe. DISCVET project will build on the DigComp Digital Competence Framework, which does not explicitly cover security from aggressive attacks, spam and scam tricks used to steal people's data and information online, providing a newly established framework of competences for individuals' digital sovereignty.

PROJECT OUTPUTS

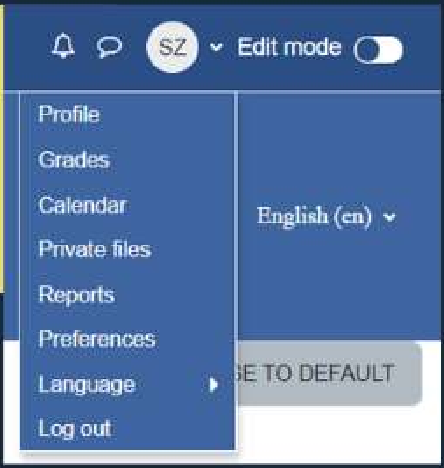
PR1 – VET teachers/trainers Digital Sovereignty Competences Framework PR2 – DISCVET online platform and training material on Digital Sovereignty Competences PR3 – interactive digital sovereignty simulation exercises PR4 – DISCVET Toolkit for VET learners / trainers

Available courses

- Managing protecting and sharing digital resources
- Protecting Personal data and Privacy
- Information Security Management
- Risk Management
- Information and Knowledge Management

Each module consists of several units, all having a theoretical learning part (PDF and digital nuggets), followed up by the simulation exercises. This is where you will test your acquired knowledge by receiving immediate feedback regarding your score.

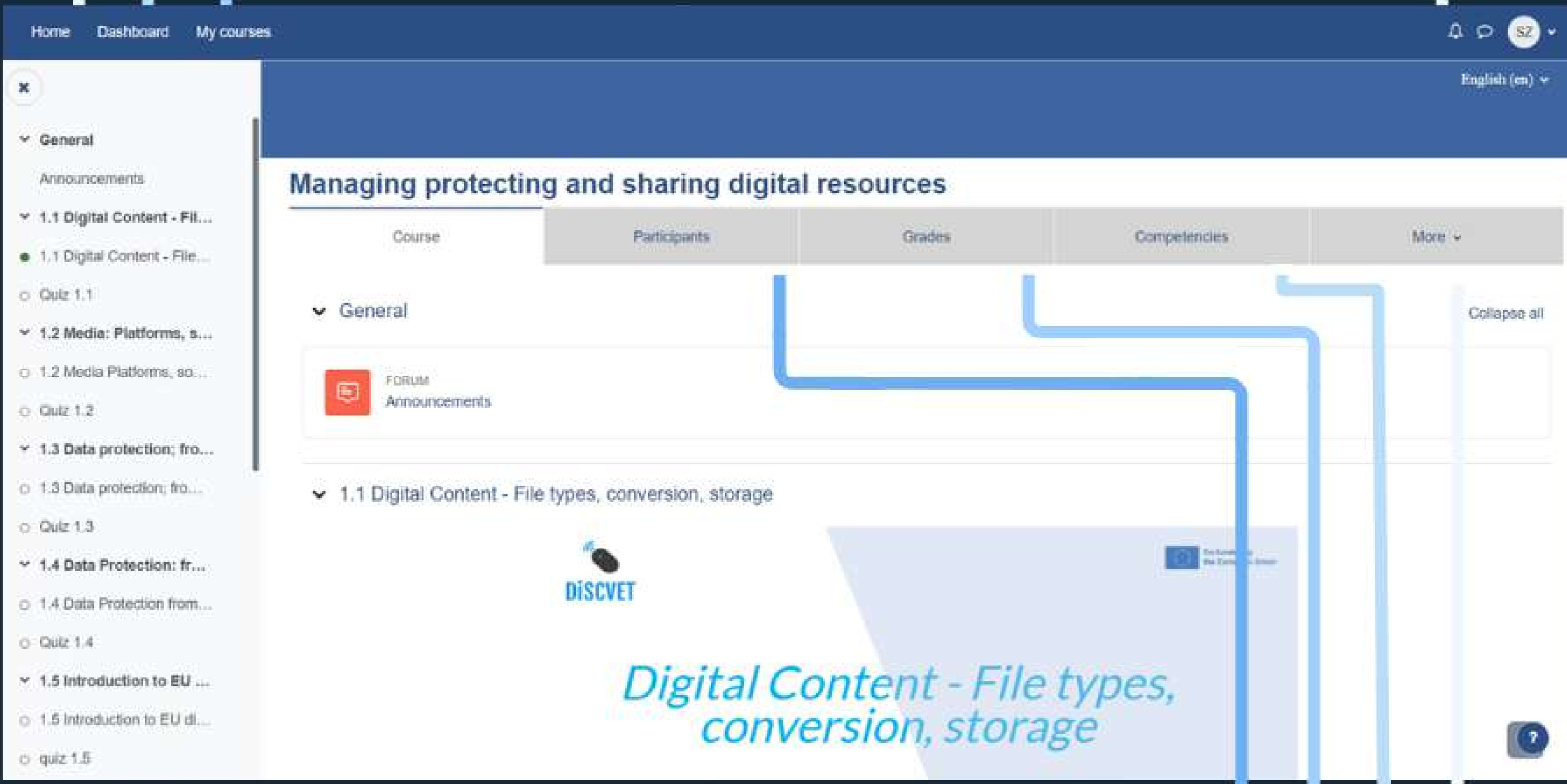
To access your profile and settings, click on the top right on the light circle with your initials. Next to it, you can find notifications (bell symbol) and chats (chat bubble symbol).



Return to the home page

Access calendar and scheduled activities

Courses you're enrolled in and your progress [%]

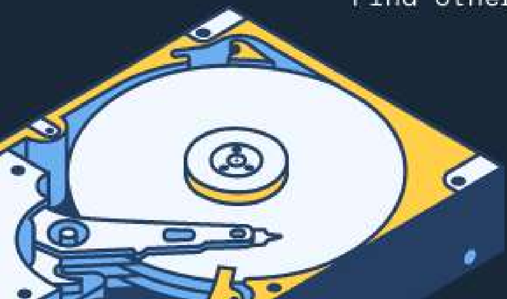

Home
Dashboard
My courses
SZ
English (en)
General
Announcements
1.1 Digital Content - Fil...
1.1 Digital Content - File...
Quiz 1.1
1.2 Media: Platforms, s...
1.2 Media Platforms, so...
Quiz 1.2
1.3 Data protection; fro...
1.3 Data protection; fro...
Quiz 1.3
1.4 Data Protection: fr...
1.4 Data Protection from...
Quiz 1.4
1.5 Introduction to EU ...
1.5 Introduction to EU di...
quiz 1.5
Managing protecting and sharing digital resources
Course
Participants
Grades
Competencies
More
General
Collapse all
FORUM
Announcements
1.1 Digital Content - File types, conversion, storage
DiSCVET
Digital Content - File types, conversion, storage

Find other people participating in this course

Your simulation exercises scores

A list of your new competencies

Unenrol from the course



4 Evidence and data from the piloting activities

4.1 Methodology

The aim of this report is to present the answers collected in the phase of the pilot test of the project results. The pilot test activity for DiscVet project was carried on during the timeframe February-April 2023.

The overall goal of this summative report is to record the perceived level of satisfaction and quality of the project results as well as their usefulness, to be able to focus on incurred issues and locate possible solutions in order to deliver the project results in their final and definitive version.

The project results tested were:

- **IO2: DiSCVET online platform and training material on Digital Sovereignty Competences**
- **IO3: Development of the interactive digital sovereignty simulation exercises**

The pilot test of IO2 have been implemented through a structured questionnaire in the form of a **Google Form** (to guarantee better accessibility and reachability of the parget group) Available in ANNEX I of this report. The questionnaire aimed to acquire useful feedback from the participants in the piloting activities, focusing on evaluating several features of the material, such as:

- the clarity of its structure;
- the effectiveness of the digital resources that it includes;
- The easiness to use and navigate through the platform;
- The amount of time spending in the platform and in its activities / components;
- The easiness to enter new data / information;
- The overall structure and aesthetics of the platform;
- The connection / loading of the components and/or their pages.

The pilot test of IO3 has been conducted through relevant structured questionnaire, focusing on evaluating several features of the simulation exercises, such as:

- Relevance with the topic and the target group's needs;
- Ease of use;
- Design.

Participants were asked to rate the different aspects of IO2 and IO3 on a 1 to 5 scale, where
1 = the lowest, unsatisfactory impression
3 = an adequate impression
5 = the highest, very good impression

The structured questionnaire has been embedded the link to the online platform https://discvet-hub.eu/login/index.php containing the material, in order to be able to monitor the achievement of the **KPIs** foreseen for this project activity.

