Co-funded by the European Union

IVAIGO

KSKD

TeneLearning
Educational and training centre

ESAFETY WOMEN

e-SAFETY WOMEN VADOVAS

2024-1-LT02-KA210-YOU-000243179

Kortų žaidimas Nr. 1 – saugumo internete refleksijų žaidimas

(Susijęs su 14 priemonių rinkinio moduliais)



Finansuojama Europos Sąjungos lėšomis. Šis kūrinys atspindi tik autoriaus nuomonę, todėl Nacionalinė agentūra ir Europos Komisija negali būti laikomos atsakingomis už jame pateiktą informaciją.

Turinys

1. Įvadas.....3
1.1 Apie projektą.....4
2. Žaidimu pagrįstas mokymasis.....7
3. Žaidimo apžvalga.....8
4. Kortų tipai.....9
5. Kaip žaisti.....10
6. Mokymosi tikslai.....11
7. Refleksija ir siūlomi atsakymai (vadovo gidas).....12
8. 14 modulių santrauka.....20
9. Patarimai moderatoriui.....23
10. Pagrindinių skaitmeninės saugos terminų žodynas..24
11. Apibendrinimas.....26

Co-funded by the European Union

ESAFETY WOMEN

1. Įvadas

„Moterų saugumas internete“ kortų žaidimas – tai interaktyvi mokymosi veikla, skirta padėti jauniems žmonėms, ypač moterims, stiprinti savo skaitmeninį raštingumą ir saugumo internete įgūdžius.

Žaidimas skatina apmąstymus, empatiją ir diskusijas, pateikiant realias situacijas ir iššūkius internete.

Ši priemonė papildo „Moterų saugumas internete“ priemonių rinkinį ir gali būti naudojama seminaruose, klasėse ar tarpusavio mokymosi sesijose.



Co-funded by the European Union
IVAIGO
TeneLearning
Educational and training centre

1.1 Apie projektą

Projektas „eSAFETY WOMEN“ (2024-1-LT02-KA210-YOU-000243179) buvo sukurtas siekiant suteikti jauniems moterims iš socialiai remtinų šeimų įgūdžių ir žinių, reikalingų saugiai naršyti internete, atpažinti ir reaguoti į lytinį smurtą internete (OGBV) bei tapti informuotomis skaitmeninėmis pilietėmis.

Jo pagrindiniai tikslai yra:

- Suteikti jaunimui, ypač jaunoms moterims iš socialiai remtinų grupių, kritinio mąstymo ir žiniasklaidos raštingumo įgūdžių, kad jie galėtų saugiai naršyti ir dalyvauti internetinėje erdvėje.

- Stiprinti šių asmenų gebėjimus atpažinti, reaguoti į OGBV ir priekabiavimo internete atvejus bei atsigauti po jų.

Co-funded by the European Union

- Skatinti ir palengvinti aktyvų jaunimo dalyvavimą internetinėse diskusijose ir pilietinėje veikloje, stiprinant jų, kaip informuotų ir aktyvių skaitmeninių piliečių, vaidmenį.

- Sukurti ir platinti tokias priemones kaip e. saugumo priemonių rinkinys ir kortų žaidimas, skirtas šviesti jaunimą apie saugumą internete ir OGBV pasekmes.

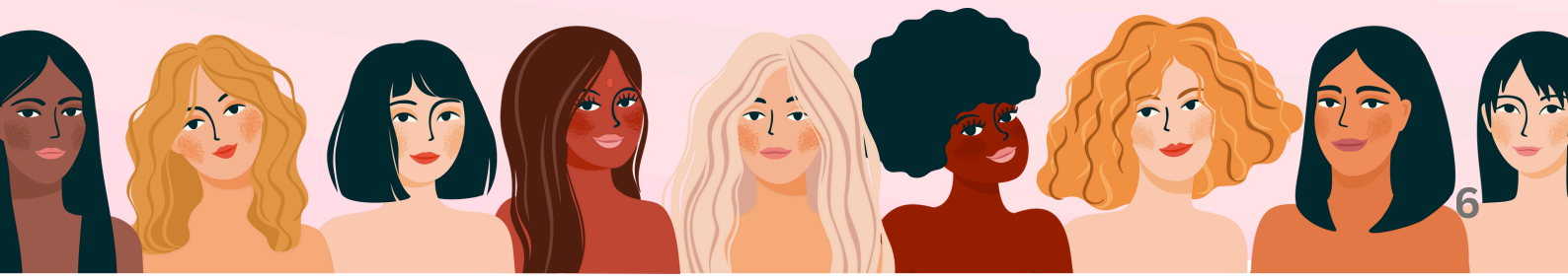
- Sukurti internetinę aplinką, kurioje visi asmenys, nepriklausomai nuo lyties ar kilmės, galėtų dalyvauti be baimės patirti priekabiavimą ar diskriminaciją.



