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

DiSCVET

ZBIRKA ORODIJ za učitelje poklicnega izobraževanja in usposabljanja

DiSCVET

Razvoj kompetenc za digitalno suverenost učiteljev in vodij usposabljanj

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

Ustvaril MIITR

Maj 2023

Ta projekt je financirala Evropska komisija. Ta publikacija odraža le stališča avtorja, Komisija pa ni odgovorna za kakršno koli uporabo informacij, ki jih ta publikacija vsebuje.
[Številka projekta: 2020-3-BE05-KA205-003110].

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

1 Vsebina

DiSCVET
ZBIRKA ORODIJ

PROJEKT: Razvoj kompetenc za digitalno suverenost učiteljev in vodij usposabljanja v poklicnem izobraževanju in usposabljanju

ZAKAJ?

Digitalna suverenost je nov koncept v digitalni dobi, ki predlaga, da bi morale imeti stranke suverenost nad svojimi digitalnimi podatki. Na ravni posameznika digitalna suverenost dokazuje sposobnost posameznikov, da si lastijo svoje podatke in nadzorujejo njihovo uporabo. Ljudje pogosto težko cenijo pomen zasebnosti, saj je posledice kršitev zasebnosti zaradi njihove izmuzljive narave težko oceniti.

Na voljo v BG, DE, EN, GR, IT, SI!

KAKO

Nova inovativna oblika vsebine usposabljanja skupaj s spletno simulacijsko platformo

ZA KOGA

Učitelji poklicnega izobraževanja in usposabljanja, organizacije poklicnega izobraževanja, ponudniki izobraževanja, organi, strokovnjaki/odločevalci

KJE

discvet-hub.eu

discvet.eu
facebook.com/discvet

Vključuje gradivo o:

- Upravljanje digitalnih virov
- Osebni podatki in zasebnost
- Upravljanje informacijske varnosti
- Upravljanje tveganj
- Upravljanje informacij in znanja

IO2 **Spletna platforma** in gradivo za usposabljanje

Ustvarjalno gradivo za usposabljanje, katerega namen je opremiti učitelje poklicnega izobraževanja in usposabljanja s potrebnimi kompetencami za povečanje njihove digitalne suverenosti in jim omogočiti usposabljanje drugih. Gradivo za usposabljanje obsega sveženj digitalnih učnih virov z uporabo koncepta mikroučenja. Ti digitalni učni drobci vsebujejo različne vire, kot so interaktivne igre, videoposnetki e-učenja, interaktivne študije primerov, infografski viri in drugo.

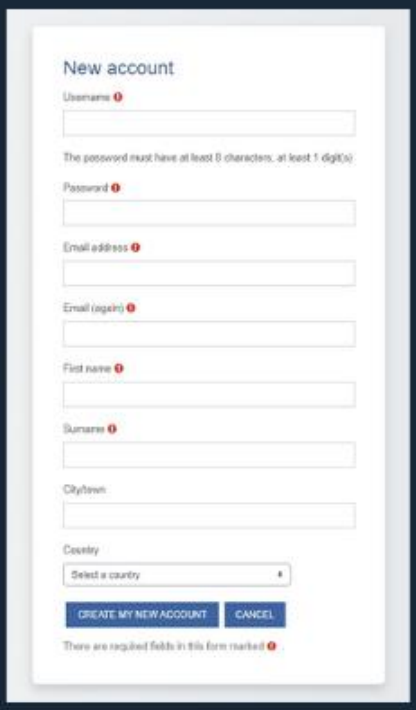
IO3 **Simulacijske vaje**

Prehod v praktično okolje je omogočen s simulacijskimi vajami, ki posnemajo uporabo v resničnem življenju, uvajajo nove aplikacije, metode in orodja ter uporabnikom omogočajo pridobivanje praktičnih izkušenj. Vaje izboljšujejo ohranjanje znanja, saj bodo uporabniki lahko načela digitalne suverenosti in digitalne varnosti uporabili v praktičnih situacijah, kot so kibernetski napadi, kršitve varnosti, ribarjenje, zlonamerna programska oprema in drugo.

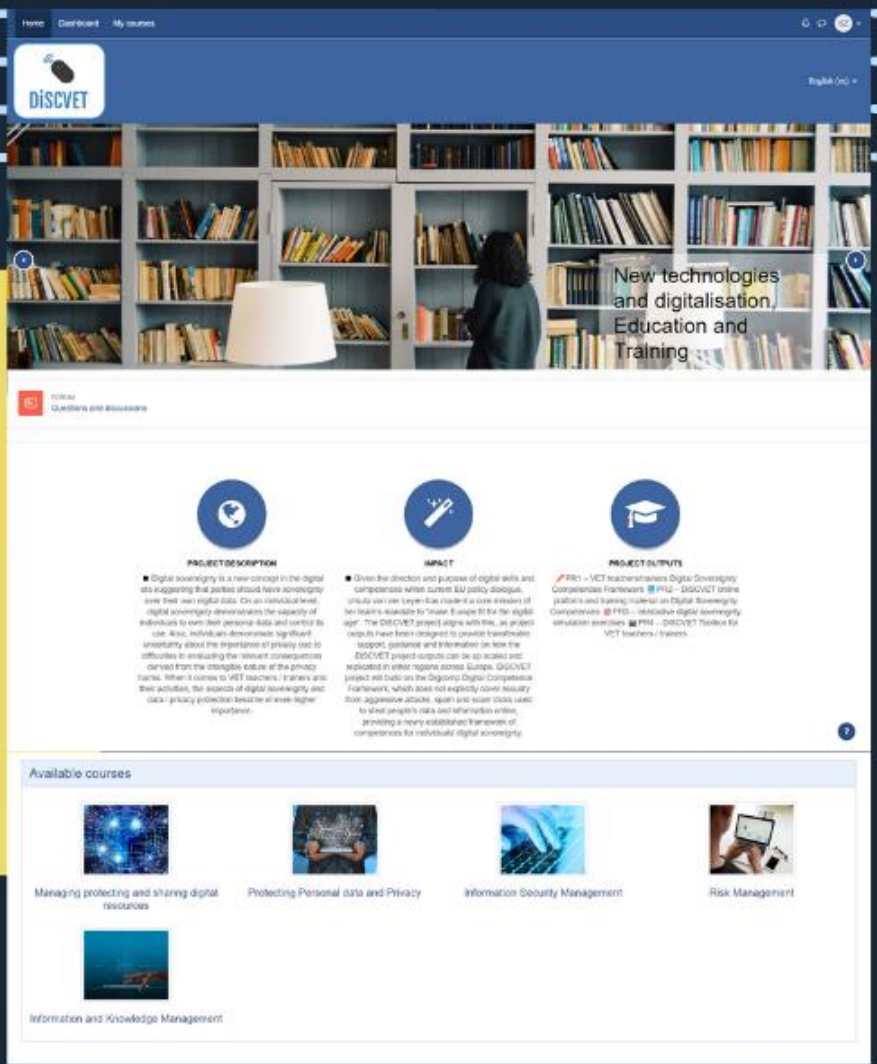
Preberite več o rezultatih, njihovi uporabi, pilotnem testiranju in nacionalnih pobudah na področju izobraževanja o digitalni varnosti! ⟶

Kako uporabljati platformo?

(discvet-hub.eu/)



Za dostop do gradiva se morajo uporabniki registrirati na platformi. Po posredovanju vseh potrebnih podatkov za ustvarjanje računa boste prejeli potrditveno e-poštno sporočilo (preverite mapo za neželeno pošto!), ki bo vsebovalo povezavo za aktivacijo računa.

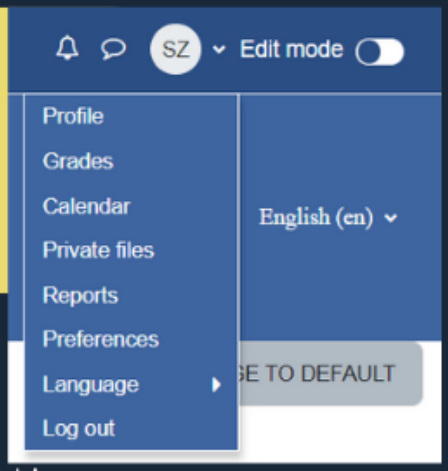


Na domači strani najdete informacije o projektu in 5 razpoložljivih tečajev. Če želite dostopati do učnega gradiva, kliknite na tečaj in pritisnite gumb za vpis.

Kvalifikacije niso potrebne!

Vsak modul je sestavljen iz več enot, ki imajo teoretični učni del (PDF in digitalni drobci), ki mu sledijo simulacijske vaje. Tu boste preizkusili svoje pridobljeno znanje in prejeli takojšnje povratne informacije o doseženem rezultatu.

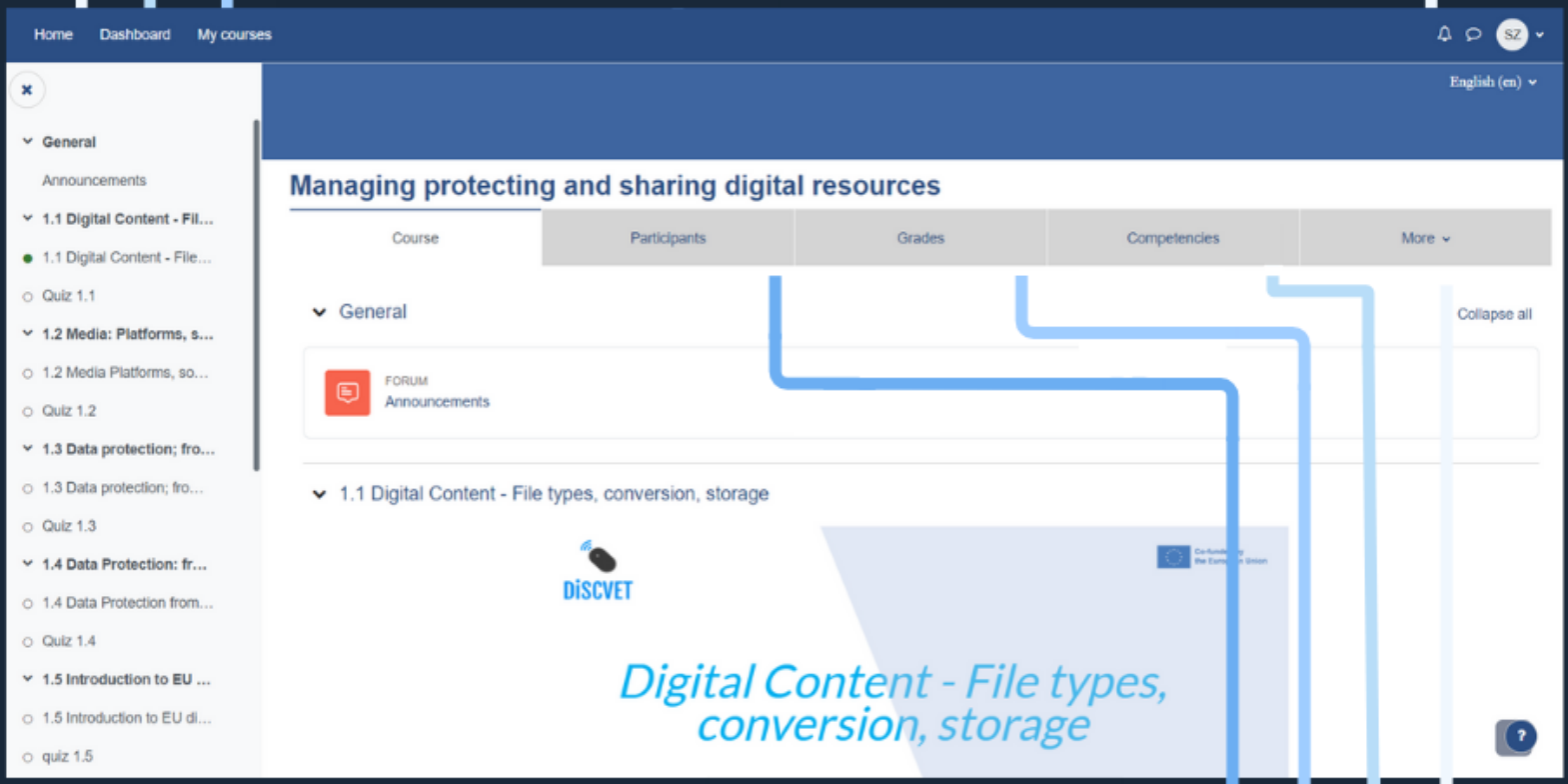
Če želite dostopati do svojega profila in nastavitev, kliknite desno zgoraj na svetel krog z vašimi začetnicami. Poleg njega so obvestila (simbol zvonca) in klepet (simbol mehurčka za klepet).