KPI IO2

KPI 7: Well-defined training course and materials that meet the needs recognized within IO1 activities (qualitative) - Measurement tool: internal evaluation by project partners and external evaluation from the NSAGs members

KPI 8: At least 180 VET teachers/trainers that will participate in the piloting activities (quantitative) – Measurement tool: number of people that have registered in the platform and completed the training course

KPI 9: 85% satisfaction of the participants from the piloting activities (quantitative) - Measurement tool: filled in structured questionnaires for the evaluation of the piloting activities

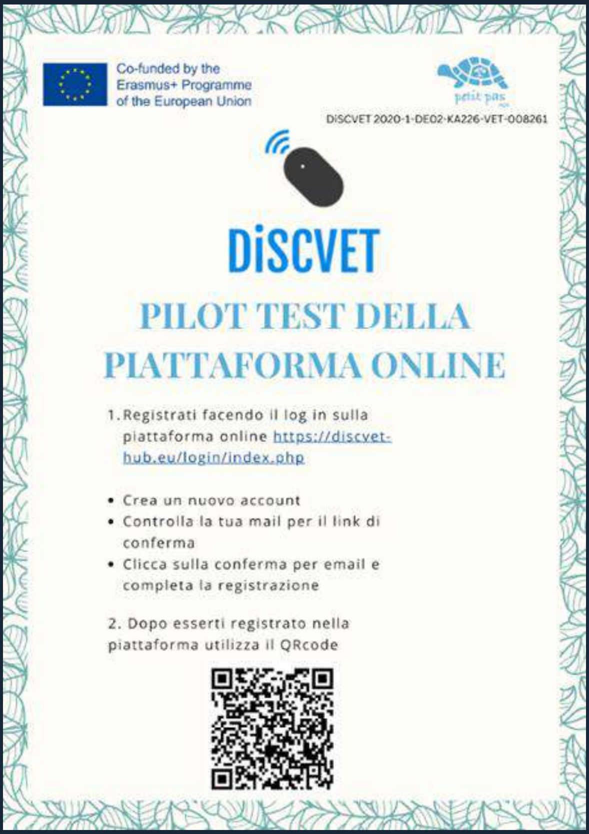
KPI IO3

KPI 10: At least 180 VET teachers/trainers that will participate in the piloting activities (quantitative) – Measurement tool: number of people that have registered in the platform and completed the simulation exercises

KPI 11: 85% satisfaction from the platform’s functionality (quantitative) - Measurement tool: filled in structured questionnaires for the evaluation of the platform

Each partner country conducted several piloting sessions (online or face-to-face), due to the difficulty to recruit 30 participants at the same time.

In **Italy** dissemination material was created to advertise the event and give instructions on how to conduct the pilot test. It was organized one session in person with the involvement of students, teachers and stakeholders to test the project results.



Co-funded by the
Erasmus+ Programme
of the European Union

petit pas

DiSCVET 2020-1-DE02-KA226-VET-008261

DiSCVET

PILOT TEST DELLA
PIATTAFORMA ONLINE

1. Registrati facendo il log in sulla piattaforma online https://discvet-hub.eu/login/index.php

- Crea un nuovo account
- Controlla la tua mail per il link di conferma
- Clicca sulla conferma per email e completa la registrazione

2. Dopo esserti registrato nella piattaforma utilizza il QRcode

In **Bulgaria** were held three piloting sessions overall – 1 in person and 2 online, with the participation of participants of VET teachers, trainers in Adult Education, and stakeholders.

In **Slovenia** the target group involved in pilot testing consisted of VET teachers, teachers, from local VET institutions and high schools, as well as a network of other Slovenian NGOs interested in similar topics, the Local Chamber of Commerce and Industry. The pilot testing sessions were held in separate moments, according to the availability of the participants, 3 sessions were organized face to face and 2 sessions online.

4.2 Results

Access to the E-learning platform per Country

Country	Number of Log-ins
Greece	40
Slovenia	32
Italy	36
Germany	11

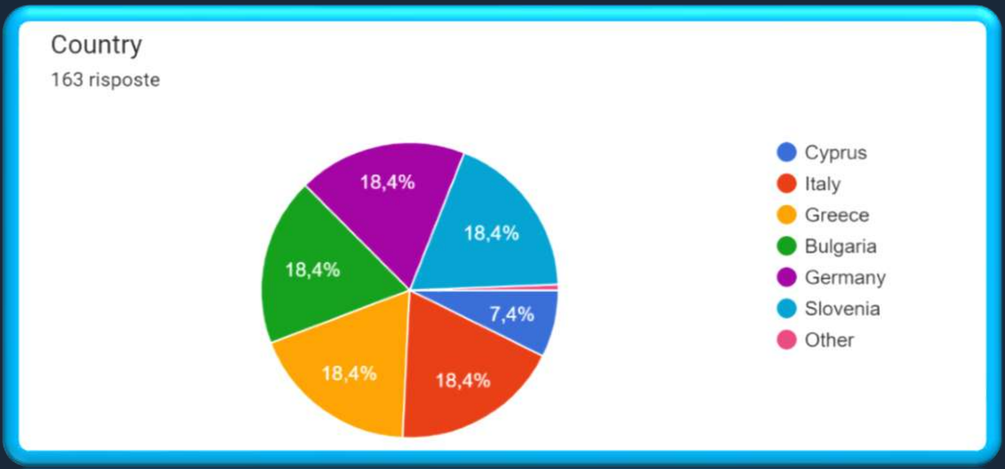
Cyprus	23
Bulgaria	35

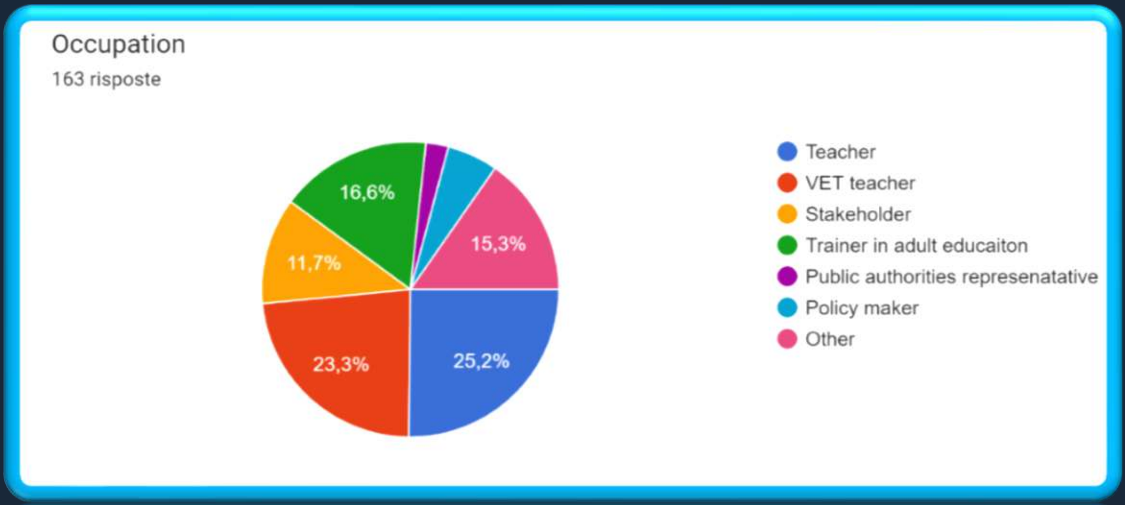
Feedback of the participants.

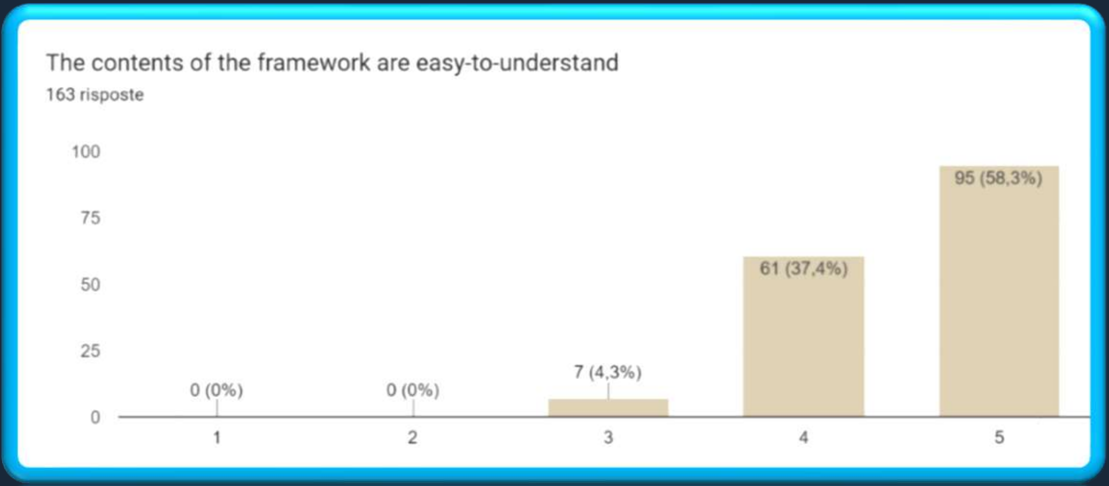
Target group occupation

In total were collected 163 answers from all partners countries, the highest percentage representing the target group occupation is 25.2% of teachers followed by the 23,3% of VET teachers.