Co-funded by the European Union
IVAIGO
TeneLearning
Educational and training centre

Šis žaidimas buvo sukurtas kaip priemonių rinkinio dalis, siekiant padaryti svarbiausias interneto saugumo sąvokas prieinamesnes ir įdomesnes. Naudodami žaidimų pagrįstą mokymosi formatą, įvairių socialinių sluoksnių dalyviai gali lengviau tyrinėti realaus gyvenimo skaitmeninius iššūkius, praktikuoti saugesnį elgesį ir stiprinti pasitikėjimą savimi internete.

Žaidimų naudojimas integracijai skatinti yra veiksmingas metodas: interaktyvūs ir bendradarbiavimu grindžiami formatai padeda įveikti barjerus, skatina dalyvių empatiją ir sudaro saugią aplinką apmąstymams ir tarpusavio mokymuisi. Šio projekto metu žaidimas tampa ne tik informacijos perteikimo priemone, bet ir įgalinimo bei socialinių pokyčių varikliu.



Co-funded by the European Union
IVAIGO
TeneLearning
Educational and training centre

2. Žaidimu pagrįstas mokymasis

Žaidimų pagrįstas mokymasis (GBL) yra įtraukusis ir dalyvaujamojo pobūdžio švietimo metodas, kuriuo naudojami žaidimai, sąveika ir žaidimas siekiant skatinti aktyvų mokymąsi.

Tai padeda besimokantiesiems įgyti žinių ir įgūdžių per patirtį, refleksiją ir bendradarbiavimą.

Šis požiūris atitinka „Erasmus+“ prioritetus, susijusius su įtrauktimi, skaitmenine transformacija ir neformaliu švietimu, nes skatina dalyvių, ypač moterų ir pažeidžiamų grupių, įsitraukimą ir empatiją.

„Moterų saugumas internete“ kortų žaidimas taiko GBL principus, sudėtingas internetinio saugumo temas paverčiant prieinamomis ir refleksyviomis mokymosi patirtimis.

Co-funded by the European Union

3. Žaidimo apžvalga

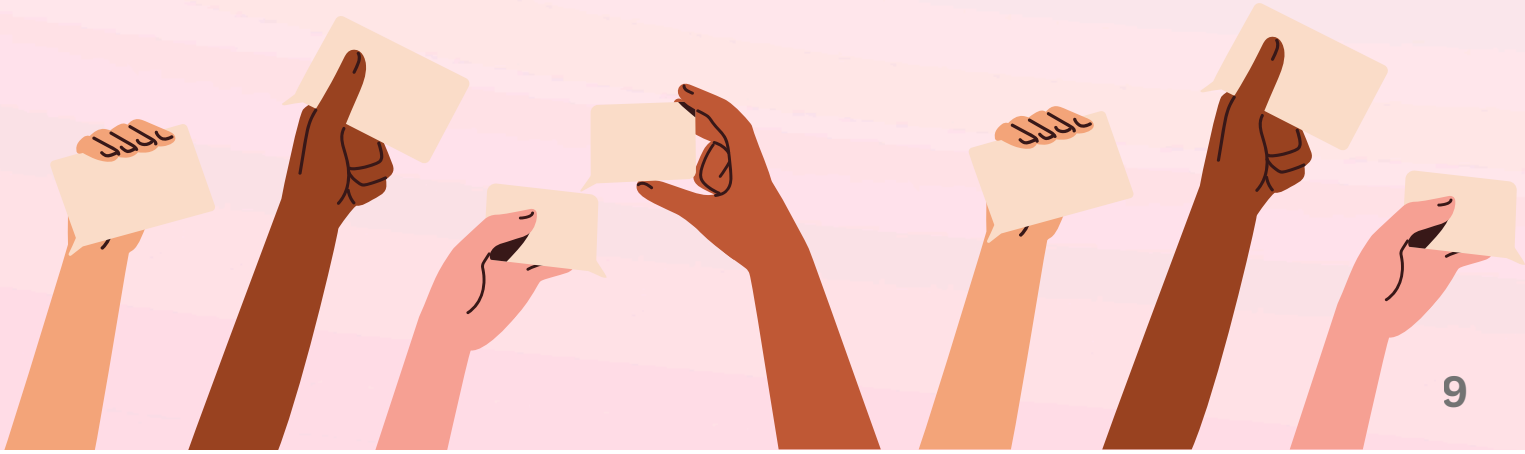
- **Žaidėjų skaičius:** 3–6 (arba žaidėjų grupės)
- **Trukmė:** 30–60 minučių
- **Tikslas:** išmokti atpažinti, aptarti ir reaguoti į saugumo internete riziką ir lyties pagrįstą skaitmeninį smurtą.
- **Reikiamos priemonės:**
  - Atspausdinta 42 kortų kaladė (14 modulių su 3 skirtingais kortų tipais)
  - Pasirinktinai: rezultatų lapas arba diskusijų laikmatis



