GEMEINSAME LEHRPLANSTRUKTUR UND BEWERTUNGSRAHMEN

Standardisierte Aufschlüsselung der Lerneinheiten und technische Abstimmung mit DigComp für den Unterricht zum Thema „Digitale Sicherheit“ in der Oberstufe

Work Package 2. Activity 1.

Project Title	SONET Seniors Wellbeing and safety on the NET
Programme	Erasmus+ KA220-ADU
Grant Agreement	2025-1-PL01-KA220-ADU-000364406

Co-funded by the European Union

Version Number	1.0
Activity Number	WP2.A1_ EDUCATIONAL FRAMEWORK
Lead Partner	Karlsruhe Institute of Technology (KIT), Germany
Date	June.2026
Task	Task 2.1: Development of the Educational Framework, Skills Map, and Joint Curriculum
Document Type	Project Deliverable / Report
Summary	Als direkte Weiterentwicklung der umfassenden Grundlagenforschung und der länderübergreifenden Erkenntnisse aus der ersten Phase setzt dieser Bericht diese empirischen Erkenntnisse in die Praxis um, indem er die strukturelle Architektur und den Bewertungsrahmen für den gemeinsamen SONET-Lehrplan festlegt. Er wurde entwickelt, um die „Autonomie-Lücke“ bei Senioren zu schließen, und beschreibt einen standardisierten Arbeitsaufwand von 12 Stunden, der in vier Kernmodule à 3 Stunden unterteilt ist (Allgemeine Sicherheit, Cybersicherheit, Medienkompetenz und Technologien für umgebungsunterstütztes Wohnen). Jedes Modul integriert multimodale Ressourcen, interaktive Sandbox-Simulationsspiele und einen quantitativen Rahmen zur Selbsteinschätzung mit 15 Fragen. Schließlich ordnet das Rahmenwerk alle 10 angestrebten Lernergebnisse systematisch den offiziellen Standards des Europäischen Referenzrahmens für digitale Kompetenz der Bürger (DigComp) zu, um grenzüberschreitende Gültigkeit und institutionelle Übertragbarkeit innerhalb der EU zu gewährleisten.

Inhaltverzeichnis

Inhaltverzeichnis 2
1 ZUSAMMENFASSUNG 3
2 EINLEITUNG UND MAKROTRENDS 6
3 GEMEINSAMER LEHRPLAN, MODULSTRUKTUREN UND BEWERTUNGSRAHMEN 7
3.1 STUDIENGANGARCHITEKTUR UND PARAMETER FÜR DEN ARBEITSAUFWAND 7
3.2 Detaillierte Aufschlüsselung nach Einheiten und Themen 11
3.4 Übersichtstabelle zu den Zielen und Lernergebnissen des Moduls 17
3.5 Multimediale Lernkomponenten 18
3.6 Interavtive Lernspiele und Simulationen 18
3.7 Die Rolle der Projektpartner bei der Lehrplanentwicklung 19
3.8 Erwartete Auswirkungen des Rahmenwerks 19
4 TECHNICSHE ANPASSUNG AN DEN EUROPÄISCHEN DigComp-RAHMEN 20
4.1 Abgedeckte DigComp-Kompetenzbereiche 20
4.2 Systematische Zuordnung der SONET- Lernergebnisse zum DigComp-Standards 20
5 SCHLUSSFOLGERUNGEN 24
6 Literaturverzeichnis 25

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

1 ZUSAMMENFASSUNG

Aufbauend auf der umfassenden Grundlagenforschung und den länderübergreifenden Erkenntnissen, die im vorherigen Bericht vorgestellt wurden, setzt dieses Dokument diese empirischen Erkenntnisse in ein strukturiertes, auf Senioren zugeschnittenes Bildungsökosystem um. Während die europäischen Gesellschaften mit den parallelen Herausforderungen der vollständigen Digitalisierung von Dienstleistungen und der beschleunigten demografischen Alterung konfrontiert sind, hat die Grundlagenforschung eine gravierende „Autonomie-Lücke“ aufgezeigt, bei der der nahezu flächendeckende Besitz von Geräten bei älteren Menschen mit einer eingeschränkten Funktionsfähigkeit einhergeht. Um diese Lücke zu schließen, wandelt dieses Rahmenkonzept traditionelle IKT-Schulungen in einen unterstützenden, gemächlichen und stark auf Wiederholungen ausgerichteten Lernpfad um, der darauf ausgelegt ist, digitale Sicherheit und langfristige digitale Souveränität in ganz Europa zu fördern.

Dieses Ergebnis legt die strukturelle Architektur, die Aufteilung in einzelne Einheiten und die Bewertungskriterien des gemeinsamen SONET-Lehrplans fest. Das Schulungsprogramm gliedert sich in vier thematische Kernmodule, die jeweils von einem eigens dafür zuständigen Projektpartner entwickelt und geleitet werden:

Modul 1: Allgemeine Sicherheit (unter der Leitung von PARASOL) – Themen: Situationsbewusstsein, grundlegende Bedienung der Geräte und tägliche Maßnahmen zur Gefahrenabwehr.

Modul 2: Cybersicherheit (unter der Leitung von E-SENIORS) – Mit den Schwerpunkten Datenschutz, Passwortverwaltung und Erkennung von Phishing-Angriffen.

Modul 3: Medienkompetenz (unter der Leitung von BLSH) – Förderung des kritischen Denkens, Erkennen von Fake News und Bewertung von KI/Deepfakes.

Modul 4: Technologien für umgebungsgestütztes Wohnen (AAL) (unter der Leitung des KIT) – Vorstellung von Sicherheitssensoren für das Smart Home, tragbaren SOS-Systemen und Hilfsmitteln für ein selbstbestimmtes Altern zu Hause.

