LINKS

Co-funded by the European Union

# Digitaalse suveräänsuse pädevuste raamistik

Co-funded by
the European Union

Seda projekti toetab Euroopa Komisjon Erasmus+ programmi kaudu. See väljaanne kajastab ainult autori seisukohti ja komisjon ei vastuta selles sisalduva teabe võimaliku kasutamise eest.

Read more about

LINKS

# Sisu

# Sissejuhatus

Projekti LINKS eesmärk on toetada Euroopa noorsootöötajaid oma andmete suveräänsuse saavutamisel ja digitaalse turvalisuse oskuste täiustamisel läbi uue, innovaatilise digipädevuse suurendamist toetava koolitussisu vormi.

Selle projekti ja taotluse esialgsetes planeerimisfaasides kinnitas vajaduste analüüs tõsiasja, et praegu puudub Euroopa jaoks ühtne digitaalse suveräänsuse ja turvalisuse kompetentsiraamistik.

DigComp (Digital Competence Framework) viitab paljudele üldistele ja üldistele põhioskustele ja -pädevustele, mis on seotud digitaalse turvalisusega tervikuna ning see väljund viitab sellele olemasolevale pädevusraamistikule, kuid on konkreetselt suunatud noorsootöötajate proaktiivsele teadlikkusele kogu Euroopas. digitaalse turvalisuse ohud.

Digitaalse suveräänsuse pädevuste raamistik määratleb pädevuste põhikomponendid, mida noorsootöötajad vajavad digitaalse suveräänsuse ja turbeprotokollide tõhusaks integreerimiseks nende lokaalsesse konteksti, samuti ELi võrdlusraamistiku loomiseks ja kinnitamiseks digitaalse turvalisuse pädevuste arendamiseks ja hindamiseks. Digitaalse turvalisuse pädevused on tugevalt seotud üldiste digipädevustega ja neid ei peeta omaette pädevusteks.

Raamistik on suunatud noorsootöötajatele, kuid on asjakohane ja huvipakkuv ka eel-/täiendus- IKT õpetajatele ja koolitajatele ning haridus- ja elukestva õppe poliitikakujundajatele seoses üksikisikute tehnoloogiliste oskuste ja suutlikkuse suurendamisega. .

Eeldame, et digikoolituse valitsusvälised organisatsioonid ja koolitusorganisatsioonid üle Euroopa võtavad selle raamistiku oma haridusliku hindamise ja õpetamistegevuse osana kasutusele, mis pikemas perspektiivis suurendab teadlikkust ja julgustab raamistiku integreerimist kohalikesse, piirkondlikesse ja riiklikesse digiharidusasutustesse Euroopa riikides.

# Projekti küsitluse ja fookusgruppide tulemused

Digitaalse suveräänsuse pädevuse raamistik põhineb projekti uuringu ja fookusrühmade metoodikal ja järeldustel. Samuti loob see ühtlustada end DigCompi raamistikuga, mis toetab pikaajalist kasutamist ja jätkusuutlikkust täiendava sihtrühmapõhise pädevusraamistikuna.

Projekti uuring aitas õppida tundma tehnoloogia ja andmekaitse kasutamist noorsootöötajate digitöö praktikates. Noorsootöötajad vajavad suuremat teadlikkust koos digitaalse identiteedi hea haldamisega, see võib aidata piirata kasutaja või organisatsiooni enda "tähelepanematusest" põhjustatud sündmusi. Nad kirjutasid vajadusest seadistada ja edastada kaugtöö turvapoliitikat, reguleerida isiklike seadmete kasutamist, kindlustada side- ja koostöökanalid ning pakkuda valvsat IT-tuge. Nad soovitasid teha kursused kättesaadavaks suuremale hulgale töötajatele ja noortele, kasutada konkreetsete ülesannete kohta asjakohasemaid näiteid, parandada võrgustike loomist ning jagada häid ja halbu kogemusi veebis. Oluline on pidevalt ajakohastada ja eriti uute ELi dokumentidega.

Suurem osa noorsootöötajatest ei ole saanud sihipärast koolitust, nad teevad veebiturvalisuse osas valikuid enda teadmiste põhjal. Nad kirjutasid, et organisatsioonide ja erakasutajate turvalisuse huvides on vaja neid aspekte süvendada ning korraldada andmekaitseametnikele erikoolitused.