Participants to the pilot test registered from all the partners' countries. A small percentage (1 respondent) registered from Fran

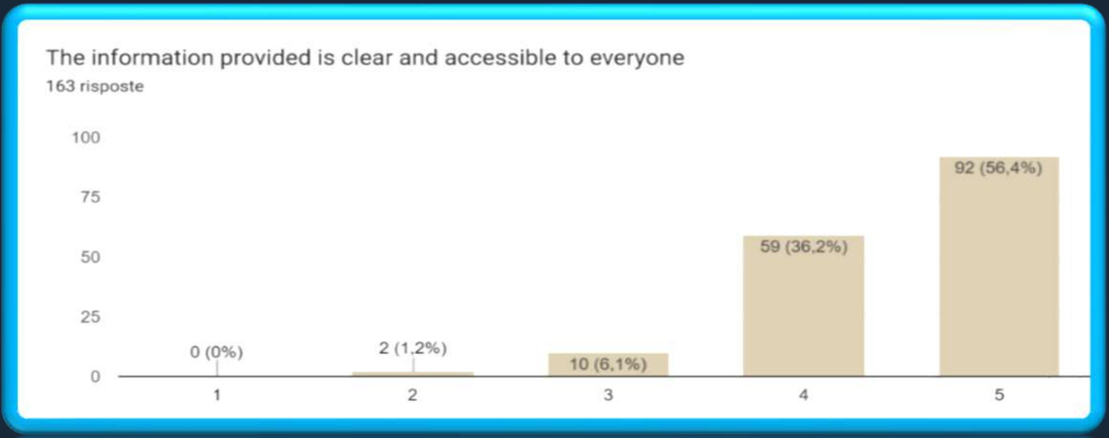






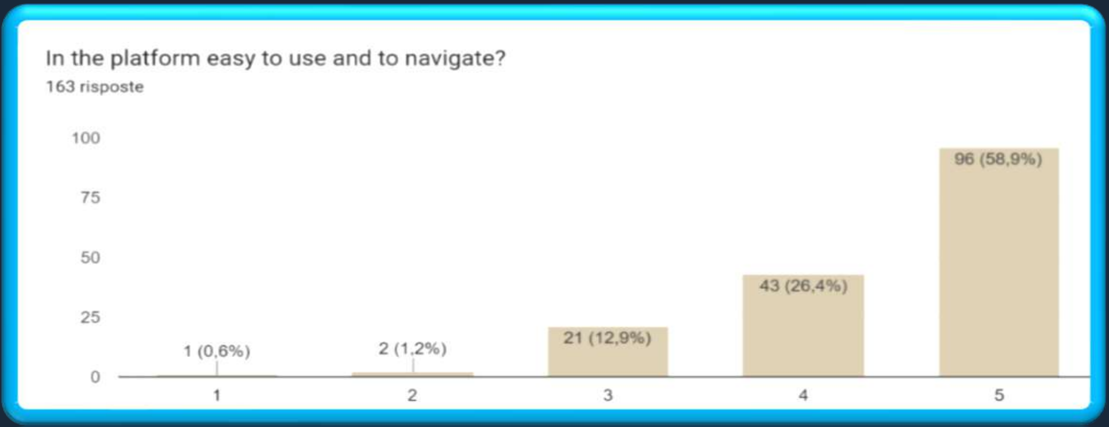
The contents of the framework are easy-to-understand

163 risposte



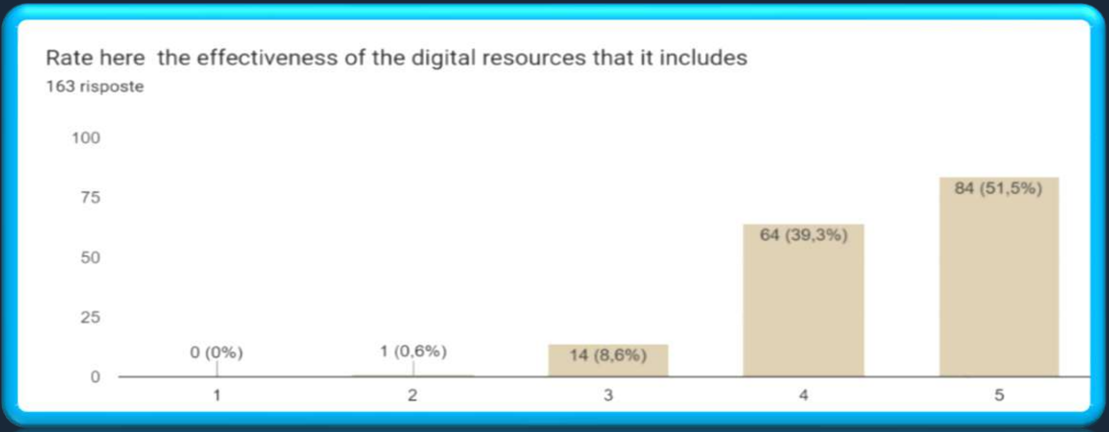
The information provided is clear and accessible to everyone

163 risposte



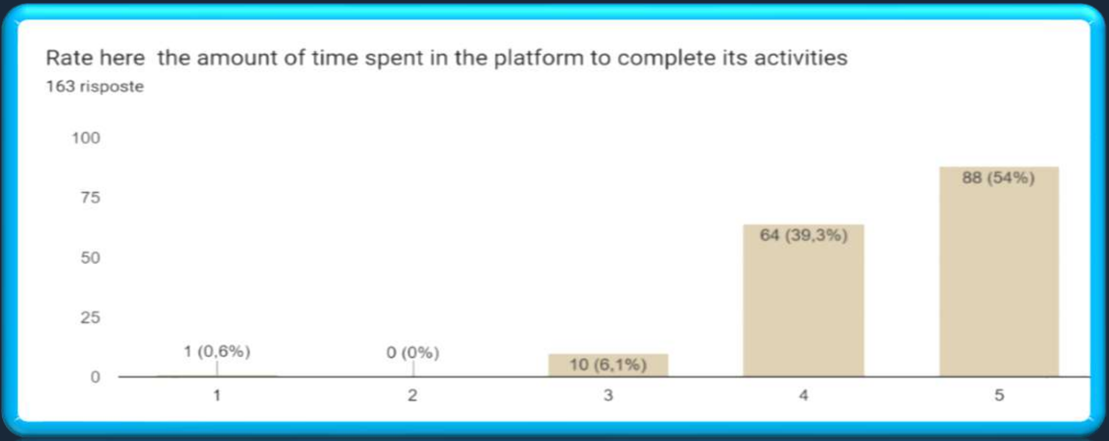
In the platform easy to use and to navigate?

163 risposte



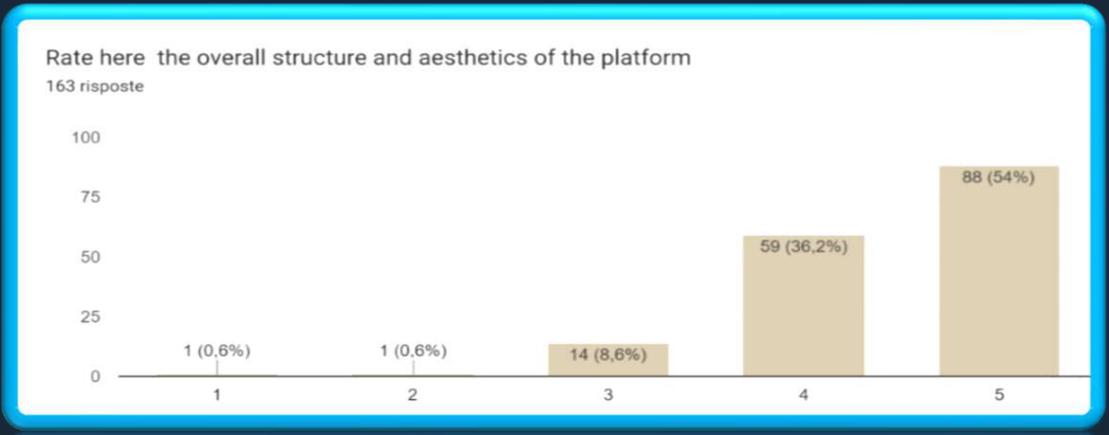
Rate here the effectiveness of the digital resources that it includes