Der Lehrplan sieht ein standardisiertes, ausgewogenes Arbeitsaufwandsmodell von genau 3 Stunden pro Modul vor, das in einem 12-stündigen vollständigen Schulungsprogramm gipfelt. Um den unterschiedlichen Lernpräferenzen gerecht zu werden, umfasst jedes Modul 1,5 Stunden strukturiertes Lesen von Präsentationsmaterial (~40 Folien) mit umfangreichen Multimedia-Komponenten, darunter ein 20-minütiger Audio-Podcast eines Experten und ein 20-minütiges Videointerview mit einem Fachspezialisten. Die aktive Festigung der Fähigkeiten wird durch ein 30-minütiges interaktives Sandbox-Simulationsspiel verstärkt, das auf der seniorenfreundlichen SONET-E-Tool-Plattform gehostet wird.

Der Wissenserhalt und die Verhaltensanpassung werden anhand eines strengen quantitativen Selbstbewertungsrahmens bewertet. Jedes Modul umfasst genau 15 positiv formulierte Multiple-Choice-Fragen (5 Fragen pro Einheit), um sprachliche

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Verwirrung zu vermeiden. Dieser Fragenpool ist ausgewogen auf drei verschiedene Schwierigkeitsstufen verteilt: Grundwissen (40 %), anwendungsbezogene Fähigkeiten (40 %) und praktische, Szenario basierte Aufgaben (20 %). Dabei wird sofortiges, erklärendes Feedback gegeben, um sichere Online-Gewohnheiten zu festigen.

Um die institutionelle Gültigkeit und eine nahtlose grenzüberschreitende Übertragbarkeit innerhalb der Europäischen Union zu gewährleisten, werden alle 10 zentralen Lernergebnisse systematisch den offiziellen Standards des Europäischen Referenzrahmens für digitale Kompetenz der Bürger (DigComp) zugeordnet und tragen damit direkt zu den Bereichen 1 (Informationskompetenz), 2 (Kommunikation), 4 (Sicherheit) und 5 (Problemlösung) bei. Letztendlich liefert dieses Rahmenwerk einen skalierbaren, validierten Bildungsplan, der Erwachsenenbildner zu „Digitalpiloten“ macht, die in der Lage sind, technologiebezogene Ängste abzubauen und ein sicheres Altern zu Hause zu gewährleisten.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