Vrnitev na domačo stran

Dostop do koledarja in načrtovanih dejavnosti

Vpisani predmeti in vaš napredek [%]



Poiščite druge udeležence tega tečaja

Rezultati vaših simulacijskih vaj

Seznam vaših novih kompetenc

Odjava iz tečaja

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

4 Dokazi in podatki iz pilotnih dejavnosti

4.1 Metodologija

Namen tega poročila je predstaviti odgovore, zbrane v fazi pilotnega preizkusa rezultatov projekta. Dejavnost pilotnega testiranja za projekt DiscVet je potekala v časovnem okviru od februarja do aprila 2023.

Splošni cilj tega zbirnega poročila je zabeležiti zaznano stopnjo zadovoljstva in kakovosti rezultatov projekta ter njihovo uporabnost, da bi se lahko osredotočili na nastala vprašanja in poiskali možne rešitve za zagotovitev rezultatov projekta v njihovi končni in dokončni različici.

Preverjeni rezultati testa so bili:

- **IO2: DiSCVET spletna platforma in gradivo za usposabljanje o kompetencah na področju digitalne suverenosti**
- **IO3: Razvoj interaktivnih vaj za simulacijo digitalne suverenosti**

Pilotni test IO2 je bil izveden s strukturiranim vprašalnikom v obliki Googlovega obrazca (za zagotovitev boljše dostopnosti in dosegljivosti ciljne skupine), ki je na voljo v PRILOGI I tega poročila. Namen vprašalnika je bil pridobiti koristne povratne informacije od udeležencev pilotnih dejavnosti s poudarkom na ocenjevanju več značilnosti gradiva, kot so:

- jasnost njegove strukture;
- učinkovitost digitalnih virov, ki jih vključuje;
- enostavnost uporabe in navigacije po platformi;
- količina časa, ki ga porabite za platformo in njene dejavnosti/komponente;
- enostavnost vnašanja novih podatkov/informacij;
- splošno strukturo in estetiko platforme;
- povezanost/naložitev sestavnih delov in/ali njihovih strani.

Pilotni preizkus IO3 je bil izveden s pomočjo ustreznega strukturiranega vprašalnika, ki se je osredotočil na ocenjevanje več značilnosti simulacijskih vaj, kot so:

- Ustreznost glede na temo in potrebe ciljne skupine;
- enostavnost uporabe;
- Oblikovanje

Udeleženci so morali različne vidike IO2 in IO3 oceniti na lestvici od 1 do 5, pri čemer so

1 = najnižji, nezadovoljiv vtis
3 = ustrezen vtis
5 = najvišji, zelo dober vtis

V strukturiran vprašalnik je bila vgrajena povezava do spletne platforme https://discvet-hub.eu/login/index.php, ki vsebuje gradivo, da bi bilo mogoče spremljati doseganje ključnih kazalnikov uspešnosti, predvidenih za to projektno dejavnost.

KPI IO2

KPI 7: Dobro opredeljeni tečaji in gradiva za usposabljanje, ki ustrezajo potrebam, prepoznanim v okviru dejavnosti IO1 (kvalitativno) - merilno orodje: notranja ocena projektnih partnerjev in zunanja ocena članov NSAG.

KPI 8: Najmanj 180 učiteljev/učiteljev poklicnega izobraževanja in usposabljanja, ki bodo sodelovali v pilotnih dejavnostih (kvantitativno) - merilno orodje: število oseb, ki so se prijavile na platformo in opravile tečaj usposabljanja

KPI 9: 85-odstotno zadovoljstvo udeležencev pilotnih dejavnosti (kvantitativno) - merilno orodje: izpolnjeni strukturirani vprašalniki za oceno pilotnih dejavnosti

KPI IO3

KPI 10: Najmanj 180 učiteljev/učiteljev poklicnega izobraževanja in usposabljanja, ki bodo sodelovali v pilotnih dejavnostih (kvantitativno) - merilno orodje: število oseb, ki so se prijavile na platformo in opravile simulacijske vaje

KPI 11: 85-odstotno zadovoljstvo s funkcionalnostjo platforme (kvantitativno) - merilno orodje: izpolnjeni strukturirani vprašalniki za oceno platforme

Vsaka partnerska država je izvedla več pilotnih srečanj (spletnih ali osebnih), saj je bilo težko hkrati zbrati 30 udeležencev.

V Italiji je bilo pripravljeno gradivo za širjenje, ki je oglaševalo dogodek in dajalo navodila za izvedbo pilotnega preizkusa. Organizirana je bila ena osebna seja z udeležbo učencev, učiteljev in zainteresiranih strani za preverjanje rezultatov projekta.

V Bolgariji so potekala tri pilotna srečanja - eno osebno in dve spletni, na katerih so sodelovali učitelji poklicnega izobraževanja in usposabljanja, izobraževalci v izobraževanju odraslih in zainteresirane strani.

V Sloveniji so ciljno skupino, vključeno v pilotno testiranje, sestavljali učitelji poklicnega izobraževanja in usposabljanja, učitelji, iz lokalnih institucij poklicnega izobraževanja in usposabljanja ter srednjih šol, pa tudi mreža drugih slovenskih nevladnih organizacij, ki jih zanimajo podobne teme, ter lokalna gospodarska zbornica. Seje pilotnega testiranja so potekale v ločenih trenutkih glede na razpoložljivost udeležencev, 3 seje so bile organizirane osebno, 2 seji pa prek spleta.

4.2 Rezultati

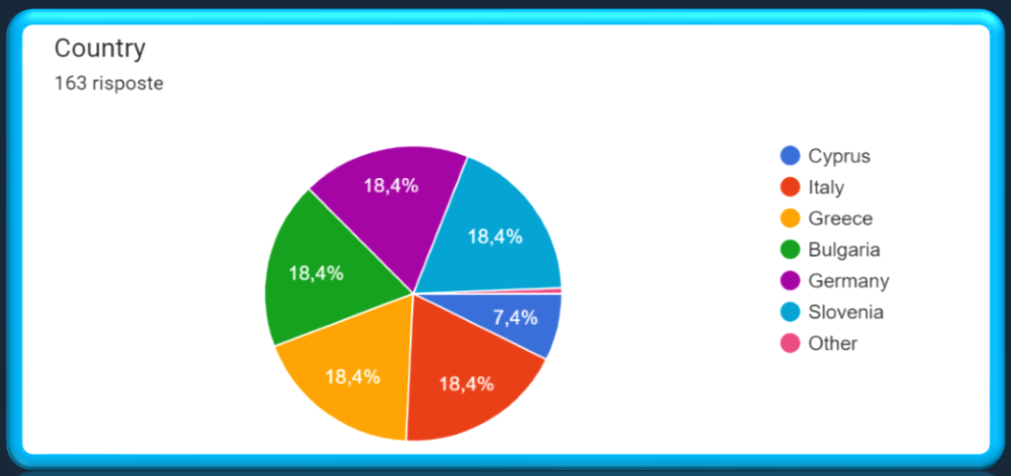
Dostopi do platforme za e-učenje na državo

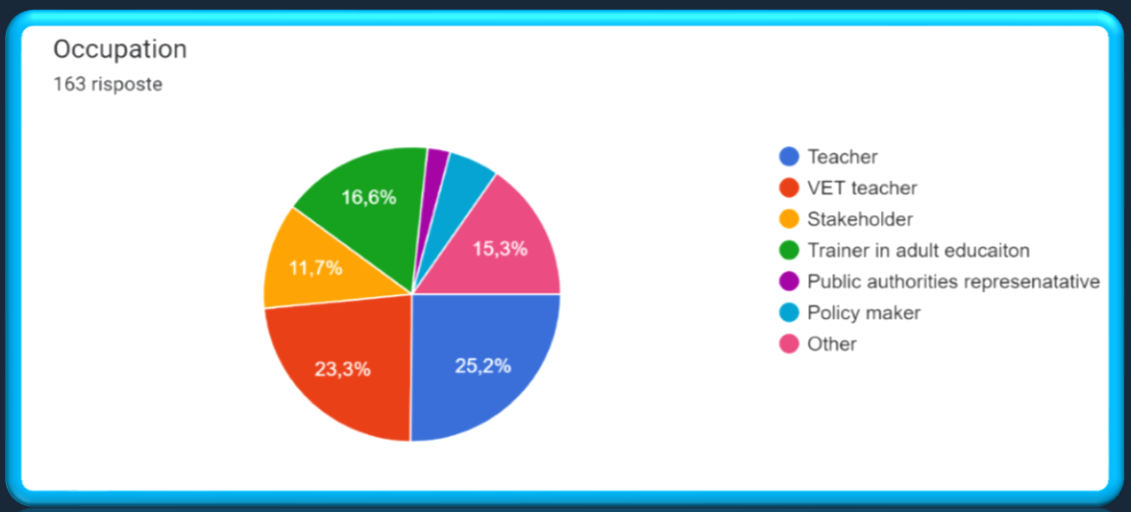
Država	Število prijav
Grčija	40
Slovenija	32

Italija	36
Nemčija	11
Ciper	23
Bolgarija	35

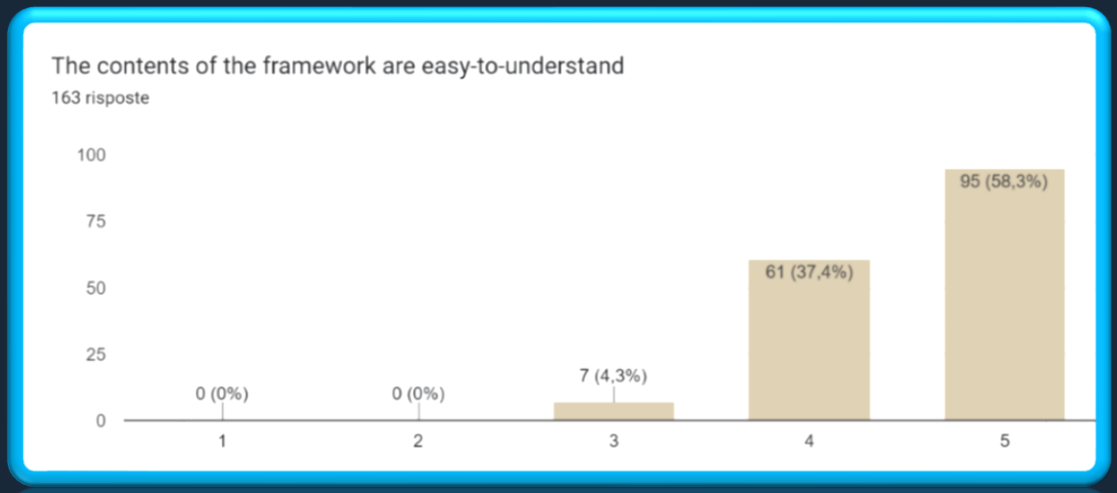
Povratne informacije udeležencev.