Co-funded by the European Union
IVAIGO
TeneLearning
Educational and training centre

4. Kortų tipai

	Kortų tipas	Tikslas	Spalva	Pavyzdys
	**Klausimų kortelė**	Skatina žaidėjus kritiškai mąstyti ir aptarti galimus atsakymus.	Mėlyna	„Kas daro slaptažodį stiprų ir saugų?“
	**Situacijos kortelė**	Pateikia realistišką internetinį scenarijų ar riziką.	Oranžinė	„Jūs gaunate elektroninį laišką iš savo „banko“, kuriame prašoma patvirtinti savo duomenis.“
	**Veiksmo kortelė**	Siūlo veiksmą, reakciją arba saugų atsaką.	Žalia	„Nespauskite nuorodos – praneškite apie ją kaip apie sukčiavimą.“



Co-funded by the European Union

5. Kaip žaisti

Pasiruošimas žaidimui:

1. Sumaišykite visas 42 kortas arba padalinkite jas į tris krūvas (Klausimas/Situacija/Veiksmas).
2. Padėkite kortų kaladę (-es) atverstą (-as) į vidurį.
3. Pirmasis žaidėjas paima vieną kortą ir perskaito ją garsiai.

Žaidimo eiga:

- Jei tai **klausimo kortelė** → visi dalijasi savo nuomone ar patirtimi.
- Jei tai **situacijos kortelė** → grupė aptaria, ką darytų.
- Jei tai **veiksmo kortelė** → žaidėjas paaiškina, kodėl tas veiksmas yra saugiausias, ir pateikia pavyzdžių.

Pasirinktinai:

- Moderatorius skiria 1 tašką už apgalvotus ar kūrybingus atsakymus.
- Laimėtojas yra žaidėjas, surinkęs daugiausiai taškų, arba grupė baigia žaidimą bendru apmąstymu.

Žaidimo variantai:

- Naudokite tik situacijų ir veiksmų korteles greitiems „problemos–sprendimo“ raundams.
- Naudokite tik klausimų korteles komandų diskusijoms ar klasės apmąstymams.

Co-funded by the European Union

6. Mokymosi tikslai

Žaisdami šį žaidimą, dalyviai gebės:

- Atpažinti rizikingą elgesį internete ir skaitmeninį manipuliavimą.
- Išmokti reaguoti į priekabiavimą internete, kibernetinį priekabiavimą ir melagingas naujienas.
- Stiprinti pasitikėjimą savimi saugiai naršant internete.
- Apmąstyti empatiją, pagarbą ir sutikimą skaitmeninėje komunikacijoje.



Co-funded by the European Union
IVAIGO
TeneLearning
Educational and training centre

7. Refleksija ir siūlomi atsakymai (vadovo gidas)

Toliau pateikiamos trumpos refleksijos pastabos ir siūlomi atsakymai kiekvienam moduliui. Jos nėra išspausdintos kortelėse – moderatoriai gali jas perskaityti arba perfrazuoti po kiekvienos diskusijos.