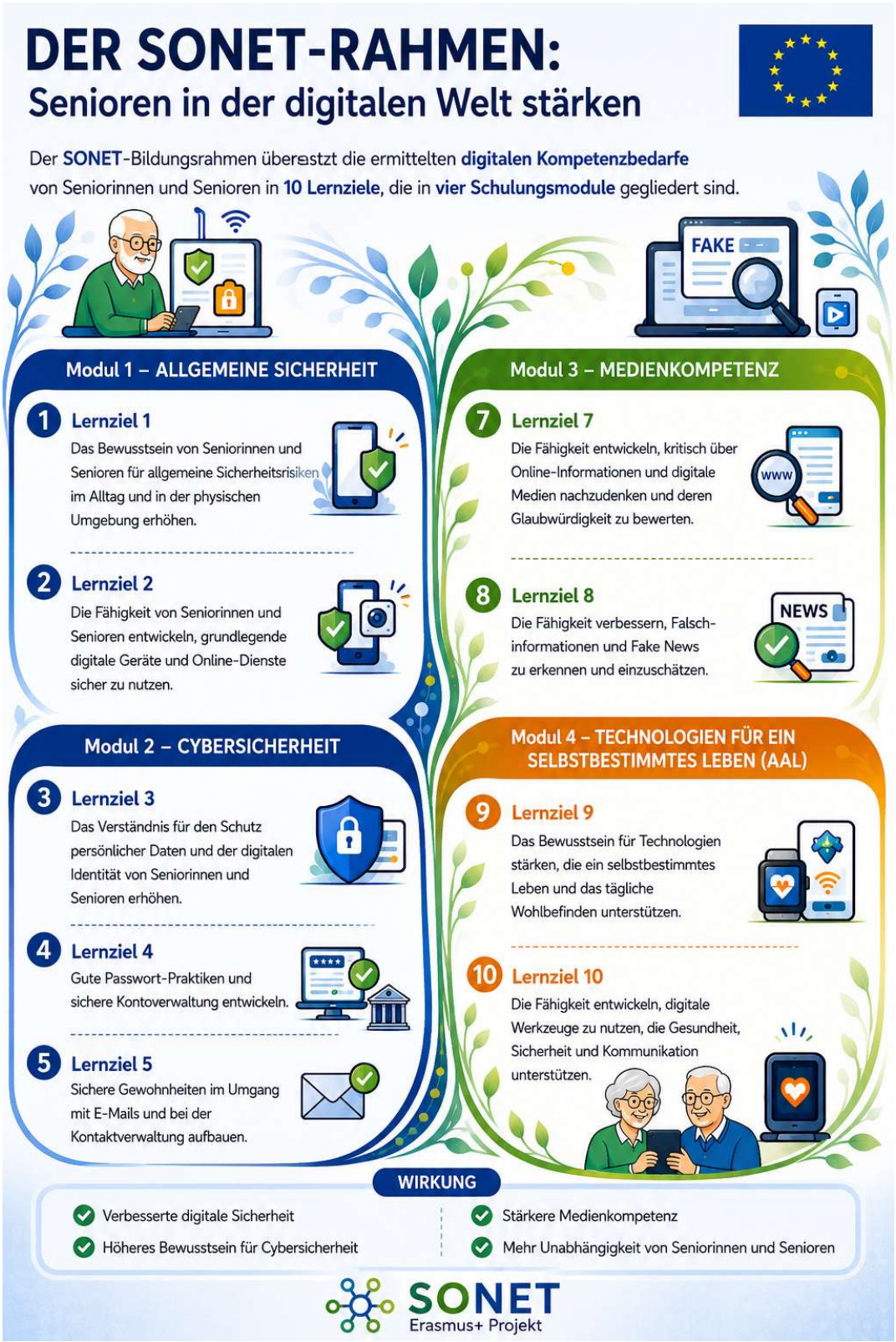

Abbildung 1: SONET-ARCHITEKTUR

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

2 EINLEITUNG UND MAKROTRENDS

In den fünf europäischen Partnerländern, die am Projekt SONET teilnehmen – darunter Polen, Spanien, Frankreich, Deutschland und Rumänien –, werden die Bereiche Erwachsenenbildung und digitale Inklusion derzeit durch zusammenwirkende Makrotrends neu geprägt. Dazu gehört die rasche demografische Alterung, die zunehmende Digitalisierung der öffentlichen Verwaltungen und die steigende Komplexität hybrider digitaler und physischer Sicherheitsrisiken. In allen fünf Ländern hat der Anteil der Bevölkerung im Alter von 65 Jahren und älter die kritische 20-Prozent-Schwelle entweder bereits überschritten oder nähert sich ihr rasch an.

Während nationale Strategien zur digitalen Transformation durchweg darauf abzielen, die soziale und gesellschaftliche Teilhabe zu fördern, sehen sich ältere Menschen gezwungen, sich in einem komplexen Umfeld zurechtzufinden, das von ausgeklügelten Cyber-Sicherheitsbedrohungen, allgegenwärtigem Finanzbetrug und tiefgreifender sozialer Isolation geprägt ist.

Die nationalen Rahmenbedingungen, institutionellen Strukturen und kulturellen Ökosysteme unterscheiden sich innerhalb des Konsortiums strukturell:

- Frankreich setzt vorrangig auf einen staatlich gelenkten, von Menschen vermittelten Ansatz über sein landesweites Netzwerk digitaler Berater, ergänzt durch strukturierte institutionelle Maßnahmen gegen den „Missbrauch von Schwäche.

- Deutschland meistert den digitalen Wandel mit einem ausgeprägten kulturellen Fokus auf den Datenschutz und stützt sich dabei in hohem Maße auf sein tief verwurzeltes Netzwerk sozialer Vereine.

- Spanien ist mit einer hohen Verbreitung mobiler Geräte, aber uneinheitlichen Funktionsmöglichkeiten konfrontiert und bekämpft die hohe Zahl an Cyberkriminalitätsfällen mit soliden institutionellen Rahmenbedingungen wie dem „Plan Mayor Seguridad.

- Polen nutzt stabile, generationenübergreifende Familienstrukturen, um digitale Kompetenzlücken zu schließen, und führt aktiv Kampagnen an der Basis sowie auf institutioneller Ebene durch, um weit verbreitete Social-Engineering-Betrugsmaschen zu bekämpfen.

- Rumänien steht vor erheblichen strukturellen Herausforderungen: Das Land hat mit einer historisch niedrigen Beteiligung Erwachsener am lebenslangen Lernen und einem ausgeprägten Gefälle zwischen Stadt und Land zu kämpfen und ist stark auf von Nichtregierungsorganisationen geleitete Maßnahmen angewiesen, um die sich überschneidenden Risiken im Zusammenhang mit digitalem Betrug und Sicherheit zu mindern.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

3 GEMEINSAMER LEHRPLAN, MODULSTRUKTUREN UND BEWERTUNGSRAHMEN

3.1 STUDIENGANGARCHITEKTUR UND PARAMETER FÜR DEN ARBEITSAUFWAND

Der gemeinsame SONET-Lehrplan ist systematisch in vier thematische Module gegliedert, die über eine interaktive Online-Plattform (E-Tool) zugänglich sind und durch Multimedia-Inhalte ergänzt werden. Um den unterschiedlichen Lernpräferenzen gerecht zu werden, umfasst jedes Modul strukturierte Präsentationen (ca. 40 Folien pro Modul), eine Audio-Podcast-Folge mit einem Experten, ein aufgezeichnetes Interview mit einem Fachmann aus der Praxis (z. B. einem Präventionsbeauftragten der Polizei oder einem Cybersicherheitsanalysten), Quizfragen zur Selbsteinschätzung sowie ein spezielles interaktives Simulationsspiel.

Der Lehrplan legt ein standardisiertes, ausgewogenes Arbeitsaufwandsmodell fest, um Flexibilität bei kurzen Schulungen, Workshop-Reihen oder Blended-Learning-Angeboten zu gewährleisten:

- Learning Content and Presentation Reading (1.5 hours per module)
- Podcasts anhören (20 Minuten pro Modul)
- Expert Interview Viewing (20 minutes per module)
- Interactive Educational Game Play (30 minutes per module)
- Self-Assessment and Reflection Quiz (20 minutes per module)
- This culminates in an estimated workload of **3 hours per module**, totalling approximately **12 hours for the full training program**.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Abbildung 3: Aufbau des SONET-Lehrplans und Rahmenkonzept zur Zuordnung von Kompetenzen für die digitale Bildung im höheren Bildungsbereich.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