163 risposte



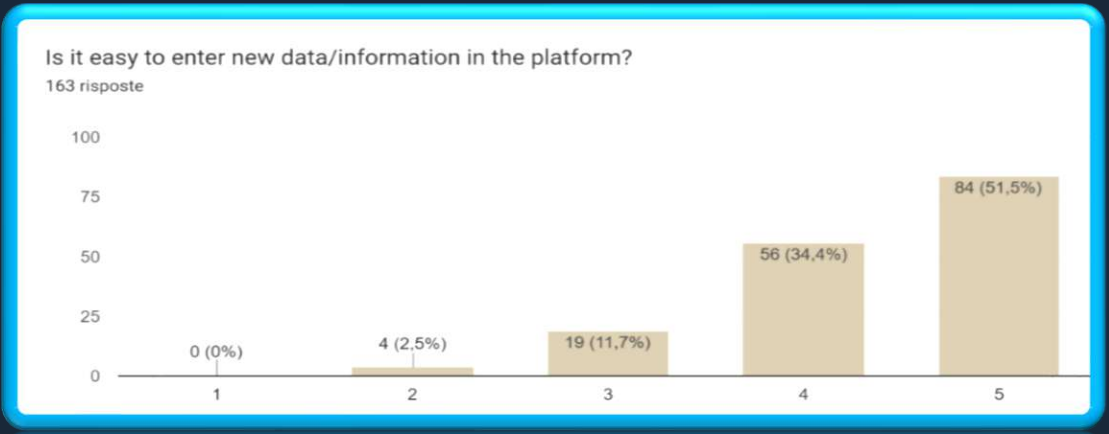
Rate here the amount of time spent in the platform to complete its activities

163 risposte



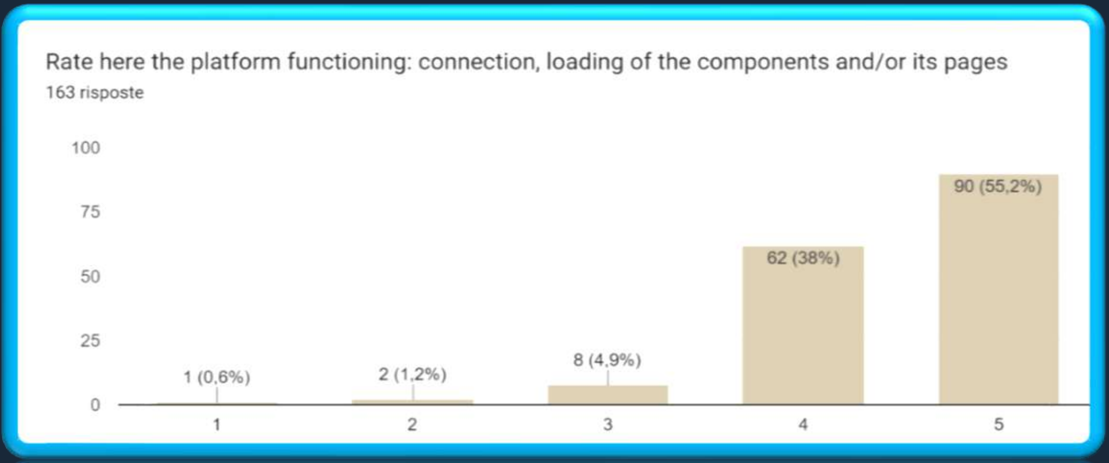
Rate here the overall structure and aesthetics of the platform

163 risposte



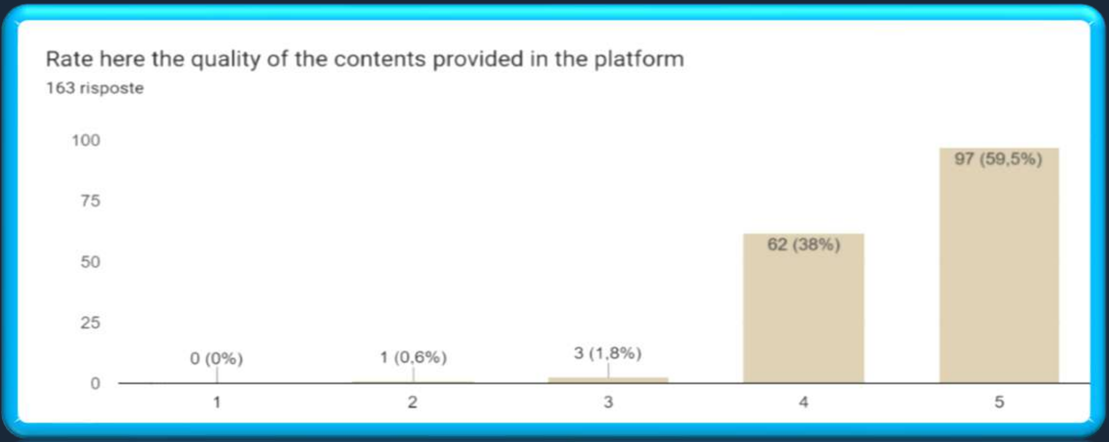
Is it easy to enter new data/information in the platform?

163 risposte



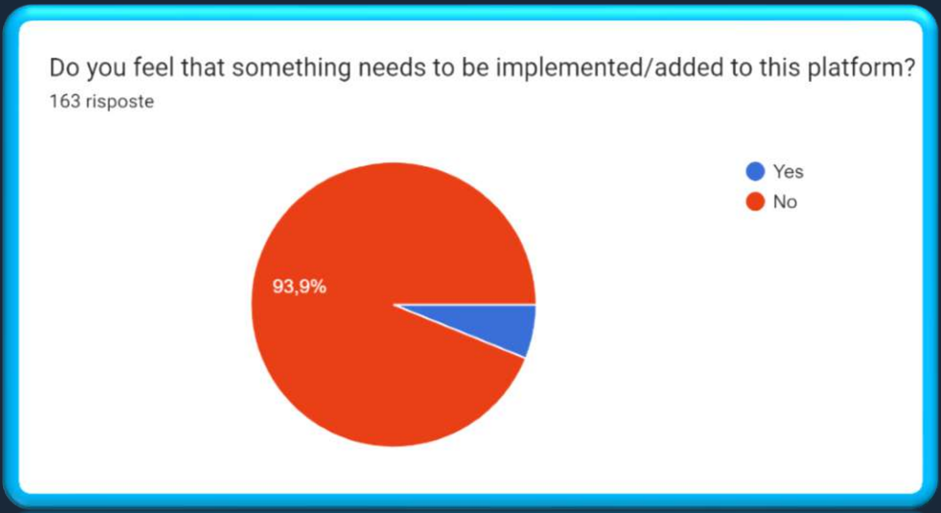
Rate here the platform functioning: connection, loading of the components and/or its pages

163 risposte



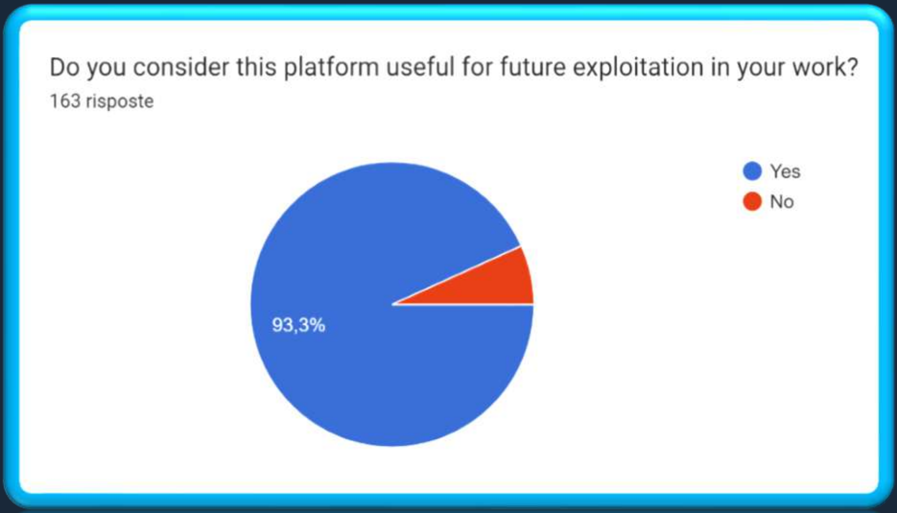
Rate here the quality of the contents provided in the platform

163 risposte



Do you feel that something needs to be implemented/added to this platform?

163 risposte



Do you consider this platform useful for future exploitation in your work?

163 risposte

As can be seen from the figures above, representing the answers collected after the pilot testing sessions in each partner country, participants to the pilot test expressed a **high level** of satisfaction rating the different aspects of the e-learning platform such as its content, ease to use and navigate, the quality of the materials uploaded, the platform functioning, assigning scores **between 4 and 5** (where 5 is the maximum score).