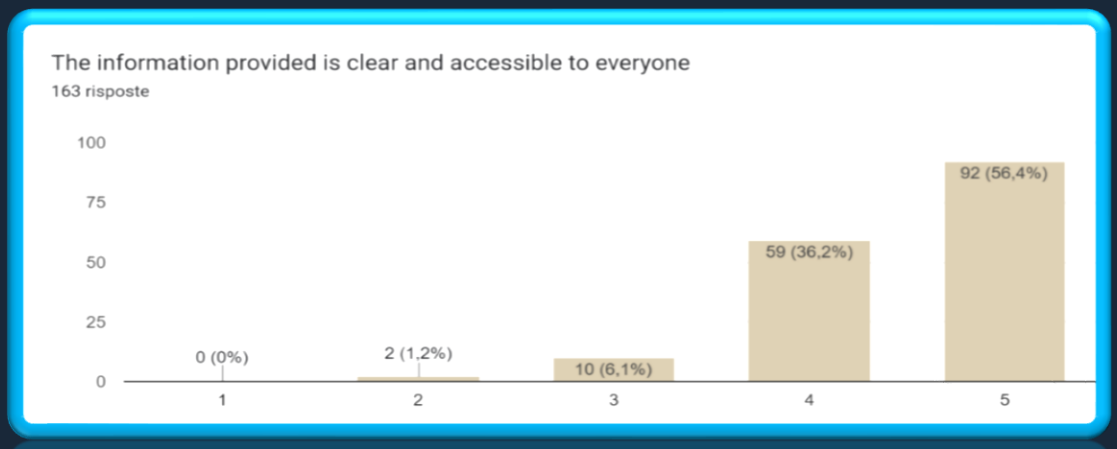
Poklici ciljne skupine

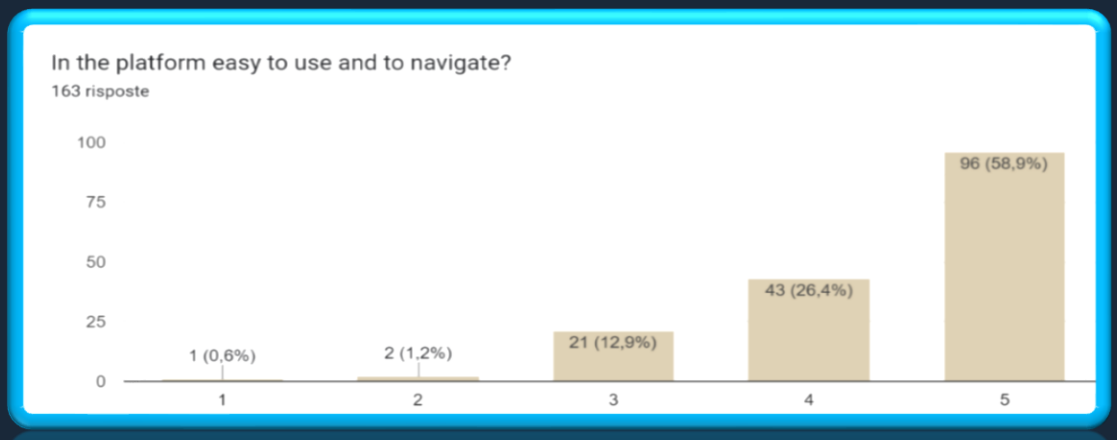




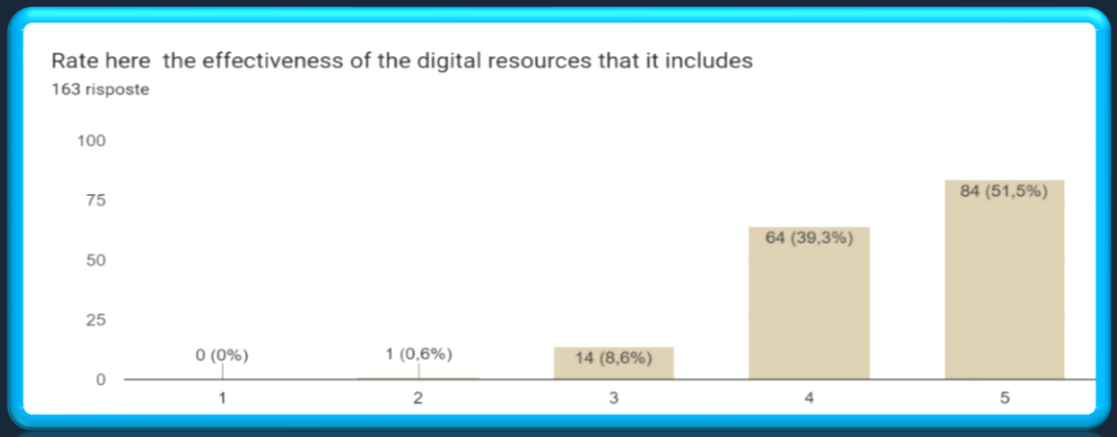
Co-funded by the
Erasmus+ Programme
of the European Union

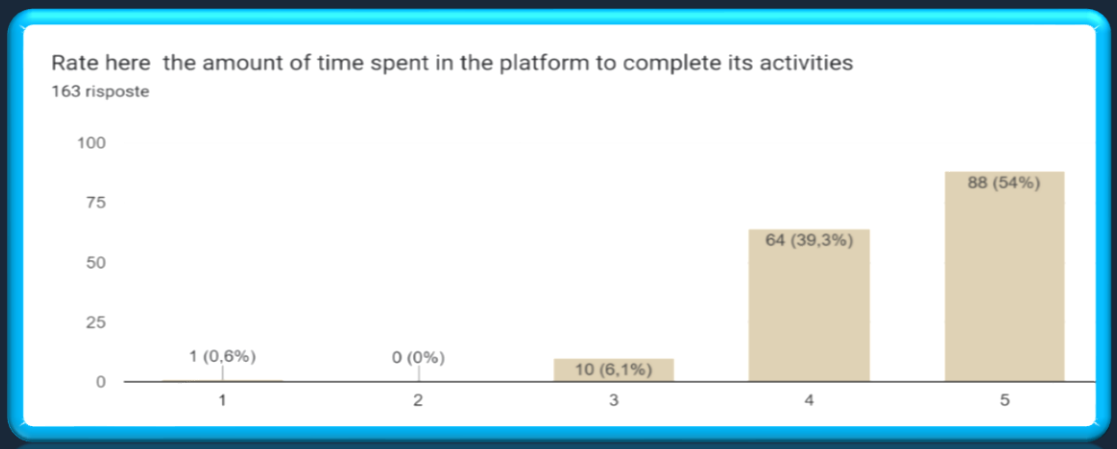


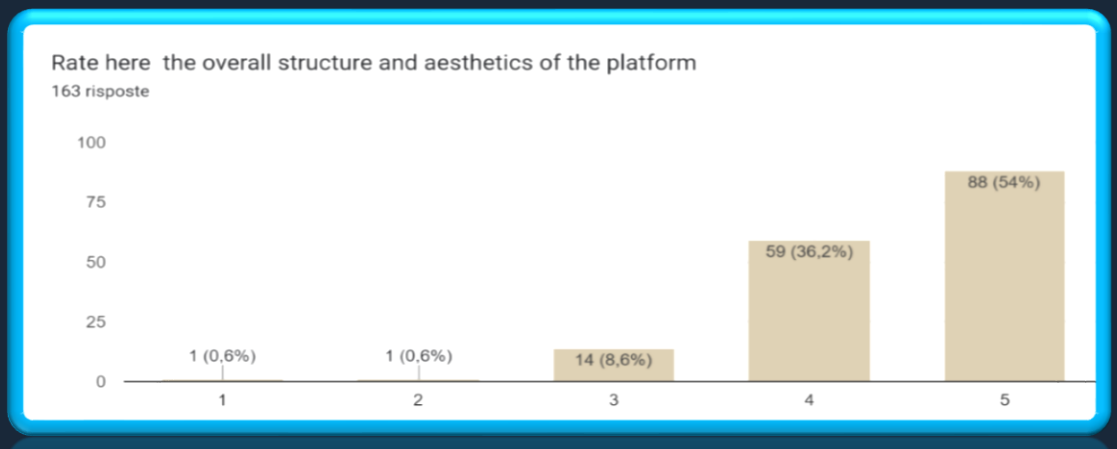




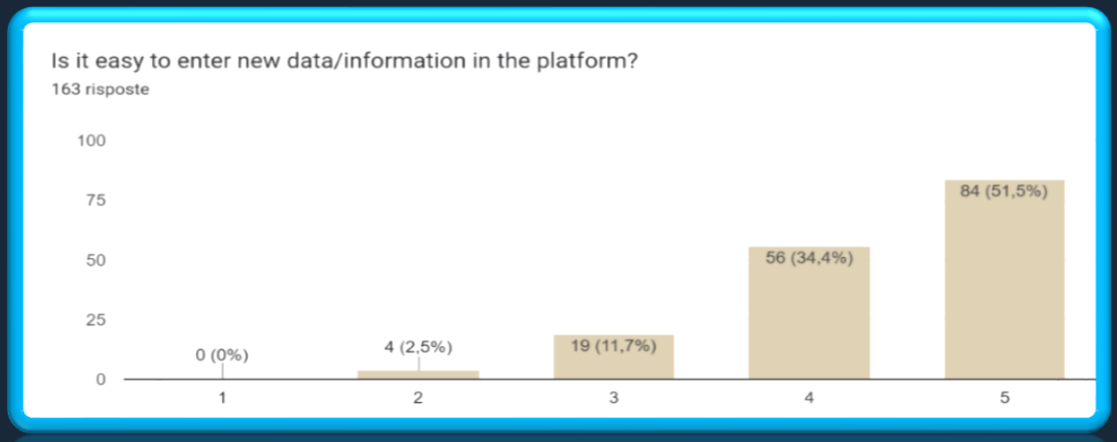
Co-funded by the
Erasmus+ Programme
of the European Union