MODUL	LERNFOKUS	LERNAKTIVITÄTEN	MULTIMEDIA-KOMPONENTEN	INTERAKTIVE KOMPONENTE	LERNZIELE	ARBEITSBELASTUNG
Modul 1: Allgemeine Sicherheit	Sicherheitsrisiken im digitalen Alltag verstehen.	Lehrvortrag, moderierte Diskussion, praktische Übungen.	Podcast mit einem Sicherheitsexperten, Interview mit einem Präventionsspezialisten der Polizei.	Interaktives Spiel zur Erkennung von Betrug und verdächtiger Kommunikation.	Die Lernenden erkennen Sicherheitsrisiken und gehen sicher mit digitalen Geräten um.	~3 Stunden
Modul 2: Cybersicherheit	Schutz personenbezogener Daten und der digitalen Identität.	Schritt-für-Schritt-Anleitungen, Übungen zum Thema Passwörter, Demonstrationen zur sicheren Anmeldung.	Podcast mit einem Spezialisten für Cybersicherheit, Experteninterview.	Simulationsspiel zur Erkennung von Phishing- und Betrugsversuchen.	Learners demonstrate safe digital behaviour and manage passwords securely	~3 Stunden
Modul 3: Medienkompetenz	Online-Informationen bewerten und Falschinformationen erkennen.	Fallstudien, Gruppendiskussionen, Analyse von Online-Inhalten.	Podcast zum Thema Falschinformationen und digitale Medien, Experteninterview.	Spiel zum Erkennen von verlässlichen und irreführenden Informationen.	Die Lernenden unterscheiden zwischen glaubwürdigen Quellen und unzuverläss	~3 Stunden

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

					igen Inhalten.	
Modul 4: AAL Technologien	Einsatz von Technologien, die ein selbstbestimmtes Leben ermöglichen.	Vorführungen von assistiven Technologien, praktische Übungen mit Geräten.	Podcast über digitale Gesundheitstechnologien, Experteninterview mit einem AAL-Spezialisten.	Simulation zur Erforschung von Smart-Home- und Hilfsgeräten.	Die Lernenden erkennen und nutzen Technologien, die die Sicherheit und das Wohlbefinden verbessern.	~3 Stunden

Tabelle 3 – Modulstruktur und Zuordnung der Aktivitäten

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

3.2 Detaillierte Aufschlüsselung nach Einheiten und Themen

MODUL 1: Allgemeine Sicherheit (Leitung: Partner: PARASOL)

Einleitung: Dieses Modul vermittelt Senioren Kenntnisse über alltägliche Sicherheitsrisiken sowohl in der physischen als auch in der digitalen Umgebung. Der Schwerpunkt liegt auf der Stärkung des Situationsbewusstseins und der Fähigkeiten zur persönlichen Sicherheit, damit Senioren selbstbewusst auf potenziell riskante Situationen, verdächtiges Verhalten und den Umgang mit Fremden reagieren können.

Lektion 1: Alltägliche Sicherheitsrisiken verstehen

Lektion 2: Sicherer Umgang mit digitalen Geräten

Lektion 3: Betrug und verdächtige Kommunikation erkennen

Lektion	BEHANDELTE THEMEN	UMFANG DER KERNINHALTE	INTERAKTIVES ELEMENT
Lektion 1	Häufige Sicherheitsrisiken für Senioren; Betrug an älteren Menschen; Verdächtige Situationen im Alltag; Situationsbewusstsein.	Erläuterung gängiger Betrugsmaschen; Beispiele aus der Praxis; Sicherheitschecklisten.	Diskussion eines Szenarios: Was würdest du in dieser Situation tun?
Lekzion 2	Grundlegende Gerätesicherheit; Sichere Nutzung von Smartphones und Tablets; Verbindung zu sicheren WLAN-Netzwerken herstellen; Vertrauenswürdige Websites erkennen.	Schritt-für-Schritt-Anleitungen für Geräte; Tipps für sicheres Surfen; Tipps für den sicheren Umgang mit Nachrichten.	Praktische Übungen mit Geräten

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Lektion 3	Telefonbetrug; Phishing-Nachrichten; betrügerische SMS und E-Mails; Taktiken zur emotionalen Manipulation.	Beispiele für verdächtige Kommunikation; Warnzeichen für Betrug; So reagieren Sie sicher.	Simulationsspiel: „Unbedenklich oder verdächtig?“

Tabelle 4.1 – Aufschlüsselung nach Lerneinheiten und Themen (Modul 1)

**Zusätzliche nicht-digitale Sicherheitsmaßnahmen: Behandelt die sichere Nutzung physischer Geldautomaten, die Navigation auf dem Weg zum Geldautomaten, Sicherheitsvorkehrungen vor der Haustür, Notfallkontakte sowie lokale Unterstützungsnetzwerke.)*

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

MODUL 2: Cybersicherheit (Leitung: Partner E-SENIORS)

Einleitung: Dieses Modul befasst sich mit dem Schutz personenbezogener Daten, der digitalen Identität und Online-Konten. Senioren lernen, wie sie Passwörter sicher verwalten, Phishing-Versuche erkennen und sich sicher in Online-Diensten bewegen können, um ihr Selbstvertrauen im Umgang mit diesen Diensten zu stärken.