Also, participants declared the usefulness of the platform for future exploitation of their work. The majority of participants to the pilot test didn't express the need to implement further the platform, 10 participants (6.1%) although, suggested some specific corrections to take into consideration as per feedback reported below:

- There are Slovene translations missing
- missing Bulgarian questions in the quizzes
- when a language is selected only the information in that language should appear
- More informative videos

Although the questionnaire used for the pilot test showed a high level of overall satisfaction, there were some aspects to highlight and take into consideration for the final improvement of the platform and its content, as visible in specific feedback summarized as follows.

Positive feedback

- *an interesting platform*
- *Good design and very useful*
- *i believe this platform is easy to understand and to use, it also as a great aesthetic*
- *The platform is very simple to use and can be easily used.*
- *very good*
- *I think this is useful and friendly*
- *Very useful and clear the content division in the platform*
- *Excellent*
- *I like that real life cases are implemented*
- *Simulation of real life is useful*
- *I was missing this knowledge*
- *Easy to understand and practical*
- *The interactive navigation and information gleaned from the website was excellent*
- *I really enjoy browsing the website and learned a lot of new things about data and privacy*
- *I will definitely use what I learned about data visualization in the future and use the platform's teaching tips*
- *Very interesting and full of information that all teachers should know*
- *Interesting! I learned a lot about interactivity and digital data management*
- *The digital world is all around us and it is important to know how to manage our data and information! The platform is very interesting and easy to read*

Aspects that need improvement

- *Some grammar mistakes can be found*
- *Mobile optimization is needed.*
- *the back button glitched, the "slovene page" was mostly in english, odd formating, aesthetically unpleasing*

- *The content seems useful; however, the way it is presented is inconvenient and confusing at times. In some chapters, the quiz & genial.ly presentation are included, in others not at all. Content in genial.ly and pdf is repetitive and unclear.*
- *It not coherent between moduls*
- *Quiz had weird formatting (double numbers).*
- *Some quizzes had missing answers, other had questions with several 100% correct answers to choose from, making the quiz a guessing game (e.g. 5.4)*
- *The presentations took a bit long to load but otherwise useful content.*
- *Geniallys took quite some time to load. The content seems useful; however, the way it is presented is inconvenient and confusing at times. In some chapters, the quiz & genial.ly presentation are included, in others not at all. Content in genial.ly and pdf is repetitive and unclear.*

4.3 Conclusion

The pilot test phase proved to be overall positive, having highlighted the satisfaction of most of the participants who positively evaluated the project results and their usefulness.

At the same time, aspects that require improvement were highlighted and mostly concerned some aspects related to the quizzes. In this regard, the suggestions provided revolve around the possibility of “*first fixing the more obvious issues such as grammar, double numbers on the quizzes, missing answers etc., all mentioned before. Then move on to upgrading the site design-wise (make the top banner smaller, move the modules to be the towards the top, make better use of spacing and layout (on all pages)). Lastly, look into the loading times for Geniallys*”

4.4 ANNEXES

Annex I - I Pilot test questionnaire

https://docs.google.com/forms/d/e/1FAIpQLSdLMxrfoPSlRcKhAgGl_Ph0LJceFrdhE5wSCiV0lWbhORUElA/viewform

Annex II - II IO1 Validation

https://drive.google.com/drive/folders/1rIvFJQheUiG38Ii7rAG5GxIAyN_e-y0o

Co-funded by the Erasmus+ Programme of the European Union

5 EU APPROACH TO DIGITAL SECURITY

5.1 General EU approach to cybersecurity

The EU has taken a comprehensive approach to cybersecurity, with a number of regulations and directives aimed at protecting digital infrastructure and personal data. Some key elements of the EU's cybersecurity strategy include:

The **General Data Protection Regulation (GDPR),** which sets rules for how personal data must be processed, stored, and protected within the EU. The GDPR applies to all businesses operating within the EU, as well as any company processing the personal data of EU citizens.

The **Network and Information Security Directive (NIS Directive),** which establishes cybersecurity measures for critical infrastructure providers, including energy, transport, and healthcare sectors. It requires these providers to report major security incidents to national authorities.

The **Cybersecurity Act**, which creates a framework for the establishment of EU-wide cybersecurity certification schemes for digital products, services, and processes.

The **EU Cybersecurity Strategy**, which is a comprehensive plan for improving cybersecurity across the EU. It includes initiatives to enhance cooperation among member states, promote research and innovation, and strengthen the EU's cybersecurity infrastructure.

5.2 Digital Education Action Plan

In Europe, there is a growing recognition of the importance of digital education in preparing individuals for the future. The European Commission has launched a new Digital Education Action Plan, which aims to promote the use of technology in education and improve digital skills among European citizens. The plan includes initiatives such as providing all schools with high-speed internet access, increasing the use of digital tools in teaching and learning, and supporting the development of innovative educational technologies. The plan also focuses on improving the digital skills of teachers and promoting lifelong learning opportunities for all citizens. By investing in digital education, the European Union hopes to promote economic growth, social inclusion, and digital citizenship across the region.

The Plan has 13 actions, 3 of which are directly related to digital education and training:

Action 5 (Digital transformation plans for education and training institutions) – aims to support digital transformation efforts through Erasmus+ cooperation projects, creates Teacher Academies for development and collaboration, and introduces an online self-assessment tool called SELFIE for Teachers to identify areas for improvement.

Action 6 (Ethical guidelines on the use of AI and data in teaching and learning for educators) - there is a growing need to understand AI's potential and to raise awareness of the possible risks as it could transform education and training, as well as our everyday lives. The guidelines provide practical support and guidance for the use of AI, help with teaching and learning, suggest better support systems for administrative processes, and present ethical considerations.

Action 7 (Common guidelines for teachers and educators) - education and training are vital in cultivating citizens' critical thinking skills needed to navigate the online world, given its unique characteristics like algorithms, "information bubbles," and "echo chambers." Therefore, supporting teachers and educators with guidance and practical examples is essential for promoting digital literacy and combating disinformation. The guidelines offer practical tips and activity plans for primary and secondary teachers, regardless of their digital education knowledge, and are complemented by a final report outlining the Expert Group's key findings and recommendations.

Overall, the Digital Education Action Plan is a comprehensive strategy to promote digital education and improve digital skills across Europe. It recognizes the importance of technology in preparing students for the future and promoting economic growth and social inclusion.

5.3 Frameworks containing digital security skills

The exponential growth of digital technologies has emphasized the need for digital security. The importance of developing and improving digital security skills is mentioned in digital technologies competencies frameworks such as the European Digital Competence, known as DigComp 2.2, and the European Digital Competence for Educators, known as DigCompEdu.

The **DigComp framework** allows European citizens to understand better what is meant by digitally competent and how to assess and develop their own digital competence. The five main domains in the competencies framework are information and data literacy, communication and collaboration, digital content creation, safety and problem-solving.

The **DigCompEdu framework** describes what it means for educators to be digitally competent and is directed to all educators at all levels of education. The framework depicts 22 competencies that are organized into six areas. These areas are professional engagement, digital resources, teaching and learning, assessment, empowering learners and facilitating learners' digital competence.

5.4 Funding research and innovation for digital learning

The EU funds research and innovation in cybersecurity and digital tech through programs such as Horizon Europe, Digital Europe Programme, and CEF (Connecting Europe Facility). The latter supports cybersecurity infrastructure and incident response teams. InvestEU funds important chains in cybersecurity in the private sector. Horizon Europe, one of the most important funding programmes for cybersecurity, funds innovative cyber defense solutions, aiming to support SMEs, simulations, and protect critical data. These programs work with the European Cybersecurity Industrial, Technology and Research Competence Center, a cluster of experts and organizations for cybersecurity deployment across countries.

5.5 Useful resources and tools (BBB)

The Fourth Industrial Revolution brought rapid developments in the fields of new technologies, communication and automation. These developments have led the transition to a digital context in employment and education. The pandemic accelerated this transition by creating a greater need for distance learning and work. This has created new dynamics and challenges with digital tools' universal and widespread use (platforms, websites, etc.).

In this context, the EU recognised the momentum and adopted the Digital Education Action Plan (2021-2027), which set out the European Commission's objectives for achieving effective, inclusive and accessible digital education across the European Union. In particular, the EU has created a range of digital tools to facilitate EU operations, training issues and communication between organisations and individuals across the EU. The main digital tools the EU has launched are:

School Education Gateway. It is an "online catalog", where you can consult educational materials, participate in online courses and access training resources for teachers and, more generally, for people interested in school education in Europe. The School Education Gateway includes publications, tutorials, teaching materials created by EU institutions, EU-funded projects, free online courses, webinars and the latest news related to European school policy and education.

eTwinning. The platform is aimed at school staff in European countries, to allow teachers and principals to communicate with each other, to create a network that allows the development of collaborations, sharing and useful projects for the European school system. eTwinning aims to promote school collaboration in Europe through the use of information and communication technologies: through the platform, in fact, school staff can communicate, exchange resources and create projects in 30 languages.