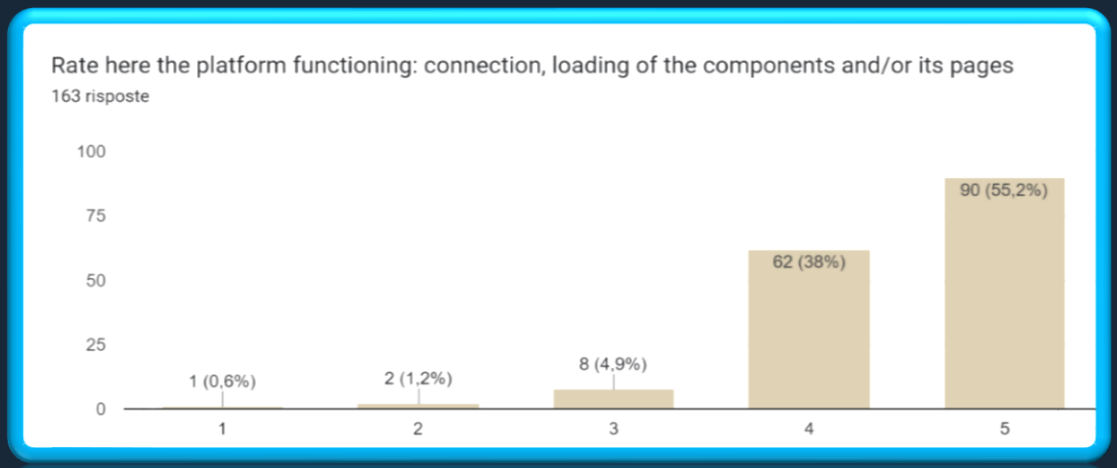


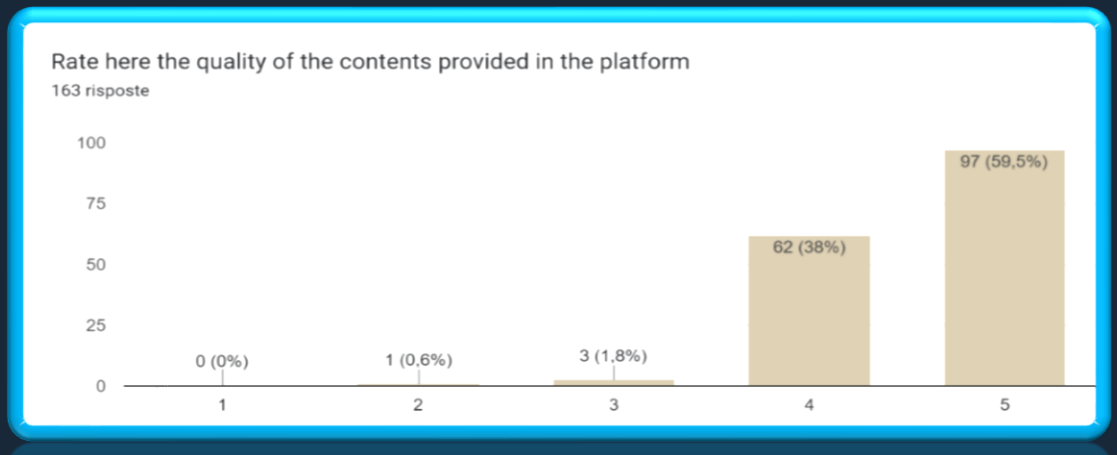


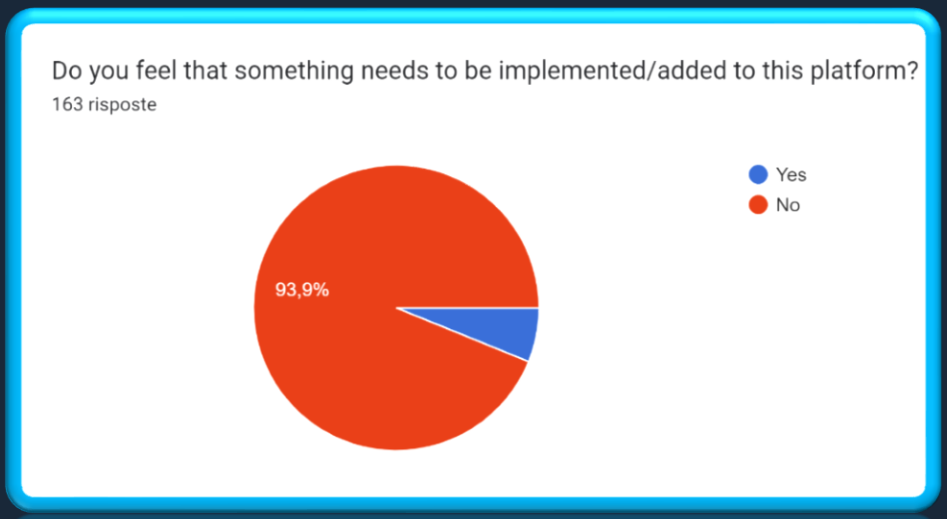


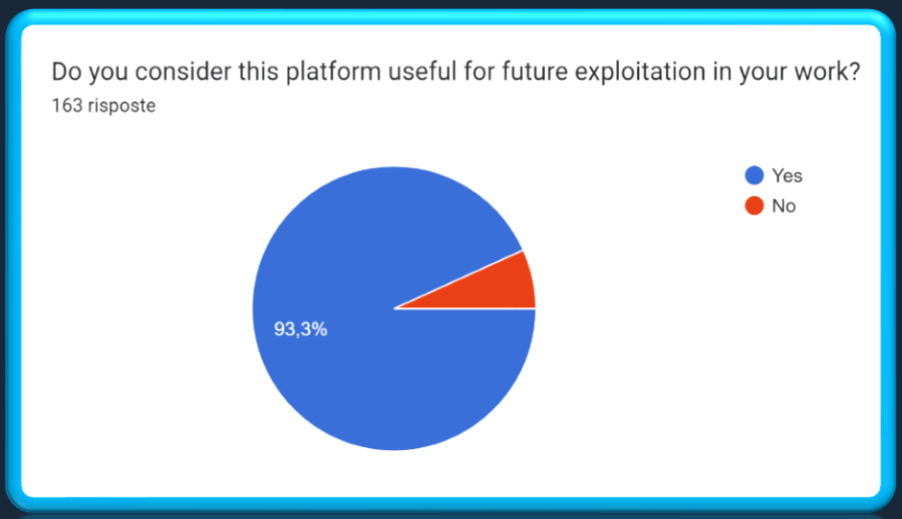
Co-funded by the
Erasmus+ Programme
of the European Union











Kot je razvidno iz zgornjih slik, ki prikazujejo odgovore, zbrane po pilotnem testiranju v vsaki partnerski državi, so udeleženci pilotnega testiranja izrazili visoko stopnjo zadovoljstva pri ocenjevanju različnih vidikov platforme za e-učenje, kot so njena vsebina, enostavnost uporabe in navigacije, kakovost naloženih gradiv in delovanje platforme, pri čemer so dodelili ocene med 4 in 5 (pri čemer je 5 najvišja ocena).

Prav tako so udeleženci navedli uporabnost platforme za prihodnje izkoriščanje njihovega dela. Večina udeležencev pilotnega preizkusa ni izrazila potrebe po

nadaljnjem izboljševanju platforme, 10 udeležencev (6,1 %) pa je predlagalo nekatere posebne popravke, ki jih je treba upoštevati v skladu s povratnimi informacijami, navedenimi v nadaljevanju:

- manjkajo slovenski prevodi
- v kvizih manjkajo bolgarska vprašanja
- ob izbiri jezika bi se morale prikazati samo informacije v tem jeziku
- več informativnih videoposnetkov

Čeprav je vprašalnik, ki je bil uporabljen za pilotni preizkus, pokazal visoko raven splošnega zadovoljstva, je bilo treba izpostaviti in upoštevati nekatere vidike za končno izboljšanje platforme in njene vsebine, kot je razvidno iz posebnih povratnih informacij, ki so povzete v nadaljevanju.

Pozitivne povratne informacije

- *Zanimiva platforma*
- *Dobra zasnova in zelo uporabna*
- *Menim, da je to platformo enostavno razumeti in uporabljati, prav tako je zelo estetska*
- *Platforma je zelo preprosta za uporabo in jo je mogoče zlahka uporabljati.*
- *Zelo dobra*
- *Mislim, da je uporabna in prijazna uporabniku*
- *Zelo uporabna in jasna razdelitev vsebine v platformi*
- *Odlično*
- *Všeč mi je, da se izvajajo primeri iz resničnega življenja*
- *Simulacija resničnega življenja je koristna*
- *To znanje mi je manjkalo*
- *Enostaven za razumevanje in praktičen*
- *Interaktivna navigacija in informacije, pridobljene na spletni strani, so bile odlične*
- *Resnično uživam v brskanju po spletni strani in izvedel sem veliko novega o podatkih in zasebnosti*
- *Vsekakor bom to, kar sem se naučil o vizualizaciji podatkov, uporabil v prihodnosti in uporabil učne nasvete platforme*
- *Zelo zanimivo in polno informacij, ki bi jih morali poznati vsi učitelji*
- *Zanimivo! Veliko sem se naučil o interaktivnosti in upravljanju digitalnih podatkov*
- *Digitalni svet je povsod okoli nas in pomembno je, da znamo upravljati s podatki in informacijami!*
- *Platforma je zelo zanimiva in enostavna za branje*

Vidiki, ki jih je treba izboljšati

- *Najdemo nekaj slovničnih napak*
- *Potrebna je optimizacija za mobilne naprave.*

- *Gumb za nazaj se je kvaril, "slovenska stran" je bila večinoma v angleščini, čudno oblikovanje, estetsko neprijetno*
- *Vsebina se zdi uporabna, vendar je način njene predstavitve včasih neprijeten in zmeden. V nekaterih poglavjih sta vključena kviz in predstavitev genial.ly, v drugih pa sploh ne. Vsebina v genial.ly in pdf se ponavlja in je nejasna.*
- *Ni skladna med moduli*
- *kviz je bil čudno oblikovan (dvojne številke).*
- *V nekaterih kvizih so manjkali odgovori, v drugih so bila vprašanja z več 100 % pravilnimi odgovori, tako da je kviz postal igra ugibanja (npr. 5.4).*
- *Predstavitve so se nalagale nekoliko dlje časa, sicer pa je bila vsebina uporabna.*
- *Geniallys so se nalagali kar nekaj časa. Vsebina se zdi uporabna, vendar je način njene predstavitve včasih neprijeten in zmeden. V nekaterih poglavjih sta vključena kviz in predstavitev genial.ly, v drugih pa sploh ne. Vsebina v genial.ly in pdf se ponavlja in je nejasna.*

4.3 Sklep

Faza pilotnega testiranja se je na splošno izkazala za pozitivno, saj je pokazala zadovoljstvo večine udeležencev, ki so pozitivno ocenili rezultate projekta in njihovo uporabnost.

Hkrati so bili izpostavljeni vidiki, ki jih je treba izboljšati, večinoma pa so se nanašali na nekatere vidike, povezane s kvizi. V zvezi s tem so se podani predlogi nanašali na možnost, da se "najprej odpravijo očitnejše težave, kot so slovnica, dvojne številke v kvizih, manjkajoči odgovori itd. Nato se bi morali lotiti nadgradnje oblikovanja spletne strani (zmanjšati zgornjo pasico, premakniti module proti vrhu, bolje uporabite razmike in postavitev (na vseh straneh). Nazadnje pa se moramo posvetiti času nalaganja za Geniallys."

4.4 Priloge

Annex I - I Pilot test vprašalnik
https://docs.google.com/forms/d/e/1FAIpQLSdLMxrfoPSlRcKhAgGl_Ph0LJceFrdhE5wSCiV0lWbhORUElA/viewform

Annex II - II IO1 Validacija https://drive.google.com/drive/folders/1rIvFJQheUiG38li7rAG5GxIAyN_e-y0o

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

5 PRISTOP EU K DIGITALNI VARNOSTI

5.1 Splošni pristop EU k kibernetski varnosti

EU je sprejela celovit pristop h kibernetski varnosti s številnimi uredbami in direktivami za zaščito digitalne infrastrukture in osebnih podatkov. Nekateri ključni elementi strategije EU za kibernetsko varnost vključujejo:

Splošna uredba o varstvu podatkov (GDPR), ki določa pravila za obdelavo, shranjevanje in zaščito osebnih podatkov v EU. Splošna uredba o varstvu podatkov velja za vsa podjetja, ki poslujejo v EU, in za vsa podjetja, ki obdelujejo osebne podatke državljanov EU.