Lektion 1: Personenbezogene Daten und digitale Identität

Lektion 2: Passwortsicherheit und Kontoschutz

Lektion 3: Sichere Nutzung von Online-Diensten

LEKTION	BEHANDELTE THEMEN	CORE CONTENT SCOPE	INTERACTIVES ELEMENT
Lektion 1	Was sind personenbezogene Daten? Risiken bei der Weitergabe personenbezogener Daten; Schutz der digitalen Identität.	Beispiele für sensible Daten; Datenschutzeinstellungen auf Online-Plattformen.	Übung: Welche Informationen sollten vertraulich bleiben?
Lektion 2	Erstellung sicherer Passwörter; Strategien zur Passwortverwaltung; Zwei-Faktor-Authentifizierung.	Beispiele für Passwörter; Sicherheitsmaßnahmen.	Workshop zur Passworterstellung
Lektion 3	Sicherheit beim Online-Banking; Sichere Identifizierung von Websites; Sichere Online-Transaktionen.	Sichere Websites erkennen (HTTPS); Verdächtige Links vermeiden.	Simulationsspiel: „Finde die Phishing-Nachricht.“

Tabelle 4.2 – Aufschlüsselung nach Lerneinheiten und Themen (Module 2)

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

MODUL 3: Medienkompetenz (unter der Leitung des Partners: BLSH)

Einleitung: Dieses Modul hilft Senioren dabei, kritisches Denken beim Umgang mit Online-Informationen zu entwickeln. Die Teilnehmer lernen, Quellen zu bewerten, Falschinformationen zu erkennen und zu verstehen, wie KI-generierte Inhalte und manipulierte Medien die öffentliche Wahrnehmung beeinflussen können.

Lektion 1: Online-Informationen verstehen

Lektion 2: Fehlinformationen und Fake News erkennen

Lektion 3: Von KI generierte Inhalte und Manipulation von Medien

Lektion	BEHANDELTE THEMEN	CORE CONTENT SCOPE	INTERACTIVES ELEMENT
Lektion 1	Wie sich Informationen im Internet verbreiten; Verschiedene Arten von Medienquellen; Glaubwürdige vs. unzuverlässige Informationen.	Beispiele für vertrauenswürdige Quellen; Einführung in Tools zur Faktenprüfung.	Übung zum Quelltextvergleich
Lektion 2	Merkmale von Fake News; Manipulierte Schlagzeilen und Bilder; Emotionale Manipulation in den Medien.	Beispiele für virale Falschinformationen; Verantwortungsbewusste Praktiken beim Teilen von Inhalten.	Spiel: „Finde die Fake News.“
Lektion 3	Durch KI generierte Bilder und Texte; Deepfakes; Erkennung manipulierter Medien.	Beispiele für KI-generierte Inhalte; So überprüfen Sie Informationen.	Übung: Echte Bilder vs. KI-generierte Bilder

Tabelle 4.3 – Aufschlüsselung nach Lerneinheiten und Themen (Module 3)

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

MODUL 4: Technologien für das umgebungsgestützte Wohnen (Leitung: Partner: KIT)

Einleitung: Dieses Modul führt Senioren in Technologien ein, die ein selbstbestimmtes Leben, die Gesundheitsüberwachung und die Sicherheit zu Hause unterstützen, und stärkt so ihr Vertrauen im Umgang mit assistiven Technologien zur Verbesserung ihrer Sicherheit und Selbstständigkeit.

Lektion 1: Einführung in assistive Technologien

Lektion 2: Sicherheitstechnologien für das Smart Home

Lektion 3: Digitale Hilfsmittel für Gesundheit und Kommunikation

Lektion	BEHANDELTE THEMEN	CORE CONTENT SCOPE	INTERACTIVES ELEMENT
Lektion 1	Was ist „Ambient Assisted Living“ (AAL)?; Vorteile von assistiven Technologien; Beispiele für Geräte zur Unterstützung älterer Menschen.	Überblick über Smart-Home-Technologien; Tools zur Gesundheitsüberwachung.	Diskussion: Wie kann Technologie den Alltag verbessern?
Lektion 2	Notfallwarnsysteme; Sturzmelder; Sicherheitssensoren für den Haushalt.	Beispiele für Smart-Home-Lösungen.	Fallstudie: Gestaltung einer sichereren Wohnumgebung
Lektion 3	Apps zur Gesundheitsüberwachung; Telemedizin-Dienste; Kommunikationstechnologien.	Nutzung von Apps zur Gesundheitsüberwachung; digitale Tools für die Kommunikation innerhalb der Familie.	Simulationsspiel: „Smart Home Safety Builder“.

Tabelle 4.4 – Detaillierte Aufschlüsselung nach Lerneinheiten und Themen (Module 4)

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

3.3 Rahmenkonzept für die Verteilung von Fragen zur Selbsteinschätzung

Um eine ausgewogene Abdeckung zu gewährleisten, legt das System strenge quantitative Anforderungen an die Gestaltung der Quizze fest: Jedes einzelne Modul muss genau 15 Multiple-Choice-Fragen enthalten, die gleichmäßig auf 5 Fragen pro Einheit verteilt sind, um sicherzustellen, dass alle Themen vollständig abgedeckt werden.

THEMATISCHER BLOCK	ZIELANZAHL DER FRAGEN
Lektion 1 (Konzeptionelles Verständnis)	5 Fragen
Einheit 2 (Umsetzung taktischer Fähigkeiten)	5 Fragen
Lektion 3 (Szenario zur Erkennung von Bedrohungen)	5 Fragen
Gesamtpunktzahl pro Modul	**15 Fragen**

Tabelle 5 – Rahmenkonzept für die Verteilung der Fragen zur Selbsteinschätzung

** Beispiel für die Formulierung einer Frage im standardisierten Rahmen:

Sie erhalten eine Nachricht, in der steht, dass Ihr Bankkonto gesperrt wurde, und in der Sie aufgefordert werden, auf einen Link zu klicken, um Ihre Daten zu bestätigen. Was sollten Sie tun?

Antwortmöglichkeiten: A. Klicken Sie sofort auf den Link

B. Wenden Sie sich über die offizielle Telefonnummer an die Bank

C. Antworten Sie bitte unter Angabe Ihrer Kontonummer

D. Leite die Nachricht an Freunde weiter.

Richtige Bezeichnung: B

Erläuterung zum System: Banken fordern keine persönlichen Daten über Nachrichten mit Links an. Wenden Sie sich stets über offizielle Kanäle an die Bank.