1. Saugus įrenginio naudojimas

- **Klausimas:** naudokite unikalius slaptažodžius, sudarytus iš 12 ir daugiau simbolių, įskaitant raides, skaičius ir simbolius. Venkite jų pakartotinio naudojimo.
- **Situacija:** visada patikrinkite siuntėją ir niekada nespauskite įtartinų nuorodų.
- **Veiksmas:** sukčiavimo laiškai dažnai atrodo teisėti – patikrinkite siuntėjo adresą ir praneškite apie juos, kad padėtumėte apsaugoti kitus.

Co-funded by the European Union

2. Saugus prisijungimas

- **Klausimas:** viešasis Wi-Fi dažnai nėra šifruojamas, todėl hakeriai gali perimti jūsų duomenis.
- **Situacija:** visada naudokite VPN ir po to atsijunkite.
- **Veiksmas:** išjungus automatinius prisijungimus sumažėja sekimo rizika.

3. Buvimas socialinėje erdvėje

- **Klausimas:** venkite skelbti savo buvimo vietą, kontaktinius duomenis ar asmeninius įpročius.
- **Situacija:** internetinis priekabiavimas turėtų būti dokumentuojamas ir pranešamas.
- **Veiksmas:** blokuojant piktnaudžiautojus, užkertamas kelias pakartotiniams kontaktams ir apsaugoma jūsų gerovė.

Co-funded by the European Union
IVAIGO
TeneLearning
Educational and training centre

4. Internetinio gyvenimo administratorius

- **Klausimas:** netikros parduotuvės dažnai neturi saugių mokėjimo galimybių ar teisinės informacijos.
- **Situacija:** visada tikrinkite URL adresus, ar juose yra „https://“ ir įmonės duomenys.
- **Veiksmas:** niekada neįveskite banko duomenų per elektroniniu paštu ar žinutėmis siunčiamas nuorodas.

5. Pažintys ir santykiai

- **Klausimas:** sukčiai dažnai vengia vaizdo skambučių, pasakoja prieštaringas istorijas arba spaudžia siekdami intymumo.
- **Situacija:** nėra nieko blogo pasakyti „ne“ ir nutraukti bendravimą.
- **Veiksmas:** jei jaučiate spaudimą ar manipuliaciją, pasikalbėkite su kuo nors, kam pasitikite.

Co-funded by the European Union

6. Sudėtingų situacijų įveikimas

- **Klausimas:** jei jūsų turinys nutekėjo, praneškite apie tai platformai ir valdžios institucijoms.
- **Situacija:** grasinimai paskelbti asmeninį turinį yra šantažas – nedelsiant surinkite įrodymus.
- **Veiksmas:** niekada nereaguokite emociškai; kreipkitės profesionalios pagalbos arba kibernetinių nusikaltimų pagalbos.

7. Kibernetinis priekabiavimas

- **Klausimas:** remkite savo draugą, išklausydami jį, patvirtindami jo jausmus ir kartu pranešdami apie piktnaudžiavimą.
- **Situacija:** negalima ignoruoti patyčių – tylėjimas stiprina patyčių vykdytojus.
- **Veiksmas:** teigiama parama padeda aukoms jaustis mažiau izoliuotoms.

Co-funded by the European Union
IVAIGO
TeneLearning
Educational and training centre

8. Neapykanta internete

- **Klausimas:** tyla normalizuoja neapykantos kalbas. Išsilavinę atsakymai sukuria saugesnę aplinką.
- **Situacija:** praneškite ir atsakykite faktiniais, pagarbiais pranešimais.
- **Veiksmas:** skatinkite įtrauktį ir empatiją savo internetinėse bendruomenėse.

9. Skaitmeninis pėdsakas

- **Klausimas:** reguliariai ieškokite savęs „Google“ ir naudokite privatumo nustatymus.
- **Situacija:** susisiekite su tinklalapiais, kad būtų pašalinta nepageidaujama informacija.
- **Veiksmas:** valdykite tai, ką dalinatės – viskas, kas yra internete, palieka pėdsaką.

Co-funded by the European Union
IVAIGO
TeneLearning
Educational and training centre

10. Melagienos

- **Klausimas:** patikrinkite informaciją patikimais šaltiniais arba faktų tikrinimo svetainėmis.
- **Situacija:** venkite dalytis informacija prieš ją patikrinę.
- **Veiksmas:** mokykite bendraamžius apie patikimus informacijos šaltinius.