Direktiva o varnosti omrežij in informacij (direktiva NIS), ki določa ukrepe kibernetske varnosti za ponudnike kritične infrastrukture, vključno z energetskim, prometnim in zdravstvenim sektorjem. Od teh ponudnikov zahteva, da o večjih varnostnih incidentih poročajo nacionalnim organom.

Zakon o kibernetski varnosti, ki vzpostavlja okvir za vzpostavitev certifikacijskih shem kibernetske varnosti za digitalne izdelke, storitve in procese po vsej EU.

Strategija EU za kibernetsko varnost, ki je celovit načrt za izboljšanje kibernetske varnosti v EU. Vključuje pobude za krepitev sodelovanja med državami članicami, spodbujanje raziskav in inovacij ter krepitev infrastrukture kibernetske varnosti EU.

5.2 Načrt digitalnega izobraževanja

V Evropi se vse bolj zavedamo pomena digitalnega izobraževanja za pripravo posameznikov na prihodnost. Evropska komisija je začela izvajati nov akcijski načrt za digitalno izobraževanje, katerega cilj je spodbujati uporabo tehnologije v izobraževanju in izboljšati digitalne spretnosti evropskih državljanov. Načrt vključuje pobude, kot so zagotavljanje visoko hitrostnega dostopa do interneta vsem šolam, večja uporaba digitalnih orodij pri poučevanju in učenju ter podpora razvoju inovativnih izobraževalnih tehnologij. Načrt se osredotoča tudi na izboljšanje digitalnih spretnosti učiteljev in spodbujanje možnosti vseživljenjskega učenja za vse državljane. Evropska unija upa, da bo z vlaganjem v digitalno izobraževanje spodbujala gospodarsko rast, socialno vključenost in digitalno državljanstvo v regiji.

Načrt vsebuje 13 ukrepov, od katerih so trije neposredno povezani z digitalnim izobraževanjem in usposabljanjem:

Ukrep 5 (Načrti digitalne preobrazbe za ustanove za izobraževanje in usposabljanje) - cilj je podpreti prizadevanja za digitalno preobrazbo prek projektov sodelovanja Erasmus+, vzpostaviti akademije za učitelje za razvoj in sodelovanje ter uvesti spletno orodje za samoocenjevanje, imenovano SELFIE za učitelje, s katerim se ugotavljajo področja za izboljšave.

Ukrep 6 (Etične smernice o uporabi umetne inteligence in podatkov pri poučevanju in učenju za izobraževalce) - vse bolj je treba razumeti potencial umetne inteligence (AI) in ozaveščati o možnih tveganjih, saj bi lahko spremenila izobraževanje in usposabljanje ter tudi naše vsakdanje življenje. Smernice zagotavljajo praktično podporo in smernice za uporabo AI, pomagajo pri poučevanju in učenju, predlagajo boljše podporne sisteme za upravne postopke ter predstavljajo etične vidike.

Ukrep 7 (Skupne smernice za učitelje in vzgojitelje) - izobraževanje in usposabljanje sta ključnega pomena za razvijanje veščin kritičnega mišljenja državljanov, ki so potrebne za krmarjenje v spletnem svetu zaradi njegovih edinstvenih značilnosti, kot so algoritmi, "informacijski mehurčki" in "odmevne komore". Zato je podpora učiteljem in vzgojiteljem s smernicami in praktičnimi primeri bistvena za spodbujanje digitalne pismenosti in boj proti dezinformacijam. Smernice ponujajo praktične nasvete in načrte dejavnosti za osnovnošolske in srednješolske učitelje, ne glede na njihovo znanje o digitalnem izobraževanju, dopolnjuje pa jih končno poročilo, v katerem so predstavljene ključne ugotovitve in priporočila strokovne skupine.

Na splošno je akcijski načrt za digitalno izobraževanje celovita strategija za spodbujanje digitalnega izobraževanja in izboljšanje digitalnih spretnosti po vsej Evropi. V njem je priznan pomen tehnologije pri pripravi učencev na prihodnost ter spodbujanju gospodarske rasti in socialne vključenosti.

5.3 Okvirji, ki vsebujejo znanja in spretnosti s področja digitalne varnosti

Eksponentna rast digitalnih tehnologij je poudarila potrebo po digitalni varnosti. Pomen razvijanja in izboljševanja veščin digitalne varnosti je omenjen v okvirih kompetenc na področju digitalnih tehnologij, kot sta Evropska digitalna kompetenca, znana kot DigComp 2.2, in Evropska digitalna kompetenca za izobraževalce, znana kot DigCompEdu.

Okvir DigComp evropskim državljanom omogoča, da bolje razumejo, kaj pomeni digitalna kompetenca ter kako oceniti in razviti lastno digitalno kompetenco. Pet glavnih področij v okviru kompetenc so informacijska in podatkovna pismenost, komunikacija in sodelovanje, ustvarjanje digitalnih vsebin, varnost in reševanje problemov.

Okvir DigCompEdu opisuje, kaj za izobraževalce pomeni biti digitalno kompetenten, in je namenjen vsem izobraževalcem na vseh ravneh izobraževanja. Okvir prikazuje 22 kompetenc, ki so razvrščene v šest področij. Ta področja so strokovno udejstvovanje, digitalni viri, poučevanje in učenje, ocenjevanje, opolnomočenje učencev in omogočanje digitalne usposobljenosti učencev.

5.4 Financiranje raziskav in inovacij za digitalno učenje

EU financira raziskave in inovacije na področju kibernetske varnosti in digitalnih tehnologij v okviru programov, kot so Obzorje Evropa, program Digitalna Evropa in CEF (Instrument za povezovanje Evrope). Slednji podpira infrastrukturo za kibernetsko

varnost in skupine za odzivanje na incidente. InvestEU financira pomembne verige na področju kibernetske varnosti v zasebnem sektorju. Horizon Europe, eden najpomembnejših programov financiranja kibernetske varnosti, financira inovativne rešitve na področju kibernetske obrambe, katerih cilj je podpora malim in srednje velikim podjetjem, simulacijam in zaščiti kritičnih podatkov. Ti programi sodelujejo z evropskim industrijskim, tehnološkim in raziskovalnim kompetenčnim centrom za kibernetsko varnost, skupkom strokovnjakov in organizacij za uvajanje kibernetske varnosti po državah.

5.5 Koristni viri in orodja

Četrta industrijska revolucija je prinesla hiter razvoj na področju novih tehnologij, komunikacij in avtomatizacije. Ta razvoj je privedel do prehoda na digitalno okolje na področju zaposlovanja in izobraževanja. Pandemija je ta prehod pospešila, saj je ustvarila večjo potrebo po učenju in delu na daljavo. To je ustvarilo novo dinamiko in izzive ob vsesplošni in razširjeni uporabi digitalnih orodij (platforme, spletne strani itd.).

V tem kontekstu je EU prepoznala zagon in sprejela akcijski načrt za digitalno izobraževanje (2021-2027), v katerem so določeni cilji Evropske komisije za doseganje učinkovitega, vključujočega in dostopnega digitalnega izobraževanja v Evropski uniji. EU je zlasti ustvarila vrsto digitalnih orodij za lažje delovanje EU, vprašanja usposabljanja ter komunikacijo med organizacijami in posamezniki po vsej EU. Glavna digitalna orodja, ki jih je uvedla EU, so:

Vrata za šolsko izobraževanje. Gre za "spletni katalog", v katerem lahko poiščete izobraževalno gradivo, sodelujete v spletnih tečajih in dostopate do virov usposabljanja za učitelje in na splošno za ljudi, ki jih zanima šolsko izobraževanje v Evropi. School Education Gateway vključuje publikacije, priročnike, učna gradiva, ki so jih pripravile institucije EU, projekte, ki jih financira EU, brezplačne spletne tečaje, spletne seminarje in najnovejše novice, povezane z evropsko šolsko politiko in izobraževanjem.

eTwinning platforma je namenjena šolskemu osebju v evropskih državah, da bi učiteljem in ravnateljem omogočila medsebojno komuniciranje, vzpostavila mrežo, ki omogoča razvoj sodelovanja, izmenjavo in koristne projekte za evropski šolski sistem. eTwinning želi z uporabo informacijskih in komunikacijskih tehnologij spodbujati sodelovanje šol v Evropi: prek platforme lahko namreč šolsko osebje komunicira, izmenjuje vire in ustvarja projekte v 30 jezikih.

Učni kotiček. Gre za platformo, namenjeno tako učencem kot učiteljem. Glede na starostno skupino so učencem na voljo različna gradiva, vključno z igrami, tekmovanji in knjigami dejavnosti, ki jim omogočajo spoznavanje različnih vidikov Evropske unije, od zakonov do okolja in zgodovine. Za učitelje je platforma dober vir za iskanje izobraževalnega gradiva, namenjenega osnovnošolcem ali srednješolcem.

Podpora, možnosti za napredno učenje in usposabljanje za mlade (Skip-Youth). Gre za mrežo sedmih centrov, od katerih se vsak ukvarja s prednostnim področjem na področju mladine. Konkretno platforma zagotavlja učne vire za mlade, tečaje usposabljanja in priložnosti za mreženje.

Elektronska platforma za izobraževanje odraslih v Evropi (EPALE). Gre za večjezično in odprto evropsko spletno skupnost, ki se ji lahko pridružijo strokovnjaki s področja izobraževanja odraslih iz vse Evrope. Platforma ponuja možnost uvajanja digitalnih spretnosti prek brezplačnih spletnih tečajev, dostop do primerov dobrih praks v izobraževanju odraslih in virov za e-učenje.

Samorefleksija o učinkovitem učenju s spodbujanjem uporabe inovativnih izobraževalnih tehnologij (SELFIE) je brezplačno orodje, namenjeno pomoči šolam pri vključevanju digitalnih tehnologij v poučevanje, učenje in ocenjevanje. SELFIE ima močno raziskovalno podlago in je bil razvit na podlagi okvira Evropske komisije za spodbujanje učenja v digitalni dobi v izobraževalnih organizacijah.

6 NACIONALNI KONTEKST

6.1 Slovenija

Slovenija si v zadnjih letih aktivno prizadeva za izboljšanje svoje digitalne infrastrukture in infrastrukture za kibernetsko varnost. Država je prepoznala pomen kibernetske varnosti kot bistvenega elementa nacionalne varnosti in razvila različne pobude za izboljšanje svojih zmogljivosti na področju kibernetske varnosti. Slovenske nacionalne zmogljivosti kibernetske varnosti in njihove vloge so opredeljene na operativni ravni: SI-CERT je nacionalna enota za zagotavljanje kibernetske varnosti, MORS je odgovoren za področje obrambe ter varstva pred naravnimi in drugimi nesrečami (vključno z zaščito kritične infrastrukture), policija zagotavlja kibernetsko varnost v okviru javne varnosti in boja proti kibernetskemu kriminalu, Slovenska obveščevalno-varnostna agencija (SOVA) izvaja protiobveščevalno dejavnost, nastajajoči SIGOVCERT pa skrbi za kibernetsko varnost v javni upravi. Na področju udejstvovanja so vključeni tudi drugi deležniki, kot so upravljavci kritične infrastrukture v zasebnem in javnem sektorju.