- Linguistic Restrictions:

  Fragen müssen einfach, praxisnah und direkt auf den Inhalt bezogen sein. Negative oder verwirrende Fragestellungen (z. B. „Welche dieser Optionen ist NICHT sicher?“) sind zu vermeiden; stattdessen sollten direkte, positive Formulierungen verwendet werden (z. B. „Welche Maßnahme ist die sicherste?“).

- Verteilung der Schwierigkeitsgrade::

  Die Fragen müssen einen angemessenen Schwierigkeitsgrad aufweisen und zum Nachdenken anregen, ohne dabei knifflig zu sein oder irreführende Formulierungen zu verwenden.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- Feedback-Mechanismus:
  Unmittelbar nachdem ein Lernender seine Antwort abgeschickt hat, muss die Plattform eine kurze Erklärung anzeigen, die das sichere Verhalten bekräftigt.

Die Fragen sind auf drei verschiedene Niveaus verteilt, um ein Gleichgewicht zwischen Verständnis und praktischer Anwendung herzustellen (siehe Tabelle 10).

ZIEL-SCHWIERIGKEITSGRAD	PROZENTUALE ZUWEISUNG
Leicht (Grundkenntnisse)	40%
Medium (Kontext der angewandten Fertigkeiten)	40%
Praktische, szenariobasierte Aufgaben	20%

Tabelle 6 – Verteilung der Schwierigkeitsgrade bei der Selbsteinschätzung

3.4 Übersichtstabelle zu den Zielen und Lernergebnissen des Moduls

Die folgende Tabelle gibt einen Überblick über die quantitative Gesamtverteilung der von der Partnerschaft entwickelten gezielten Bildungselemente innerhalb des umfassenden Rahmens.

THEMATISCHES KERNMODUL	LERNOBJEKTIVE	LEHRZIELE
Allgemeine Sicherheit (Modul 1)	3	3
Cybersicherheit (Modul 2)	3	3
Medienkompetenz (Modul 3)	2	2
Ambient Assisted Living (Modul 4)	2	2
Gesamtarchitektur des Frameworks	10	10

Tabelle 7 – Übersichtstabelle zu den strategischen Rahmengrößen

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

3.5 Multimediale Lernkomponenten

Jedes Modul umfasst vielfältige Lernformate, um unterschiedlichen Lernpräferenzen gerecht zu werden und das Engagement älterer Lernender zu fördern:

- Bildungsvorträge:
  Jede Partnerorganisation erstellt pro Modul etwa 40 Folien mit Lerninhalten, in denen die wichtigsten Kompetenzkonzepte klar, verständlich und strukturiert dargestellt werden.

- Podcasts:
  Jedes Modul umfasst eine Podcast-Folge, in der Experten auf diesem Gebiet hochaktuelle Themen wie Bedrohungen der Cybersicherheit, digitale Sicherheit oder assistive Technologien zur Unterstützung auditiver Lerner erörtern.

- Experteninterviews:
  Jedes Modul enthält ein aufgezeichnetes Videointerview mit einem Fachmann (z. B. Experten für Cybersicherheit, Präventionsspezialisten der Polizei, Fachleute für digitale Inklusion oder Spezialisten für Gesundheitstechnologie), um praktische Einblicke und Beispiele aus der Praxis zu vermitteln.

3.6 Interavtive Lernspiele und Simulationen

Um das Engagement der Nutzer zu steigern und den Erwerb praktischer Fähigkeiten zu fördern, enthält jedes Modul ein interaktives Lernspiel, das reale digitale Situationen simuliert und es Senioren ermöglicht, strategische Entscheidungsfindung und Problemlösung in einer sicheren Testumgebung zu üben:

- Modul „Allgemeine Sicherheit“:
  Ein Simulationsspiel, bei dem die Lernenden potenzielle Sicherheitsrisiken und Anzeichen für Betrug in alltäglichen Situationen erkennen.

- Modul „Cybersicherheit“:
  Ein interaktives Szenario, in dem die Lernenden Phishing-E-Mails, verdächtige Links und komplexe Versuche des Identitätsbetrugs erkennen müssen.

- Modul „Medienkompetenz“:
  Eine spielerische Aktivität, bei der die Lernenden aufgefordert werden, aktiv zwischen glaubwürdigen Quellen und irreführenden Falschinformationen im Internet zu unterscheiden.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- Modul „Ambient Assisted Living“:
  Eine digitale Simulation, die zeigt, wie assistive Technologien in der Praxis eingesetzt werden können, um die Sicherheit und Selbstständigkeit zu Hause zu verbessern. SONET E-Tool Platform Specifications

Alle fertiggestellten Bildungsressourcen, Medienkanäle und Lernergebnisse sind strukturell in das offizielle SONET E-Tool integriert. Diese interaktive digitale Plattform wurde sorgfältig so konzipiert, dass sie die Richtlinien für eine seniorenfreundliche Barrierefreiheit im Internet erfüllt. Das Portal umfasst alle Lernmodule, Multimedia-Präsentationen, Experten-Podcasts, Videointerviews, simulierte Lernszenarien, Referenzblätter zum Herunterladen sowie interaktive Quizze zur Selbsteinschätzung. Das E-Tool bietet eine intuitive, barrierearme Lernumgebung, in der Senioren selbstständig oder unter persönlicher Anleitung von Erwachsenenbildnern auf die Ressourcen zugreifen können.