11. Catfishing

- **Klausimas:** intymus turinys, dalijamasi internete, gali būti netinkamai panaudotas ar paverstas ginklu.
- **Situacija:** niekada nesiųskite pinigų ir neatskleiskite asmeninių duomenų.
- **Veiksmas:** praneškite apie įtartinas sąskaitas ir nedelsdami jas užblokuokite.

Co-funded by the European Union
IVAIGO
TeneLearning
Educational and training centre

12. Erzinimas internete

- **Klausimas:** troliai siekia reakcijos – nereaguokite.
- **Situacija:** išjunkite komentarus arba blokuokite pažeidėjus.
- **Veiksmas:** išsaugokite ramybę; praneškite apie pakartotinius priekabiavimo atvejus.

13. Sutikimas dalintis nuotraukomis ir vaizdo įrašais

- **Klausimas:** kiekvienas žmogus turi teisę kontroliuoti savo įvaizdį internete.
- **Situacija:** visada paklauskite prieš dalindamiesi nuotraukomis, kuriose yra kitų žmonių.
- **Veiksmas:** gerbkite ribas – sutikimas yra skaitmeninės etikos dalis.

Co-funded by the European Union

14. Laiko socialiniuose tinkluose valdymas

- **Klausimas:** pernelyg dažnas vartojimas gali sukelti nerimą, sutrikusią koncentraciją ir sumažėjusią savigarbą.
- **Situacija:** nerimas be telefono yra ženklas, kad reikia pailsėti.
- **Veiksmas:** nustatykite laiką, kurį praleisite neprisijungę prie interneto, kad atkurtumėte psichinę pusiausvyrą.



Co-funded by the European Union
IVAIGO
KSKD
TeneLearning
Educational and training centre

8. 14 modulių santrauka

Modulis	Fokusas	Svarbiausi mokymosi aspektai
1. Saugus įrenginio naudojimas	Slaptažodžiai ir duomenų apsauga	Naudokite stiprius slaptažodžius, venkite sukčiavimo laiškų ir įtartinų nuorodų.
2. Saugus prisijungimas	Saugus tinklų naudojimas	Venkite naudoti viešąjį Wi-Fi be apsaugos; saugumo sumetimais naudokite VPN.
3. Buvimas socialinėje erdvėje	Atsakingas socialinių medijų naudojimas	Saugokite privatumą, venkite pernelyg atviro dalijimosi informacija ir elkitės pagarbiai su komentarais internete.
4. Internetinio gyvenimo administratorius	Internetinės parduotuvės ir informacijos saugumas	Prieš įvedant asmens ar mokėjimo duomenis, patikrinkite svetainės autentiškumą.
5. Pažintys ir santykiai	Pasitikėjimas ir saugumas internete	Atpažinkite apgaulingą elgesį ir žinokite, kada reikia nutraukti nesaugų bendravimą.
6. Sudėtingų situacijų įveikimas	Kova su skaitmeninėmis grėsmėmis	Išlikite ramūs, surinkite įrodymus ir kreipkitės pagalbos, jei susiduriate su šantažu ar priekabiavimu.

Co-funded by the European Union

7. Kibernetinis priekabiavimas	Pagarbus elgesys skaitmeninėje erdvėje	Remkite aukas, praneškite apie patyčias ir skatinkite teigiamą bendravimą internete.
8. Neapykanta internete	Kova su diskriminacija	Konstruktyviai reaguokite į neapykantos kalbas ir skatinkite empatiją internete.
9. Skaitmeninis pėdsakas	Sąmoningumas apie tapatybę internete	Reguliariai peržiūrėkite savo veiklą internete ir kontroliuokite bendrinamą informaciją.
10. Melagienos	Medijų raštingumas	Prieš dalindamiesi informacija, patikrinkite faktus ir remkitės patikimais informacijos šaltiniais.
11. Catfishing	Tapatybės vagystė internete	Niekada nesidalykite asmenine informacija ir nesiųskite pinigų nepažįstamiems žmonėms internete.
12. Erzinimas internete	Konfliktų valdymas internete	Nereaguokite į trolius; praneškite apie neigiamus vartotojus arba juos užblokuokite.
13. Sutikimas dalintis nuotraukomis ir vaizdo įrašais	Privatumas ir sutikimas	Prieš skelbdami ar dalydamiesi kitų asmenų nuotraukomis, visada paprašykite jų leidimo.
14. Laiko socialiniuose tinkluose valdymas	Sveiki skaitmeniniai įpročiai	Valdykite ekrano laiką ir darykite skaitmenines pertraukas, kad palaikytumėte psichinę gerovę.