POBUDA 1	
Ime	Safe on the Internet
Lokacija	National
Trajanje	2011 -

Opis	SI-CERT ozavešča prebivalce in izvaja izobraževalni program "Varno na internetu". Ta POBUDA je namenjena širši javnosti, s posebnimi vsebinami za mala podjetja, obrtnike in samostojne podjetnike pa ozavešča o varni uporabi interneta. Projekt financira Ministrstvo za izobraževanje, znanost in šport, sodeluje pa tudi v kampanjah evropskega meseca kibernetske varnosti.
Rezultat/učinek	POBUDA je doslej sodelovala z več organizacijami in institucijami, kot so: Agencija Evropske unije za varnost omrežij in informacij, Evropski potrošniški center, Agencija za komunikacijska omrežja in storitve Republike Slovenije, Informacijski pooblaščenec RS, Urad za intelektualno lastnino, Združenje bank Slovenije, Zveza potrošnikov Slovenije.
Link do vira	https://www.varninainternetu.si/

POBUDA 2	
Ime	Safer Internet Centre Slovenia
Lokacija	National
Trajanje	2005 -
Opis	Center za varnejši internet (SIC) Slovenija je nacionalni projekt za spodbujanje in zagotavljanje boljšega interneta za otroke. Projekt sofinancira Evropska izvršna agencija za zdravje in digitalno politiko (HaDEA), v Sloveniji pa ga finančno podpira tudi Urad vlade za informacijsko varnost. Projekt vodi konzorcij partnerjev, ki ga koordinirajo Fakulteta za družbene vede Univerze v Ljubljani, Akademska in raziskovalna mreža Slovenije (ARNES), Zveza prijateljev mladine Slovenije (ZPMS) in Mladinsko informativno svetovalno središče Slovenije (MISSS). SAFE.SI od leta 2005 deluje kot nacionalna točka za ozaveščanje otrok in mladostnikov o varni rabi interneta in mobilnih naprav. Njihove dejavnosti so namenjene štirim ciljnim skupinam: otrokom, mladostnikom, staršem in strokovnjakom (učiteljem, socialnim delavcem, mladinskim delavcem itd.). Poslanstvo kampanje

	ozaveščanja je informirati mlade uporabnike interneta in mobilnih naprav, kako se lahko zaščitijo pred tveganji ter varno in odgovorno uporabljajo splet in druge nove tehnologije.
Rezultat/učinek	SAFE.si spodbuja sodelovanje slovenskih deležnikov ter institucij iz javne in zasebne sfere za večjo varnost otrok in mladostnikov na spletu ter njihovo zaščito pred morebitnimi nevarnostmi in tveganji. Sodelovali so z Agencijo za komunikacijska omrežja in storitve RS, Združenjem za pediatrijo, Ministrstvom za izobraževanje, znanost in šport (priprava akcijskega načrta za digitalizacijo izobraževanja) itd.
Link do vira	https://safe.si/

PREDLOGI ZA VREDNOTENJE IN IZVAJANJE

Poleg omenjenih pobud Slovenija prispeva k nacionalnemu sistemu kibernetske varnosti tudi z visokošolskimi programi (npr. Fakulteta za računalništvo in informatiko) in predmeti o kibernetski varnosti na vseh ravneh izobraževanja ter z rezultati raziskovalnih organizacij. Strokovna združenja so dala pobudo za izboljšave in pomoč pri ozaveščanju različnih ciljnih skupin (npr. Gospodarska zbornica Slovenije, ISACA, SI-CERT). Čeprav si Slovenija prizadeva za izobraževanje državljanov o digitalni varnosti, so še vedno možne izboljšave.

Da bi izboljšala raven znanja med državljani, bi lahko Slovenija izvajala pobude brez povezave, na primer promocijo v osnovnih in srednjih šolah. Digitalna varnost bi lahko postala obvezen del šolskega učnega načrta, s čimer bi zagotovili, da se otroci že od zgodnjega otroštva učijo o spletnih varnostnih tveganjih. Pobude bi bilo treba razširiti na širše ciljne skupine, kot so odrasli in podjetja. V Sloveniji je bila pripravljena strategija kibernetske varnosti, vendar brez akcijskega načrta za njeno izvajanje.

6.2 Grčija

V Grčiji sta digitalna in kibernetska varnost v zadnjih letih postali vse pomembnejši, saj je država postala bolj odvisna od tehnologije in interneta. Grška vlada je sprejela ukrepe za okrepitev ukrepov kibernetske varnosti in zaščito kritične infrastrukture, kot sta energetski in prometni sistem države. Grško ministrstvo za digitalno politiko je leta 2019 uvedlo novo nacionalno strategijo kibernetske varnosti, ki vključuje vrsto pobud za izboljšanje kibernetske varnosti v javnem in zasebnem sektorju. Strategija se osredotoča na štiri ključna področja:

zaščito, odkrivanje, odzivanje in okrevanje. Vključuje ukrepe, kot so izboljšanje varnosti kritične infrastrukture, razvoj kampanj za ozaveščanje o kibernetski varnosti in izboljšanje sposobnosti države za odzivanje na kibernetske grožnje. Grška vlada je ustanovila tudi nacionalni organ za kibernetsko varnost, ki je odgovoren za usklajevanje prizadevanj za kibernetsko varnost v javnem in zasebnem sektorju. Organ si prizadeva za prepoznavanje in zmanjševanje tveganj za kibernetsko varnost, razvoj politik in predpisov o kibernetski varnosti ter zagotavljanje smernic in podpore organizacijam in posameznikom.

POBUDA 1	
Ime	National Cybersecurity Strategy
Lokacija	National, public sector
Trajanje	2019 –
Opis	Grško ministrstvo za digitalno politiko, telekomunikacije in informacije je leta 2019 začelo izvajati nacionalno strategijo kibernetske varnosti. Cilj strategije je izboljšati kibernetsko varnost v javnem in zasebnem sektorju ter zaščititi kritično infrastrukturo pred kibernetskimi grožnjami. Strategija temelji na štirih glavnih stebrih: zaščita, odkrivanje, odzivanje in okrevanje. Ti stebri so podprti z vrsto pobud, med katerimi so: krepitev varnosti kritične infrastrukture razvijanje ozaveščenosti o kibernetski varnosti izboljšanje sposobnosti države za odzivanje na kibernetske grožnje spodbujanje mednarodnega sodelovanja. The National Cybersecurity Strategija vključuje tudi posebne cilje in roke za izvajanje pobud. Na splošno strategija predstavlja celovit pristop k izboljšanju kibernetske varnosti v Grčiji in zaščiti pred kibernetskimi grožnjami
Rezultat/učinek	Izboljšana ozaveščenost o kibernetski varnosti okrepljena varnost kritične infrastrukture:

	Okrepljene zmogljivosti za odzivanje na incidente Okrepljeno mednarodno sodelovanje Na splošno je nacionalna strategija kibernetske varnosti pozitivno vplivala na kibernetsko varnost v Grčiji. Čeprav je treba še vedno opraviti veliko dela pri obravnavi trenutnih groženj in izzivov, je strategija pripomogla k večji ozaveščenosti o tveganjih za kibernetsko varnost, izboljšanju varnosti kritične infrastrukture, povečanju zmogljivosti za odzivanje na incidente in spodbujanju mednarodnega sodelovanja.
Link do vira	https://www.trade.gov/market-intelligence/greece-cyber-security-strategy

POBUDA 2	
Ime	National Cybersecurity Authority
Lokacija	National, public sector
Trajanje	2019 -
Opis	Nacionalni organ za kibernetsko varnost (NCA) je grška vladna agencija, ki je odgovorna za usklajevanje in izvajanje politik in pobud na področju kibernetske varnosti v javnem in zasebnem sektorju. Organ NCA je bil ustanovljen leta 2019 kot del grške nacionalne strategije kibernetske varnosti. Glavne odgovornosti agencije NCA vključujejo: razvoj in izvajanje politik in predpisov o kibernetski varnosti: NCA je odgovoren za razvoj politik in predpisov za izboljšanje kibernetske varnosti v različnih sektorjih v Grčiji. usklajevanje prizadevanj za kibernetsko varnost: NCA usklajuje prizadevanja za kibernetsko varnost med različnimi vladnimi agencijami ter organizacijami zasebnega sektorja in mednarodnimi partnerji. ugotavljanje in zmanjševanje tveganj za kibernetsko varnost: NCA je odgovoren za prepoznavanje in zmanjševanje tveganj za kibernetsko varnost, vključno s

	tistimi, ki so povezana s kritično infrastrukturo. Zagotavljanje smernic in podpore: NCA zagotavlja smernice in podporo organizacijam in posameznikom glede najboljših praks na področju kibernetske varnosti in odzivanja na incidente.
Rezultat/učinek	Ker je bil nacionalni organ za kibernetsko varnost v Grčiji ustanovljen leta 2019, je še razmeroma zgodaj, da bi lahko v celoti ocenili rezultate in učinek njegovih dejavnosti. Vendar je bilo od njegove ustanovitve zabeleženih več pomembnih dogodkov, ki kažejo, da ima NCA pozitiven vpliv na kibernetsko varnost v Grčiji. Organ NCA je s kampanjami za ozaveščanje javnosti, programi usposabljanja in drugimi pobudami igral pomembno vlogo pri ozaveščanju o tveganjih za kibernetsko varnost in najboljših praksah v Grčiji. To je pripomoglo k izboljšanju splošne ravni kibernetske varnosti v državi. Na splošno je organ NCA od svoje ustanovitve leta 2019 dosegel pomemben napredek pri izboljšanju kibernetske varnosti v Grčiji. Čeprav je treba še vedno opraviti veliko dela za reševanje trenutnih izzivov na področju kibernetske varnosti, je NCA dosegel pozitiven učinek in ima ključno vlogo pri zaščiti Grčije pred kibernetskimi grožnjami.
Link do vira	https://www.concordia-h2020.eu/consortium/national-cyber-authority-ncsa/

PREDLOGI ZA VREDNOTENJE IN IZVAJANJE

Čeprav je Grčija dosegla napredek pri ozaveščanju državljanov o digitalni varnosti, so še vedno možne izboljšave. V nadaljevanju je predstavljenih nekaj možnih rešitev za izboljšanje ravni znanja in ozaveščenosti o digitalni varnosti v Grčiji, s poudarkom na tem, kako lahko druge države/institucije izvajajo podobne pobude:

POBUDE ZA IZOBRAŽEVANJE: Ena od možnih rešitev je večji poudarek na digitalni varnosti v izobraževalnih ustanovah, kot so šole in univerze. Vlade in ustanove lahko razvijejo in izvajajo izobraževalne programe, ki mlade učijo osnovnih veščin in praks na področju kibernetske varnosti. Ti programi so lahko namenjeni tudi odraslim, ki morda niso imeli priložnosti spoznati digitalne varnosti v zgodnejših letih življenja.

KAMPANJE ZA OZAVEŠČANJE JAVNOSTI: Vlade lahko izvajajo kampanje za ozaveščanje javnosti, da bi povečale ozaveščenost o pomenu digitalne varnosti in zagotovile navodila, kako se zaščititi na spletu. Te kampanje so lahko v različnih oblikah, kot so plakati, oglasi in objave v družbenih medijih.

CERTIFIKATI ZA KIBERNETSKO VARNOST: Druga rešitev je uvedba certifikatov kibernetske varnosti, ki jih lahko posamezniki pridobijo po opravljenem tečaju usposabljanja. Ti certifikati lahko posameznikom zagotovijo priznano kvalifikacijo, ki dokazuje njihovo znanje in spretnosti na področju kibernetske varnosti.

SODELOVANJE Z JAVNIM SEKTORJEM: Vlade lahko sodelujejo z organizacijami zasebnega sektorja, da bi državljanom zagotovile usposabljanje in podporo na področju digitalne varnosti. Telekomunikacijska podjetja lahko na primer svojim strankam zagotovijo smernice o varni uporabi interneta.