3.7 Die Rolle der Projektpartner bei der Lehrplanentwicklung

Der gemeinsame Lehrplan wird im Rahmen einer stark kooperativen Matrix entwickelt, in der jeder Projektpartner die strukturelle Verantwortung für bestimmte Kernkomponenten übernimmt.:

- Modul 1 (Allgemeine Sicherheit): Entwickelt und geleitet von PARASOL.
- Modul 2 (Cybersicherheit): Entwickelt und geleitet von E-SENIORS.
- Modul 3 (Medienkompetenz): Entwickelt und geleitet von BLSH.
- Modul 4 (Ambient Assisted Living (AAL): Entwickelt und geleitet vom KIT.

Alle Partner leisten einen aktiven Beitrag, indem sie Standard-Lehrtexte entwickeln, lokalisierte Multimedia-Materialien, Selbsttests, Podcasts und Interviews erstellen, an Vorlagen für interaktive Spielszenarien mitwirken und an konsortialübergreifenden Validierungsprüfungen teilnehmen. Um uneingeschränkte lokale Zugänglichkeit und Chancengleichheit zu gewährleisten, werden alle endgültigen Materialien in die Sprachen der Partner übersetzt.

3.8 Erwartete Auswirkungen des Rahmenwerks

Die gemeinsame pädagogische Methodik und der gemeinsame Lehrplan zielen darauf ab, europaweit die folgenden langfristigen strategischen Ergebnisse zu erzielen:

- Das digitale Selbstvertrauen, die Selbstwirksamkeit und die funktionale Selbstständigkeit älterer Menschen stärken.
- Das Bewusstsein für Cybersicherheit und die täglichen Gewohnheiten im Bereich Datenschutz stärken.
- Eine sichere und eigenständige Teilhabe am gesellschaftlichen Leben in der digitalen Gesellschaft fördern.

Förderung eines aktiven und gesunden Alterns in der gewohnten Umgebung durch den Einsatz von assistiven Technologien.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

4 TECHNICSHE ANPASSUNG AN DEN EUROPÄISCHEN DigComp-RAHMEN

4.1 Abgedeckte DigComp-Kompetenzbereiche

Um die institutionelle Gültigkeit zu gewährleisten und die grenzüberschreitende Übertragbarkeit innerhalb der Europäischen Union zu erleichtern, leistet das SONET-Rahmenwerk einen direkten Beitrag zu vier Kernkompetenzbereichen, die im etablierten Europäischen Referenzrahmen für digitale Kompetenzen der Bürger (DigComp) definiert sind:

DigComp-Bereich	Schwerpunkt im Projekt SONET
Bereich 1 – Informations- und Datenkompetenz	Online-Informationen bewerten, Gerüchte nachverfolgen und die Quellen von Inhalten überprüfen.
Bereich 2 – Kommunikation und Zusammenarbeit	Einsatz digitaler Kommunikationsmittel zur Unterstützung von Familien und zur Vernetzung in der Pflege.
Bereich 4 – Sicherheit	Umsetzung von Cybersicherheit, Betrugsbekämpfung und Schutz personenbezogener Daten.
Bereich 5 – Problemlösung	Einsatz von assistiven Technologien zur Förderung des persönlichen Wohlbefindens und eines selbstbestimmten Lebens.

Tabelle 8 – SONET-Schwerpunkte in den verschiedenen DigComp-Kompetenzbereichen

4.2 Systematische Zuordnung der SONET- Lernergebnisse zum DigComp-Standards

Um die institutionelle Gültigkeit zu gewährleisten und die grenzüberschreitende Übertragbarkeit innerhalb der Europäischen Union zu erleichtern, sind die 10 SONET-Lernergebnisse strukturell an den etablierten Europäischen Referenzrahmen für digitale Kompetenz der Bürger (DigComp) ausgerichtet.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

MODUL	GEZIELTE LERNOBJEKTIVE	MESSBARE LERNERGEBNISSE	DIGCOMP BEREICH	SPEZIFISCHES DIGCOMP-MAPPING
Allgemeine Sicherheit	Das Bewusstsein für allgemeine Sicherheitsrisiken schärfen.	Erkennen Sie häufige Sicherheitsrisiken im digitalen Alltag und im realen Leben.	Bereich 4: Sicherheit	4.1 Schutz von Geräten und personenbezogenen Daten.
Allgemeine Sicherheit	Sicherer Umgang mit digitalen Geräten und alltäglichen Technologien.	Einfache digitale Geräte sicher bedienen und eine Verbindung zu Internetdiensten herstellen.	Bereich 1: Lese- und Schreibkompetenz	1.1 Durchsuchen, Suchen und Navigieren in Daten, Informationen und Inhalten.
Allgemeine Sicherheit	Die Fähigkeit verbessern, betrügerische Kommunikation zu erkennen.	Erkennen Sie Warnzeichen für Online-Betrug, Phishing und Spoofing-Versuche.	Bereich 4: Sicherheit	4.2 Schutz personenbezogener Daten und der Privatsphäre.
Cybersicherheit	Das Verständnis für den Schutz personenbezogener Daten verbessern.	Erläutern Sie die Grundprinzipien des Datenschutzes im Internet und identifizieren Sie sensible Daten.	Bereich 4: Sicherheit	4.2 Umgang mit personenbezogenen Daten und Datenschutz.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Cybersicherheit	Entwickeln Sie sichere Gewohnheiten beim Umgang mit Passwörtern und Konten.	Erstellen Sie selbst sichere Passwörter und befolgen Sie die üblichen Sicherheitsmaßnahmen.	Bereich 4: Sicherheit	4.1 Schutzvorrichtungen.
Cybersicherheit	Die sichere Nutzung von Online-Dienstleistungsplattformen verbessern.	Zeigen Sie, wie man sich sicher bei wichtigen Websites anmeldet und diese sicher nutzt.	Bereich 4: Sicherheit	4.1 Schutz von Geräten und der digitalen Identität.
Medienkompetenz	Entwickeln Sie kritisches Denken im Umgang mit Online-Informationen.	Unterscheide anhand von Anhaltspunkten zwischen zuverlässigen und unzuverlässigen Quellen.	Bereich 1: Lese- und Schreibkompetenz	1.2 Bewertung von Daten, Informationen und digitalen Inhalten.
Medienkompetenz	Die Fähigkeit verbessern, Fake News und Gerüchte zu erkennen.	Nennen Sie konkrete Beispiele für Fake News und erklären Sie, warum diese irreführend sind.	Bereich 1: Lese- und Schreibkompetenz	1.2 Bewertung der Glaubwürdigkeit von Informationen.
AAL Technologies	Das Bewusstsein für assistive Smart-Technologien stärken.	Ermitteln Sie konkrete Hilfsmittel, die ein sicheres, selbstbestimmtes Leben ermöglichen.	Bereich 5: Problemlösung	5.2 Ermittlung digitaler Anforderungen und technologis