Co-funded by the European Union

Toliau pateiktoje lentelėje apibendrinami pagrindiniai kiekvieno modulio akcentai ir svarbiausi mokymosi aspektai.

Tai padeda moderatoriams greitai suprasti, ko moko kiekvienas kortų rinkinys, ir užtikrina e-SAFETY WOMEN priemonių rinkinio ir kortų žaidimo suderinamumą.



Co-funded by the European Union
IVAIGO
TeneLearning
Educational and training centre

9. Patarimai moderatoriui

- Skatinkite empatiją – nėra „neteisingų“ atsakymų.
- Leiskite dalyviams paaiškinti savo mąstymą prieš pateikiant savo mintis.
- Naudokite realius pavyzdžius iš pačios grupės skaitmeninės patirties.
- Kiekvieną sesiją baikite viena bendra „auksine taisykle“ dėl saugumo internete.



Co-funded by the European Union
IVAIGO
TeneLearning
Educational and training centre

10. Pagrindinių skaitmeninės saugos terminų žodynas

Sąvoka	Apibūdinimas
Sukčiavimas	Internetinis sukčiavimo būdas, kai užpuolikai siunčia suklastotus elektroninius laiškus ar pranešimus, apsimetantys teisėtomis institucijomis, siekdami pavogti asmens duomenis, slaptažodžius ar kredito kortelių informaciją.
Virtualus privatus tinklas (VPN)	Saugus ryšys, kuris šifruoja interneto srautą ir apsaugo vartotojų privatumą, kai jie naudojasi viešaisiais arba nepatikimais tinklais.
Melagienos	Neteisinga arba klaidinanti informacija, pateikiama kaip naujienos, dažnai platinama socialinėje žiniasklaidoje siekiant manipuliuoti nuomonėmis ar emocijomis.
Catfishing	Suklastotos tapatybės internete sukūrimas siekiant apgauti ar manipuliuoti kitais, dažniausiai romantiškame kontekste.
Kibernetinis priekabiavimas	Skaitmeninių technologijų, pvz., socialinės žiniasklaidos, žinučių programėlių ar forumų, naudojimas siekiant priekabiauti, bauginti ar gėdyti kitus.

Co-funded by the European Union

Erzinimas internete (trolling)	Sąmoningas provokuojančių ar įžeidžiančių komentarų skelbimas internete, siekiant išprovokuoti reakcijas ar ginčus.
Skaitmeninis pėdsakas	Informacijos ir pėdsakų, kuriuos vartotojai palieka internete, pvz., įrašų, nuotraukų ir paskyros duomenų, rinkimas.
Neapykantos kalbos internete	Komunikacija, kuria naudojantis skaitmeninėmis platformomis puolama asmuo ar grupė dėl lyties, etninės priklausomybės, religijos ar kitų savybių.
Sutikimas	Leidimas, suteiktas laisvai ir aiškiai prieš dalijantis kieno nors asmeniniais duomenimis, nuotraukomis ar vaizdo įrašais internete.
Dviejų veiksnių autentifikavimas (2FA)	Papildoma saugumo priemonė, reikalaujanti dviejų patvirtinimo formų (pvz., slaptažodžio ir kodo), norint prisijungti prie paskyros.
Skaitmeninė gerovė	Subalansuotas ir sveikas skaitmeninių technologijų naudojimas, kuris palaiko psichinę, emocinę ir socialinę sveikatą.

Co-funded by the European Union

11. Apibendrinimas

Sukurta pagal projektą „e-SAFETY WOMEN“ (2024-1-LT02-KA210-YOU-000243179), finansuojamą pagal Europos Sąjungos programą „Erasmus+“.

Įgyvendinta Asociacija IVAIGO (Lietuva), TeneLearning S.L. (Ispanija) ir Kuşadası Sürdürülebilir Kalkınma Derneği (Turkija).



Co-funded by the European Union