MEDNARODNO SODELOVANJE: Države lahko sodelujejo pri pobudah za izboljšanje digitalne varnosti. To lahko vključuje izmenjavo informacij o kibernetskih grožnjah in najboljših praksah, skupne vaje usposabljanja in usklajeno odzivanje na kibernetske incidente.

6.3 Italija

Italija je sprejela pomembne ukrepe za izboljšanje splošne digitalne/kibernetske varnosti. Država se zaveda pomena kibernetske varnosti in sprejema različne pobude za izboljšanje svojih zmogljivosti za kibernetsko varnost. Leta 2021 je bila ustanovljena nacionalna agencija za kibernetsko varnost (ACN). Njen cilj je povečati nacionalno kibernetsko varnost in odpornost za digitalni razvoj države, doseči nacionalno in evropsko strateško avtonomijo v digitalnem sektorju, spodbujati posebna usposabljanja za razvoj delovne sile v tem sektorju, podpirati kampanje ozaveščanja, spodbujati splošno kulturo kibernetske varnosti ter razvijati mednarodne ukrepe in projekte za varen svetovni kibernetski prostor. Vlada je uvedla tudi nacionalno strategijo kibernetske varnosti, katere cilj je okrepiti digitalno odpornost in zmogljivosti države proti kibernetskim grožnjam. Osredotoča se na zaščito kritične infrastrukture, izmenjavo informacij, raziskave in razvoj ter usposabljanje in izobraževanje.

POBUDA 1	
Ime	Cloud Strategy Italy
Lokacija	For the Italian Public Administration
Trajanje	15/12/2021 -
Opis	Strategija za oblak v Italiji, ki sta jo pripravila Oddelek za digitalno preobrazbo in Nacionalna agencija

	za kibernetsko varnost (ACN), vsebuje strateške smernice za prehod podatkov in digitalnih storitev javne uprave v oblak s pomočjo tristopenjskega sistema klasifikacije podatkov. Strateški: podatki in storitve, katerih ogrožanje bi lahko vplivalo na nacionalno varnost. Kritični: podatki in storitve, katerih ogrožanje bi lahko povzročilo škodo pri ohranjanju funkcij, pomembnih za družbo, zdravje, varnost ter gospodarsko in socialno blaginjo države. Običajni: podatki in storitve, katerih ogrožanje ne povzroči prekinitve državnih storitev ali v vsakem primeru škoduje gospodarski in družbeni blaginji države. Z namenom usmerjanja in spodbujanja varnega, nadzorovanega in popolnega sprejetja tehnologij v oblaku v javnem sektorju v skladu z načeli varstva zasebnosti ter priporočili evropskih in nacionalnih institucij.
Rezultat/učinek	Digitalna infrastruktura bo zanesljivejša in varnejša, javna uprava pa se bo lahko organizirano odzvala na kibernetske napade ter zagotovila neprekinjeno in kakovostno uporabo podatkov in storitev.
Link do vira	https://www.acn.gov.it/

POBUDA 2	
Ime	Safer Internet Center – Connected Generations
Lokacija	National
Trajanje	1/07/2016 –
Opis	Projekt Center za varnejši internet (SIC) - Connected Generations sofinancira Evropska komisija v okviru programa Digitalna Evropa, koordinira ga Ministrstvo za izobraževanje in zasluge in je član mreže, ki jo spodbuja Evropska komisija na spletni platformi "Better Internet for Kids", ki jo upravlja European

	Schoolnet v tesnem sodelovanju z INSAFE (mreža, ki združuje vse evropske SIC-e) in Inhope (mreža, ki združuje vse evropske telefonske številke). Izobraževalno poslanstvo SIC je zagotavljanje informacij, nasvetov in podpore otrokom, najstnikom, staršem, učiteljem in vzgojiteljem za lažje poročanje o nezakonitem gradivu na spletu. Splošni cilj je razvijati storitve z inovativno in kakovostnejšo vsebino, da bi mladim uporabnikom zagotovili spletno varnost, hkrati pa povezane naložbe obravnavati kot "pozitivno" priložnost za "družbeno" in gospodarsko rast celotne skupnosti.
Rezultat/učinek	zagotavljanje podpore in svetovanja za ozaveščanje o spletnih nevarnostih.
Link do vira	https://www.generazioniconnesse.it/site/it/safer-internet-centre/

PREDLOGI ZA VREDNOTENJE IN IZVAJANJE

V Italiji obstaja več pobud na področju kibernetske varnosti. Pripravljena je bila tudi nacionalna strategija kibernetske varnosti 2022-2026, katere cilj je načrtovanje, usklajevanje in izvajanje ukrepov za večjo varnost in odpornost države. Ta strategija predvideva uresničitev 82 ukrepov do leta 2026. Veljaven predlog bi lahko bil, da se v šolske izobraževalne načrte vključijo predmeti o spletni varnosti in učne ure o kibernetski varnosti ter se ne prepuščajo le presoji dodatnih predmetov, obšolskih dejavnosti ali učnih načrtov šol, v katerih se učijo predmete, povezane z informacijskim usposabljanjem.

6.4 Ciper

Po navedbah OCECPR je "vizija ciprske strategije kibernetske varnosti delovanje informacijskih in komunikacijskih tehnologij na Cipru s potrebno stopnjo varnosti v korist vsakega uporabnika". Glavni cilj strategije je razviti in ohraniti varno elektronsko okolje na Cipru za vsa podjetja in državljane z razvojem politik v okviru sodelovanja med vsemi pristojnimi organi. V tej smeri je Ciper odobril številne ukrepe, ki so bili spodbujeni na nacionalni ravni, kot so oblikovanje okvira za varnost in celovitost informacijskih infrastruktur ter ozaveščanje vseh zainteresiranih strani in ciprske družbe o pomembnih varnostnih zadevah in oblikovanje skupin za odzivanje na računalniške grožnje (CCERT/CSIRT). Poleg tega je Ciper zavezan prispevati k evropskemu in mednarodnemu sodelovanju pri odzivanju na grožnje v kibernetskem prostoru.

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

POBUDA 1	
Ime	National Cybersecurity Coordination Centre (NCCC-CY) for the Republic of Cyprus
Lokacija	National
Trajanje	21 December 2021 -
Opis	Organ za digitalno varnost (DSA) je bil decembra 2021 s sklepom ciprskega ministrskega sveta imenovan za NCCC-CY. Njegove glavne naloge so zagotavljanje znanja in omogočanje dostopa do strokovnega znanja o industrijskih, tehnoloških in raziskovalnih vprašanjih kibernetske varnosti. Poleg tega je spodbujanje in omogočanje sodelovanja zagonskih podjetij, MSP ter akademskih in raziskovalnih skupnosti na nacionalni ravni v čezmejnih projektih in pri ukrepih na področju kibernetske varnosti, ki se financirajo iz ustreznih programov Unije. Poleg tega center zagotavlja tehnično pomoč zainteresiranim stranem, tako da jih podpira v fazi prijave projektov, ki jih upravlja kompetenčni center, in si prizadeva za vzpostavitev sodelovanja z ustreznimi dejavnostmi na nacionalni, regionalni in lokalni ravni, kot so nacionalne politike na področju raziskav, razvoja in inovacij na področju kibernetske varnosti, zlasti politike, navedene v nacionalni strategiji kibernetske varnosti.
Rezultat/učinek	Od 4. maja 2022 lahko DSA v sodelovanju s Fundacijo za raziskave in inovacije - CY črpa in usmerja razpoložljiva sredstva za kibernetsko varnost, potem ko je Evropska komisija odobrila njen predlog. Da je agencija DSA lahko delovala v tej smeri, jo je morala Evropska komisija temeljito oceniti glede njene sposobnosti upravljanja zadevnih sredstev. Evropska komisija je oceno opravila po predložitvi predloga 17. februarja 2022 in ga odobrila 4. maja.
Link do vira	https://dsa.cy/en/activities/nccc

Poleg skupine CCERT obstajajo tudi različne pobude, namenjene ozaveščanju o kibernetski varnosti in spodbujanju najboljših praks. Med njimi sta vsakoletni Ciprski izziv kibernetske varnosti, katerega namen je prepoznati in razviti najboljše talente na področju kibernetske varnosti v državi, ter ustanovitev ciprskega združenja za kibernetsko varnost, katerega cilj je spodbujati raziskave, izobraževanje in inovacije na področju kibernetske varnosti. DSA si prizadeva za večjo ozaveščenost o kibernetski varnosti in razvoj kibernetskih kompetenc na različnih poslovnih področjih. Organizira usposabljanja, delavnice in spletne seminarje ter ponuja informativne sestanke za študente, ki se zanimajo za študij kibernetske varnosti, mala in srednje velika podjetja ter starejše državljane. Ministrstvo za izobraževanje in kulturo izvaja tudi izobraževalne programe o kibernetski varnosti v šolah. Cilj teh programov je učencem zagotoviti potrebno znanje in spretnosti za zaščito na spletu ter povečati ozaveščenost o kibernetskih grožnjah.

Vendar pa je na Cipru še vedno veliko prostora za izboljšave na področju digitalne/kibernetske varnosti. Natančneje, več sredstev bi lahko namenili programom izobraževanja in usposabljanja na področju kibernetske varnosti, zlasti za mala in srednje velika podjetja, ki so lahko bolj izpostavljena kibernetskim napadom. Poleg tega bi lahko večje sodelovanje med vlado, akademskimi krogi in zasebnim sektorjem pripomoglo h krepitvi splošne kibernetske varnosti v državi.

6.5 Bolgarija

Bolgarija je z nacionalno strategijo kibernetske varnosti, zakonom o varstvu osebnih podatkov in direktivo o varnosti omrežij in informacij napredovala pri izboljšanju kibernetske varnosti. Državna agencija za elektronsko upravljanje usklajuje politike in zagotavlja usposabljanje. Bolgarski center CERT odkriva grožnje in se nanje odziva, kompetenčni center za kibernetsko varnost pa si prizadeva za spodbujanje strokovnega znanja. Med izzivi so pomanjkanje usposobljenih strokovnjakov, slaba ozaveščenost javnosti in nedavni kibernetski napadi.