Learning Corner. This is a platform aimed at both students and teachers. Depending on the age group, students are provided with different materials, including games, contests and activity books, which allow them to learn about different aspects of the European Union, from laws to the environment and history. For teachers, the platform is a good source to find educational materials dedicated to primary or secondary school students.

Support, Advanced Learning and Training Opportunities for youth (Skip-Youth). It is a network of seven centers each working on a priority area within the youth field. Specifically, the platform provides youth learning resources, training courses, and networking opportunities.

Electronic Platform for Adult Learning in Europe (EPALE). It is a European online community, multilingual and open, to which adult education professionals from all over Europe can join. The platform provides the opportunity to implement digital skills through free online courses, access to examples of good practice in adult learning and e-learning resources.

Self-reflection on Effective Learning by Fostering the use of Innovative Educational Technologies (SELFIE) is a free tool designed to help schools embed digital technologies into teaching, learning and assessment. SELFIE has a strong basis in research and was developed based on the European Commission framework on promoting digital-age learning in educational organisations.

6 NATIONAL CONTEXT

6.1 Slovenia

Slovenia has been actively working to improve its digital and cybersecurity infrastructure in recent years. The country has recognized the importance of cybersecurity as an essential component of national security and has developed various initiatives to enhance its cybersecurity capabilities. Slovenia's national cyber security capabilities and their roles are defined at the operational level: SI-CERT is the national asset of cyber security assurance, and the MORS is responsible in the field of defense and protection against natural and other disasters (including the protection of critical infrastructure), the police ensure cyber security in the context of public safety and the fight against cybercrime, Slovenian Intelligence and Security Agency (SOVA) conducts counterintelligence, and the emergent SIGOVCERT is responsible for cyber security in public administration. In the field of engagement, other stakeholders are also included, such as the operators of critical infrastructure in the private and public sectors.

INITIATIVE 1	
Name	Safe on the Internet
Location	National
Duration	2011 –
Description	SI-CERT has been raising national awareness and running an educational programme "Safe on the Internet". This

	initiative is targeted at the general public with specific content for small businesses, craftsmen, and sole proprietors to raise awareness on the safe use of the Internet. The project is financed by the Ministry of Education, Science and Sport, and is also participating in the campaigns of the European month of cyber security.
Results/Impact	So far, the initiative has cooperated with several organizations and institutions, such as: European Union Agency for Network and Information Security, European Consumer Centre, Agency for Communication Networks and Services of the Republic of Slovenia, Information Commissioner of the RS, Intellectual Property Office, Association of Banks of Slovenia, Consumer Association of Slovenia.
Source link	https://www.varninainternetu.si/

INITIATIVE 2	
Name	Safer Internet Centre Slovenia
Location	National
Duration	2005 -
Description	Safer Internet Centre (SIC) Slovenia is the national project promoting and ensuring a better internet for kids. The project is co-financed by the European Health and Digital Executive Agency (HaDEA); in Slovenia financial support also comes from the Government Information Security Office. The project is run by a consortium of partners coordinated by the Faculty of Social Sciences at the University of Ljubljana, the Academic and Research Network of Slovenia (ARNES), the Slovenian Association of Friends of Youth (ZPMS), and the Youth Information and Counselling Center of Slovenia (MISSS). Since 2005, SAFE.SI has been working as a national awareness-raising point for children and teenagers on the safe use of the internet and mobile devices. Their activities are aimed at four target groups: children,

	adolescents, parents, and professionals (teachers, social workers, youth workers, etc.). The mission of the awareness campaign is to inform young Internet and mobile users how they can protect themselves from risks and use the web and other new technologies safely and responsibly.
Results/Impact	SAFE.si is encouraging cooperation with Slovenian stakeholders, and institutions from the public and private spheres, to make children and adolescents safer online and to protect them from potential dangers and risks. They cooperated with Agency for Communication Networks and Services of the Republic of Slovenia, the Association for Paediatrics, the Ministry of Education, Science and Sport (preparation of an action plan for the digitization of education), etc.
Source link	https://safe.si/

EVALUATION AND IMPLEMENTATION SUGGESTIONS

Besides the initiatives mentioned, Slovenia has been contributing to national cyber security systems through higher-education programs (e. g. Faculty of Computer and Information Science) and courses on cyber security at all levels of education, and the results of research organizations. Professional associations have initiated improvements and assistance in raising awareness among various target groups (e. g. Chamber of Commerce and Industry of Slovenia, ISACA, SI-CERT). While Slovenia has made efforts to educate its citizens about digital security, there is still room for improvement.

To improve the level of knowledge among citizens, Slovenia could implement offline initiatives, such as a promotion at primary and secondary schools. Digital security could become an obligatory part of the school curriculum to ensure that children are taught about online security risks from an early age. Initiatives should be expanded to wider target groups, such as adults and businesses. A cybersecurity strategy has been developed in Slovenia but without an action plan to implement it.

6.2 Greece

In Greece, digital and cybersecurity have become increasingly important in recent years as the country has become more reliant on technology and the internet. The

Greek government has taken steps to strengthen cybersecurity measures and protect critical infrastructure, such as the country's energy and transportation systems. In 2019, the Greek Ministry of Digital Policy launched a new National Cybersecurity Strategy, which includes a range of initiatives to improve cybersecurity across the public and private sectors. The strategy focuses on four key areas: protection, detection, response, and recovery. It includes measures such as improving the security of critical infrastructure, developing cybersecurity awareness campaigns, and enhancing the country's ability to respond to cyber threats. The Greek government has also established a National Cybersecurity Authority, which is responsible for coordinating cybersecurity efforts across the public and private sectors. The authority works to identify and mitigate cybersecurity risks, develop cybersecurity policies and regulations, and provide guidance and support to organizations and individuals.

INITIATIVE 1	
Name	National Cybersecurity Strategy
Location	National, public sector
Duration	2019 -
Description	The National Cybersecurity Strategy of Greece was launched in 2019 by the Ministry of Digital Policy, Telecommunications and Information. The strategy aims to improve cybersecurity across the public and private sectors and to protect critical infrastructure from cyber threats. The strategy is based on four main pillars: protection, detection, response, and recovery. These pillars are supported by a range of initiatives, including: Strengthening critical infrastructure security Developing cybersecurity awareness Enhancing the country's ability to respond to cyber threats Promoting international cooperation The National Cybersecurity Strategy also includes specific targets and timelines for the implementation of its initiatives. Overall, the strategy represents a comprehensive approach to improving cybersecurity in

	Greece and protecting against cyber threats.
Results/Impact	Improved cybersecurity awareness Strengthened critical infrastructure security: Enhanced incident response capabilities Increased international cooperation Overall, the National Cybersecurity Strategy has had a positive impact on cybersecurity in Greece. While there is still work to be done to address ongoing threats and challenges, the strategy has helped to raise awareness of cybersecurity risks, improve critical infrastructure security, enhance incident response capabilities, and promote international cooperation.
Source link	https://www.trade.gov/market-intelligence/greece-cyber-security-strategy

INITIATIVE 2	
Name	National Cybersecurity Authority
Location	National, public sector
Duration	2019 -
Description	The National Cybersecurity Authority (NCA) is a Greek government agency responsible for coordinating and implementing cybersecurity policies and initiatives across the public and private sectors. The NCA was established in 2019 as part of Greece's National Cybersecurity Strategy. The NCA's main responsibilities include: Developing and implementing cybersecurity policies and regulations: The NCA is responsible for developing policies and regulations to improve cybersecurity across different sectors in Greece. Coordinating cybersecurity efforts: The NCA works to coordinate cybersecurity efforts across different government agencies, as well as with private sector

	organizations and international partners. Identifying and mitigating cybersecurity risks: The NCA is responsible for identifying and mitigating cybersecurity risks, including those related to critical infrastructure. Providing guidance and support: The NCA provides guidance and support to organizations and individuals on cybersecurity best practices and incident response.
Results/Impact	As the National Cybersecurity Authority (NCA) in Greece was established in 2019, it is still relatively early to fully assess the results and impact of its activities. However, there have been several notable developments since its establishment that suggest that the NCA is making a positive impact on cybersecurity in Greece. The NCA has played a role in raising awareness of cybersecurity risks and best practices in Greece, through public awareness campaigns, training programs, and other initiatives. This has helped to improve the overall level of cybersecurity in the country. Overall, the NCA has made important strides in improving cybersecurity in Greece since its establishment in 2019. While there is still work to be done to address ongoing cybersecurity challenges, the NCA has made a positive impact and is playing a critical role in protecting Greece against cyber threats.
Source link	https://www.concordia-h2020.eu/consortium/national-cyber-authority-ncsa/

EVALUATION AND IMPLEMENTATION SUGGESTIONS

Even though Greece has made progress in raising awareness about digital security among its citizens, there is still room for improvement. Here are some possible solutions to improve the level of knowledge and awareness of digital security in Greece, with a focus on how other countries/institutions can implement similar initiatives:

EDUCATION INITIATIVES: One possible solution is to increase the emphasis on digital security in educational institutions, such as schools and universities. Governments and institutions can develop and implement educational programs that teach basic cybersecurity skills and practices to young people. These programs can also target

Co-funded by the Erasmus+ Programme of the European Union

adults who may not have had the opportunity to learn about digital security earlier in life.