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

				cher Lösungen.
AAL Technologies	Die operative Nutzung von assistiver Technologie ausbauen.	Die grundlegende Anwendung eines AAL-Tools erfolgreich demonstrieren.	Bereich 2: Kommunikation	2.1 Interaktion mithilfe digitaler Technologien.

Tabelle 9 – Systematische Zuordnung der SONET-Lernergebnisse zu den DigComp-Standards

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

5 SCHLUSSFOLGERUNGEN

Die im Rahmen von Arbeitspaket 2 entwickelte gemeinsame pädagogische Methodik und der gemeinsame Lehrplan zielen darauf ab, in den teilnehmenden europäischen Partnerregionen die folgenden Ergebnisse auf Makroebene zu erzielen:

- Das digitale Selbstvertrauen und die Selbstständigkeit älterer Menschen stärken::
  Aktiver Abbau von technikbezogenen Ängsten und Hemmschwellen durch unterstützende geragogische Lernkonzepte und positive Bestätigung.

- Verbesserung der Gewohnheiten im Bereich Cybersicherheit und Datenschutz:
  Älteren Lernenden sollen umsetzbare, dauerhaft sichere Verhaltensweisen vermittelt werden, damit sie Phishing-Versuche erfolgreich erkennen, psychologischen Drangmanövern widerstehen und ihre Passwörter sicher verwalten können.

- Örderung einer sicheren Teilhabe am gesellschaftlichen und sozialen Leben:
  Senioren in die Lage versetzen, selbstständig mit digitalen staatlichen Registern, Online-Verwaltungsplattformen (wie Cl@ve, BundID, France Connect), Gesundheitssystemen und Kommunikationskanälen innerhalb der Familie zu interagieren.

- Förderung eines aktiven und gesunden Alterns:
  Optimierung der physischen Sicherheit zu Hause und der langfristigen Selbstständigkeit durch die Integration von assistiven Technologien (Lösungen für das umgebungsunterstützte Wohnen, tragbare SOS-Notfallalarme, intelligente Sensoren) in den Alltag.

Durch die Kombination einer gemeindebasierten Bereitstellungsinfrastruktur (öffentliche Bibliotheken, Seniorenverbände, Vereine) mit einer Peer-to-Peer-Vermittlung von Freiwilligen und multimodalen, interaktiven E-Tool-Plattformen bietet das SONET-Rahmenkonzept ein umfassendes, nachhaltiges und in hohem Maße übertragbares Bildungsmodell für die digitale Teilhabe älterer Menschen in ganz Europa.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

6 Literaturverzeichnis

1. Główny Urząd Statystyczny (GUS), Społeczeństwo informacyjne w Polsce w 2025 r., Warsaw, Poland, 2026.
2. Council of Ministers of the Republic of Poland, Programme for the Development of Digital Competences, 2023.
3. Supreme Audit Office (NIK), Digital Exclusion - Audit Report, Warsaw, Poland, 2025.
4. Instituto Nacional de Estadística (INE), Encuesta sobre Equipamiento y Uso de TIC en los Hogares 2025, Madrid, Spain, 2025.
5. R. Tirado-Morueta et al., "Digital inclusion of older people in Spain: Technological support services for seniors as predictor," Ageing & Society, 2023.
6. E. M. García-Jáñez, "Design and development of services in public libraries for digital inclusion of older adults," Revista General de Información y Documentación, 2024.
7. Agence Nationale de la Cohésion des Territoires (ANCT), France Numérique Ensemble (2023–2027): Stratégie nationale pour l'inclusion numérique, Paris, France, 2023.
8. INSEE and Ministère de l'Intérieur, Sécurité et société, Paris, France, 2021.
9. Statistisches Bundesamt (Destatis), "Bevölkerung im Wandel: 15. koordinierte Bevölkerungsvorausberechnung," Wiesbaden, Germany, 2023.
10. Initiative D21 e.V., "D21-Digital-Index 2024/2025: Annual Status of the Digital Society," Berlin, Germany, 2025.
11. N. Döring and S. Hellwig, "Geragogik und digitale Medien: Anforderungen an eine altersgerechte Didaktik," Zeitschrift für Weiterbildungsforschung, vol. 47, no. 1, pp. 45-62, 2023.
12. OECD, Reviews of Labour Market and Social Policies: Romania 2025, Paris: OECD Publishing, 2025.
13. Reveal Marketing Research, 61% of Romanians in urban area have been the target of online fraud attempts, Bucharest, Romania, 2025.
14. European Union Agency for Fundamental Rights, Ageing in digital societies: enablers and barriers to access digital services for older persons, June 2022.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Consortium

FUNDACJA PARASOL

Acufade

Eseniors

KIT Karlsruher Institut für Technologie

BRIDGE EDUCATION

Co-funded by
the European Union