POBUDA 1	
Ime	State e-Government Agency (SEGA)
Lokacija	National, public sector
Trajanje	2016 -
Opis	Državna agencija za e-upravo (SEGA) je odgovorna za politike elektronskega upravljanja in kibernetske varnosti v državi. Agencija se usklajuje z drugimi vladnimi organi in zagotavlja usposabljanje za

	kibernetsko varnost za zaposlene v javnem sektorju.
Rezultat/učinek	SAEG si prizadeva za izboljšanje kibernetske varnosti v državi s spodbujanjem varne elektronske komunikacije, izvajanjem ukrepov za informacijsko varnost in rednimi revizijami vladnih informacijskih sistemov.
Link do vira	https://www2.e-gov.bg/en/about_us

POBUDA 2	
Ime	National Cybersecurity Educational Program
Lokacija	National, srednje šole (od 7. Do)
Trajanje	2016 -
Opis	Ta program je namenjen učencem od 7. do 12. razreda in se osredotoča na ozaveščanje o tveganjih za kibernetsko varnost, spodbujanje varnega in odgovornega vedenja na spletu ter spodbujanje učencev k razmišljanju o poklicni poti na področju kibernetske varnosti. Program ima tri glavne dele: predavanja, vaje in tekmovanja. Cilj pobude je spodbujati kulturo ozaveščanja in izobraževanja o kibernetski varnosti v Bolgariji ter pomagati pri oblikovanju usposobljene delovne sile na področju kibernetske varnosti.
Rezultat/učinek	Program je pripomogel k povečanju zanimanja za izobraževanje in poklicno pot na področju kibernetske varnosti med mladimi v Bolgariji, hkrati pa je spodbudil nacionalne organizacije k oblikovanju partnerstev za krepitev zmogljivosti države na področju kibernetske varnosti. Pripeljal je tudi do nastanka nove generacije strokovnjakov za kibernetsko varnost, ki so opremljeni s potrebnim znanjem in veščinami za zaščito bolgarske digitalne infrastrukture.
Link do vira	https://ccdcoe.org/uploads/2018/10/Bulgaria_National-

	program-Digital-Bulgaria-2025_2019_original.pdf

PREDLOGI ZA VREDNOTENJE IN IZVAJANJE

Čeprav Bolgarija sprejema potrebne ukrepe za napredek na področju kibernetske varnosti, je vedno mogoče še kaj izboljšati. Nacionalni izobraževalni program za kibernetsko varnost bi lahko na primer razširili, da bi zajel širše občinstvo, vključno z odraslimi in podjetji. Kljub temu je dobro, da se usmeri na mlado občinstvo, saj bodo prav oni oblikovali prihodnost. To bi lahko izvajale tudi druge države. Poleg izobraževalnih pobud so v Bolgariji za zaščito pred kibernetskimi grožnjami potrebne tudi celovitejše politike in predpisi o kibernetski varnosti. To vključuje strožje zakone in predpise o varstvu podatkov ter izboljšane standarde kibernetske varnosti za kritično infrastrukturo.

6.6 Nemčija

Vprašanja, povezana z izobraževanjem na področju digitalne/kibernetske varnosti, so za Nemčijo prednostna naloga, da bi se lahko spoprijela z izzivi, ki jih prinašata nov razvoj na področju kibernetskega upravljanja in digitalnega prehoda. Natančneje, nemška vlada je v sodelovanju z zainteresiranimi stranmi v tem sektorju začela razvijati digitalno strategijo.

"Digitalna strategija 2025" opredeljuje prednostne naloge nemške vlade, in sicer razvoj digitalnih kompetenc in spodbujanje uporabe novih orodij za krepitev procesov digitalizacije v Nemčiji. Strategija temelji na desetih stebrih, pomembnih za digitalizacijo, vključno s stebrom, ki se osredotoča na uvajanje digitalnega izobraževanja v vseh fazah posameznikovega življenja.

Nemška digitalna strategija 2025 je bila sprejeta leta 2016 za obdobje 10 let. Cilj ukrepov strategije ni le omogočiti nemškemu gospodarstvu, da se spopade z novimi izzivi, temveč tudi zagotoviti vodilni položaj na področju kakovosti in tehnologije za prihodnja leta s kombiniranjem tradicionalnih konkurenčnih prednosti z novejšo tehnologijo, sodobnimi metodami in posebnimi podpornimi programi.

POBUDA 1	
Ime	Cyber Security Strategy for Germany
Lokacija	National
Datum	2021
Opis	Zvezni kabinet je 8. septembra 2021 sprejel strategijo kibernetske varnosti Nemčije za leto 2021, ki jo je pripravil zvezni minister za notranje zadeve in skupnost. V njej je določen okvir za kibernetsko

	varnost v naslednjih petih letih. Kibernetska varnost je naloga sedanjosti in ena od pomembnih nalog za prihodnost. To je obdobje, ki ga opredeljujejo nove priložnosti digitalnega sveta, kot so umetna inteligenca, povezane elektronske naprave in nova, inovativna komunikacijska sredstva. Da bi lahko te priložnosti izkoristili, je treba zmanjšati tveganja. Nemška strategija kibernetske varnosti 2021 nadomešča nemško strategijo kibernetske varnosti iz leta 2016. V strategiji je določena bistvena dolgoročna usmeritev politike kibernetske varnosti zvezne vlade, ki je razdeljena na vodilna načela, področja ukrepanja in strateške cilje. Strategija kibernetske varnosti se osredotoča na štiri področja delovanja: družba, zasebna industrija, vlada in EU/mednarodne zadeve. Na teh področjih ukrepanja je bilo določenih skupno 44 strateških ciljev.
Rezultat/učinek	Zvezni urad za informacijsko varnost bo postal središče za sodelovanje zveznih in državnih agencij pri preprečevanju kibernetskega kriminala, s čimer bo vzpostavljen tretji steber celovite zvezne arhitekture kibernetske varnosti: Zvezni urad za informacijsko varnost se bo pridružil Zveznemu kriminalističnemu uradu (BKA), ki to vlogo že opravlja v nemški policiji, in Zveznemu uradu za zaščito ustave, ki to počne v nemški obveščevalni skupnosti. Strategija krepi digitalno suverenost in s tem varno digitalno preobrazbo naše države. Nemško digitalno gospodarstvo se bo okrepilo z usmerjeno podporo ključnim omogočitvenim tehnologijam in povezovanjem z ustreznimi raziskovalci. Pri nastajajočih in ključnih omogočitvenih tehnologijah se bo od samega začetka uporabljal pristop "security-by-design".

POBUDA 2	
Ime	Cyber Security Research Centers

Lokacija	National
Datum	2011
Opis	Cilj financiranja raziskav je financiranje razvoja novih idej in tehnologij. Financirajo se projekti s širokega spektra raziskovalnih področij. Obsega vse od temeljnih raziskav na področju naravoslovja, okolju prijaznega trajnostnega razvoja, novih tehnologij, informacijskih in komunikacijskih tehnologij, znanosti o življenju, oblikovanja dela, financiranja strukturnih raziskav na visokošolskih ustanovah do podpore inovacijam in prenosa tehnologij. Zvezno ministrstvo za izobraževanje in raziskave (BMBF) financira tri Kompetenzzentren für IT-Sicherheitsforschung (raziskovalni centri za kibernetsko varnost). Posamezne izjemne univerze ali ne univerzitetne raziskovalne ustanove se financirajo kot raziskovalni centri za kibernetsko varnost. Centri se tematsko in organizacijsko osredotočajo na najpomembnejše izzive na področju informacijske varnosti.
Rezultat/učinek	Naloga teh centrov je razvijati dolgoročne strategije za kibernetsko varnost in izvajati s tem povezane raziskovalne projekte za soočanje s sedanjimi in prihodnjimi izzivi.

PREDLOGI ZA VREDNOTENJE IN IZVAJANJE

Nemčija si je močno prizadevala za izobraževanje svojih državljanov o digitalni varnosti, vendar je še veliko prostora za izboljšave. Čeprav so bile izvedene pobude, kot so kampanje za ozaveščanje javnosti, šolski programi in viri, ki jih financira vlada, so zaradi nenehnega razvoja digitalnih groženj potrebna nadaljnja prizadevanja.

Za izboljšanje ravni znanja državljanov o digitalni varnosti lahko Nemčija razmisli o naslednjih rešitvah:

- integrirane programe usposabljanja za javni in zasebni sektor
- Pobude javnega in zasebnega sektorja
- platforme za izmenjavo informacij
- kampanje za ozaveščanje

Druge države/institucije lahko za izvajanje podobnih pobud:

- prilagodijo obstoječe programe: preučijo uspešne pobude iz Nemčije in drugih držav ter jih prilagoditi in izvajajo v svojih izobraževalnih sistemih.
- Sodelujejo s strokovnjaki na tem področju: Sodelujejo z lokalnimi strokovnjaki iz industrije in strokovnjaki za kibernetsko varnost, da bi razvili ustrezne in praktične izobraževalne vsebine.
- Spodbujajo javno-zasebna partnerstva: Spodbujajo partnerstva med vladnimi agencijami, zasebnimi podjetji in neprofitnimi organizacijami.
- Prilagodijo komunikacijske kanale: Uporabijo kombinacijo komunikacijskih kanalov, da dosežejo široko občinstvo.
- Uporabijo različne komunikacijske kanale, da izkoristijo mešanico kanalov: Redno ocenjevanje učinkovitosti pobud za izobraževanje o digitalni varnosti.

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

7 Zaključek

Glavni cilj projekta DiscVET je bil opremiti učitelje in vodje usposabljanj v poklicnem izobraževanju in usposabljanju s potrebnimi kompetencami na področju digitalne suverenosti, da bi lahko učinkovito usposabljali druge in spodbujali varno digitalno okolje. S poudarkom na oblikovanju inovativnega gradiva za usposabljanje in interaktivnih simulacijskih vaj je bil cilj projekta izboljšati pripravljenost udeležencev na digitalno varnost. Vendar naša vizija presega ta neposredni cilj. Z opolnomočenjem učiteljev in trenerjev poklicnega izobraževanja in usposabljanja z znanjem in kompetencami, potrebnimi za digitalno suverenost, želimo prispevati k izobraževanju bolj ozaveščene ang visoko usposobljene generacije Evropejcev.

EU se zaveda pomena digitalnih spretnosti, varnih digitalnih okolij in možnosti vseživljenjskega učenja, zato je sprejela celovit pristop h kibernetski varnosti, digitalnemu izobraževanju ter financiranju raziskav in inovacij. Ta zavezanost je razvidna iz strategij, predpisov in pobud EU, katerih cilj je posameznike opremiti s potrebnimi digitalnimi spretnostmi in spodbujati varne digitalne prakse po vsej Evropi.

Da bi zagotovili učinkovitost in kakovost projekta DiscVET, cenimo povratne informacije in ocene udeležencev. S skrbno analizo in reševanjem vseh ugotovljenih težav si prizadevamo, da bi zagotovili končno in dokončno različico rezultatov projekta. Evalvacijsko poročilo nam bo služilo kot dragocen vir, ki nas bo usmerjal pri izboljševanju rezultatov projekta ter zagotavljanju visokega zadovoljstva in uporabnosti projekta med ciljno skupino.

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

8 Bibliografija

- UpGuard: Kibernetska varnost kritične digitalne infrastrukture

Pridobljeno iz: https://www.upguard.com/blog/cybersecurity-regulations-in-the-european-union#toc-3

- Evropska komisija: Digitalno učenje in IKT v izobraževanju

Pridobljeno na: https://digital-strategy.ec.europa.eu/en/policies/digital-learning

- Evropska komisija: Akcijski načrt za digitalno izobraževanje - ukrep 5

Pridobljeno na: https://education.ec.europa.eu/focus-topics/digital-education/action-plan/action-5

- Evropska komisija: Akcijski načrt za digitalno izobraževanje - ukrep 6

Pridobljeno na: https://education.ec.europa.eu/focus-topics/digital-education/action-plan/action-6

- Evropska komisija: Akcijski načrt za digitalno izobraževanje - ukrep 7

Pridobljeno na: https://education.ec.europa.eu/focus-topics/digital-education/action-plan/action-7

- Evropska komisija: Okvir DigComp

Pridobljeno na: https://joint-research-centre.ec.europa.eu/digcomp/digcomp-framework_en#ref-4-safety

- Christine Redecker: Evropski okvir za digitalne kompetence izobraževalcev: DigCompEdu

Pridobljeno na: https://publications.jrc.ec.europa.eu/repository/handle/JRC107466

- UpGuard: Predpisi o financiranju in raziskovanju (podpora raziskavam in inovacijam)

Pridobljeno na: https://www.upguard.com/blog/cybersecurity-regulations-in-the-european-union#toc-4

- Francesca Bernasconi: Digitalno izobraževanje v skladu z EU: uporabna orodja

Pridobljeno na: https://www.elearningnews.it/en/news-C-27/digital-education-according-to-the-eu-useful-tools-AR-1488/