PUBLIC AWARENESS CAMPAIGNS: Governments can run public awareness campaigns to raise awareness about the importance of digital security and to provide guidance on how to protect oneself online. These campaigns can take different forms, such as posters, advertisements, and social media posts.

CYBERSECURITY CERTIFICATIONS: Another solution is to establish cybersecurity certifications that individuals can obtain after completing a training course. These certifications can provide individuals with a recognized qualification that demonstrates their knowledge and skills in cybersecurity.

COLLABORATION WITH PRIVATE SECTOR: Governments can collaborate with private sector organizations to provide training and support to citizens on digital security. For example, telecom companies can provide guidance on safe internet usage to their customers.

INTERNATIONAL COOPERATION: Countries can collaborate on initiatives to improve digital security. This can include information sharing on cyber threats and best practices, joint training exercises, and coordinated responses to cyber incidents.

6.3 Italy

Italy has taken significant steps towards improving its overall digital/cybersecurity posture. The country has recognized the importance of cybersecurity and is taking various initiatives to enhance its cybersecurity capabilities. In 2021, the National Cybersecurity Agency (ACN) was established. It aims to increase national cyber security and resilience for the country's digital development, achieve national and European strategic autonomy in the digital sector, promote specific training courses for the development of the workforce in the sector, support awareness campaigns, promote a widespread culture of cybersecurity, and develop international actions and projects for a secure global cyberspace. The government has also introduced the National Cybersecurity Strategy (NCS), which aims to strengthen the country's digital resilience and capabilities against cyber threats. It focuses on critical infrastructure protection, information sharing, research and development, and training and education.

INITIATIVE 1	
Name	Cloud Strategy Italy
Location	For the Italian Public Administration

Duration	15/12/2021 -
Description	The Cloud Strategy Italy, created by the Department for Digital Transformation and the National Cybersecurity Agency (ACN), contains the strategic guidelines for the migration path of data and digital services of the Public Administration to the cloud, through a 3-level data classification system. Strategic: data and services whose compromise could impact national security. Critical: data and services whose compromise could cause a detriment to the maintenance of functions relevant to society, health, safety and the economic and social well-being of the country. Ordinary: data and services whose compromise does not cause the interruption of State services or, in any case, prejudice to the economic and social well-being of the country. With the aim of guiding and promoting the safe, controlled and complete adoption of cloud technologies by the public sector, in line with the principles of privacy protection and with the recommendations of European and national institutions..
Results/Impact	Digital infrastructures will be more reliable and secure and the Public Administration will be able to respond to cyber attacks in an organized manner, guaranteeing continuity and quality in the use of data and services.
Source link	https://www.acn.gov.it/

INITIATIVE 2	
Name	Safer Internet Center – Connected Generations
Location	National
Duration	1/07/2016 –
Description	The Safer Internet Center (SIC) - Connected

	Generations project is co-financed by the European Commission under the Digital Europe programme, is coordinated by the Ministry of Education and Merit and is a member of a network promoted by the European Commission on the online platform "Better Internet for Kids" managed by European Schoolnet, in close collaboration with INSAFE (network that brings together all European SICs) and Inhope (network that brings together all European hotlines). The Educational Mission of SIC is to provide information, advice and support to children, teenagers, parents, teachers and educators to facilitate the reporting of illegal material online. The general objective is to develop services with innovative and higher quality content in order to guarantee young users online security while considering, at the same time, the connected investment as a 'virtuous' opportunity for the 'social' and economic growth of the entire community.
Results/Impact	Provide support and advice to raise awareness of online dangers.
Source link	https://www.generazioniconnesse.it/site/it/safer-internet-centre/

EVALUATION AND IMPLEMENTATION SUGGESTIONS

In Italy, there are several initiatives in terms of cybersecurity. A National Cybersecurity Strategy 2022-2026 was also developed aimed at planning, coordinating and implementing measures aimed at making the country more secure and resilient. This strategy envisages the achievement of 82 measures by 2026. A valid suggestion could be to include online safety subjects and cybersecurity lessons in school educational plans, not leaving them only to the discretion of additional courses, extracurricular activities or the curriculum of schools where they study subjects related to IT training.

6.4 Cyprus

According to OCECPR "The vision of the Cybersecurity Strategy of Cyprus is the operation of information and communications technologies in Cyprus with the necessary levels of security to the benefit of every user". The strategy's main objective is to develop and maintain a safe and secure electronic environment in Cyprus for all businesses and citizens by developing policies within the frame of cooperation between all competent authorities. Towards this direction, Cyprus has approved a number of actions that have been promoted at the national level, such as the creation of a framework for the security and integrity of information infrastructures and the raising of awareness of all stakeholders and Cypriot society about relevant security matters and the formation of Computer Emergency Response Teams (CCERTs/CSIRTs). Moreover, Cyprus is committed to contributing to European and international collaboration in responding to threats in cyberspace.

INITIATIVE 1	
Name	National Cybersecurity Coordination Centre (NCCC-CY) for the Republic of Cyprus
Location	National
Duration	21 December 2021 -
Description	The Digital Security Authority (DSA) has been designated as the NCCC-CY by a decision of the Council of Ministers of Cyprus in December 2021. Its main responsibilities is to provide knowledge and to facilitate access to know-how on cybersecurity industrial, technological and research issues. In addition, is the promotion and the facilitation of participation of start-ups, SMEs and academic and research communities at national level in cross-border projects and in cybersecurity actions funded by relevant Union programmes. Furthermore, the Centre provides technical assistance to stakeholders by supporting them in the application phase for projects managed by the Competence Centre and seeks to establish collaborations with relevant activities at national, regional and local level, such as national policies on research, development and innovation in the area of cybersecurity, and in particular those policies stated in the National Cybersecurity Strategy.
Results/Impact	Since 4th of May 2022 the DSA in collaboration with the Research and Innovation Foundation - CY are able to draw and channel available funds for cyber security

	following the approval of its proposal by the European Commission. For DSA to be able to function towards this direction, it had to be evaluated in depth by the European Commission in terms of its ability to manage the funds in question. The European Commission carried out the evaluation after the submission of the proposal on 17 February 2022 and approved it on May 4th.
Source link	https://dsa.cy/en/activities/nccc

EVALUATION AND IMPLEMENTATION SUGGESTIONS

In addition to CCERT, there are various initiatives aimed at increasing cybersecurity awareness and promoting best practices. These include the annual Cyprus Cybersecurity Challenge, which seeks to identify and develop the country's top cybersecurity talent, and the establishment of the Cyprus Cybersecurity Association, which aims to promote cybersecurity research, education, and innovation. DSA works to increase cybersecurity awareness and develop cyber competencies in various business fields. It organizes trainings, workshops, and webinars, and offers information sessions for students interested in studying cybersecurity, SMEs and senior citizens. The Ministry of Education and Culture has also implemented cybersecurity education programs in schools. These programs aim to provide students with the necessary knowledge and skills to protect themselves online and raise awareness about cyber threats.

However, there is still room for improvement in the area of digital/cybersecurity in Cyprus. Specifically, more resources could be dedicated to cybersecurity education and training programs, particularly for SMEs, which may be more vulnerable to cyber-attacks. Additionally, greater collaboration between government, academia, and the private sector could help strengthen the country's overall cybersecurity posture.

6.5 Bulgaria

Bulgaria has made progress in improving cybersecurity with a National Cybersecurity Strategy, Personal Data Protection Act, and NIS Directive. The State Agency for Electronic Governance coordinates policies and provides training. CERT Bulgaria detects and responds to threats, while the Cybersecurity Competence Center aims to promote expertise. Challenges include a shortage of skilled professionals, low public awareness, and recent cyber attacks.

Co-funded by the Erasmus+ Programme of the European Union

INITIATIVE 1	
Name	State e-Government Agency (SEGA)
Location	National, public sector
Duration	2016 –
Description	State e-Government Agency (SEGA) is responsible for the country's electronic governance and cybersecurity policies. The agency coordinates with other government bodies and provides cybersecurity training to public sector employees.
Results/Impact	SAEG has been working on enhancing the country's cybersecurity capabilities by promoting secure electronic communication, implementing information security measures, and conducting regular audits of the government's information systems.
Source link	https://www2.e-gov.bg/en/about_us

INITIATIVE 2	
Name	National Cybersecurity Educational Program
Location	National, high schools (7th to 12th grade)
Duration	2016 –
Description	This program is aimed at students from 7th to 12th grade and focuses on raising awareness about cybersecurity risks, promoting safe and responsible behaviour online, and encouraging students to consider careers in cybersecurity. It has 3 main components: lectures, exercises, and competitions. The initiative aims to foster a culture of cybersecurity awareness and education in Bulgaria, and to help build a skilled workforce in the field of cybersecurity.
Results/Impact	The programme helped increase the level of interest in cybersecurity education and careers among young people

	in Bulgaria, whilst encouraging national organizations to form partnerships to strengthen the country's cybersecurity capabilities. It also has led to the emergence of a new generation of cybersecurity professionals who are equipped with the necessary knowledge and skills to protect Bulgaria's digital infrastructure.
Source link	https://ccdcoe.org/uploads/2018/10/Bulgaria_National-program-Digital-Bulgaria-2025_2019_original.pdf

EVALUATION AND IMPLEMENTATION SUGGESTIONS

While Bulgaria is taking the necessary steps to advance in cybersecurity, there is always room for improvement. For example, the National Cybersecurity Educational Program could be expanded to reach a wider audience, including adults and businesses. That being said, it's a good idea to target young audiences, as they are the ones shaping the future. This is something other countries could also implement. In addition to educational initiatives, there is a need for more comprehensive cybersecurity policies and regulations in Bulgaria to protect against cyber threats. This includes stronger data protection laws and regulations, as well as improved cybersecurity standards for critical infrastructure.

6.6 Germany

Issues related to digital/cybersecurity education are a priority for Germany in order to be able to meet the challenges posed by new developments in cyber governance and digital transition. More specifically, the German Government, in partnership with stakeholders in the sector, has proceeded to develop a Digital Strategy.

The "Digital Strategy 2025" outlines the priorities of the German government, namely to develop digital competences and promote the use of new tools to enhance Germany's digitisation processes. The strategy is based on 10 pillars important for digitisation, including a pillar focusing on the introduction of digital education at all stages of an individual's life.

Germany's Digital Strategy 2025 was adopted in 2016 for 10 years. The actions of the Strategy aim not only to enable the German economy to meet the new challenges but also to secure its leading position in both quality and technology for the coming years by combining traditional competitive advantages with newer technology, modern methods and special support programmes.

INITIATIVE 1	
Name	Cyber Security Strategy for Germany
Location	National
Date	2021
Description	On 8 September 2021, the Federal Cabinet adopted the 2021 Cyber Security Strategy for Germany prepared by the Federal Minister of the Interior and Community. It provides the framework for cyber security over the next five years. Cybersecurity is a task for the present and one of the important tasks for the future. It is an era defined by the new opportunities of the digital world, such as artificial intelligence, connected electronic devices and new, innovative means of communication. In order to be able to take advantage of these opportunities, it is essential to minimise the risks. The German Cybersecurity Strategy 2021 replaces the German Cybersecurity Strategy 2016. The strategy sets out the essential long-term direction of the federal government's cybersecurity policy, broken down into guiding principles, action areas and strategic goals. The Cyber Security Strategy focuses on four areas of action: society, private industry, government and EU/international affairs. A total of 44 strategic objectives have been set within these action areas.

Results/Impact	The Federal Office of Information Security will become a hub for federal and state agencies to work together in preventing cybercrime, creating a third pillar in the comprehensive federal cybersecurity architecture: It will take its place alongside the Federal Criminal Police Office (BKA), which already plays this role in the German police sector, and the Federal Office for the Protection of the Constitution, which does so in the domestic German intelligence community. The strategy strengthens digital sovereignty and thus the secure digital transformation of our country. Germany's digital economy will be strengthened through targeted support for key enabling technologies and networking with relevant researchers. A security-by-design approach will be applied from the outset to emerging and key enabling technologies.

INITIATIVE 2	
Name	Cyber Security Research Centers
Location	National
Date	2011

Description	Research funding has the goal of financing the development of new ideas and technologies. Funding is provided for projects in a wide spectrum of research areas. The range covers everything from basic research in natural sciences, environmentally friendly sustainable development, new technologies, information and communication technologies, the life sciences, work design, structural research funding at institutions of higher education to innovation support and technology transfer. The Federal Ministry of Education and Research (BMBF) is funding three Kompetenzzentren für IT-Sicherheitsforschung (Cyber Security Research Centers). Individual outstanding universities or non-university research institutions are funded as research centers for cyber security. The centers focus thematically and organizationally on the most important challenges in the field of IT security.
Results/Impact	The task of these centres is to develop long-term strategies for cyber security and to carry out related research projects to meet current and future challenges.

EVALUATION AND IMPLEMENTATION SUGGESTIONS

Germany has made significant efforts to educate its citizens about digital security, but there is room for improvement. While initiatives such as public awareness campaigns, school programs and government-funded resources have been implemented, the ever-evolving nature of digital threats requires continued efforts.

To improve the level of citizens' knowledge about digital security, Germany can consider the following solutions:

- Integrated training programmes for the public and private sector
- Public and private sector initiatives
- Information exchange platforms
- Awareness-raising campaigns
- To implement similar initiatives, other countries/institutions can:
- Adapt existing programmes: Study successful initiatives from Germany and other countries to adapt and implement them in their own education systems.

Co-funded by the Erasmus+ Programme of the European Union

- Work with experts in the field: Collaborate with local industry experts and cybersecurity professionals to develop relevant and practical educational content.
- Promote public-private partnerships: Encourage partnerships between government agencies, private companies, and non-profit organizations.
- Adapt communication channels: Utilize a mix of communication channels to reach a wide audience.
- Use a variety of communication channels to leverage a mix of channels: Regularly evaluate the effectiveness of digital security education initiatives.

Co-funded by the
Erasmus+ Programme
of the European Union

7 Conclusion

The DiscVET project primary objective was equipping VET teachers and trainers with the necessary competencies in digital sovereignty to effectively train others and foster a secure digital environment. With a focus on creating innovative training materials and interactive simulation exercises, the project aims to enhance participants digital security readiness. However, our vision extends beyond this immediate goal. We aim to contribute to the education of the more aware ang highly skilled generation of Europeans by empowering VET teachers and trainers with the knowledge and competencies needed for digital sovereignty.

Recognizing the importance of digital skills, secure digital environments, and lifelong learning opportunities, the EU has adopted a comprehensive approach to cybersecurity, digital education, and research and innovation funding. This commitment is evident in the EU`s strategies, regulations, and initiatives aimed at equipping individuals with the necessary digital skills and promoting secure digital practices across Europe.

To ensure the effectiveness and quality of the project DiscVET, we value the feedback and evaluation provided by participants. By carefully analysing and addressing any identified issues, we strive to deliver the final and definitive version of the project results. The evaluation report will serve as a valuable resource, guiding us in improving the project`s outcomes and ensuring the high satisfaction and usefulness of the project among the target group.

8 Bibliography

- UpGuard: Cybersecurity of Critical Digital Infrastructure
  - Obtained from: https://www.upguard.com/blog/cybersecurity-regulations-in-the-european-union#toc-3
- European commission: Digital learning and ICT in education
  - Obtained from: https://digital-strategy.ec.europa.eu/en/policies/digital-learning
- European commission: Digital Education Action Plan – Action 5
  - Obtained from:: https://education.ec.europa.eu/focus-topics/digital-education/action-plan/action-5
- European commission: Digital Education Action Plan – Action 6
  - Obtained from:: https://education.ec.europa.eu/focus-topics/digital-education/action-plan/action-6
- European commission: Digital Education Action Plan – Action 7
  - Obtained from:: https://education.ec.europa.eu/focus-topics/digital-education/action-plan/action-7
- European commission: DigComp Framework
  - Obtained from:: https://joint-research-centre.ec.europa.eu/digcomp/digcomp-framework_en#ref-4-safety
- Christine Redecker: European Framework for Digital Competence of Educators: DigCompEdu
  - Obtained from:: https://publications.jrc.ec.europa.eu/repository/handle/JRC107466
- UpGuard: Funding and Research Regulations (Support for Research and Innovation)
  - Obtained from: https://www.upguard.com/blog/cybersecurity-regulations-in-the-european-union#toc-4
- Francesca Bernasconi: Digital education according to the EU: useful tools
  - Obtained from:: https://www.elearningnews.it/en/news-C-27/digital-education-according-to-the-eu-useful-tools-AR-1488/