# Vajadus digitaalse suveräänsuse pädevuste raamistiku järele

Kasvab mure, et kodanikud, ettevõtted ja Euroopa Liidu liikmesriigid kaotavad järk-järgult kontrolli oma andmete üle, innovatsioonivõimet ning võimet kujundada ja jõustada õigusakte digitaalses keskkonnas. Selle taustal on kasvanud toetus uuele poliitilisele lähenemisviisile, mille eesmärk on suurendada Euroopa strateegilist autonoomiat digitaalvaldkonnas.

Tehnoloogiaettevõtted koguvad tohutul hulgal isikuandmeid ja ELis on kasvanud mure selle pärast, kuidas Euroopa kodanikud saavad taastada kontrolli oma digitaalsete andmete üle võrgukeskkonnas, kus praegu domineerivad peamiselt ELi-välised tehnoloogiaettevõtted.

Kuna noorsootöö kohaneb üha enam digimaailmaga, siis näeme, et ka noorsootöötajad võtavad omaks uusi lähenemisi. Kuigi digi on uus ja põnev, pakkudes lugematuid võimalusi, nõuab see siiski paremat arusaamist noorsootöö kontekstis. Olemasolevate digitaalse noorsootöö tavade, platvormide, tööriistade ja õpperaamistike kaardistamiseks digitaalse suveräänsuse pädevuste osas on vaja rohkem meetmeid.

Digitaalne suveräänsus on digiajastul uus mõiste, mida tavaliselt mõistetakse kui ‚inimeste võimet omada oma isiklikke andmeid ja kontrollida nende kasutamist".

COVID-19 pandeemial on olnud tohutu mõju enamiku inimeste igapäevaelule. Vastuseks on tehnoloogiat kohandatud, et proovida ja leevendada neid mõjusid, pakkudes inimestele digitaalseid alternatiive paljudele igapäevastele tegevustele, mida ei saa enam normaalselt sooritada. Virtuaalne suhtlemine ja veebiüritused on muutunud igapäevaseks ning on aidanud hoida inimesi lukustuses olles täielikult isolatsioonist.

Veebiõpe on paljudes kohtades muutunud ka uueks normaalsuseks, kuna koolid ja ülikoolid kasutavad õpilaste haridust õigel teel hoidmiseks veebipõhiseid õppetunde. Lisaks, kuna inimestel on lukustuse ajal paindlikum ajakava või rohkem vaba aega, on oluliselt suurenenud inimeste arv, kes kasutavad isiklikke õppe- ja arendustööriistu, näiteks keeleõpperakendusi. Tervishoid on pöördunud ka digitaalsete lahenduste poole ning nii vaimse kui ka füüsilise tervishoiu veebis kättesaadavaks tegemine on muutunud tavalisemaks ning aidanud leevendada tervishoiuteenustele juurdepääsu vähenemise negatiivseid mõjusid.

# Olemasolevad asjakohased raamistikud

.

Professionaalsete õpetajate tulemusliku ja sisuka kriteeriumipõhise digipedagoogiliste pädevuste professionaalse arengu toetamiseks on välja töötatud erinevad digipedagoogiliste pädevuste raamistikud.

Viimastel aastatel avaldatud Euroopa raamistikud annavad ülevaate sellest, kuidas peaksid välja nägema digitaalselt pädev haridusorganisatsioon DigCompOrg ja digipädev õppejõud DigCompEdu, julgustades organisatsioone tagama oma töötajate kompetentsid ja töötama välja riiklikud lahendused digipädevuse tagamiseks.

DigCompEdu on digipädevuste raamistik, mille sihtrühmaks on peamiselt ülikooli õppejõud ja töötajad.

DigCompi raamistik tuvastab digipädevuse põhikomponendid viies valdkonnas:

1. Teabe- ja andmepädevus: teabevajaduste sõnastamine, digitaalsete andmete, teabe ja sisu leidmine ja hankimine. Otsustama allika ja selle sisu asjakohasust. Digitaalsete andmete, teabe ja sisu salvestamiseks, haldamiseks ja korraldamiseks.
2. Suhtlemine ja koostöö: suhelda, suhelda ja teha koostööd digitaaltehnoloogiate kaudu, olles samal ajal teadlik kultuurilisest ja põlvkondadevahelisest mitmekesisusest. Osaleda ühiskonnaelus avalike ja erasektori digiteenuste ning osaluskodaniku kaudu. Oma digitaalse kohaloleku, identiteedi ja maine haldamiseks.
3. Digitaalse sisu loomine: digitaalse sisu loomine ja redigeerimine Teabe ja sisu täiustamiseks ja integreerimiseks olemasolevasse teadmistepagasi, mõistes samas, kuidas autoriõigusi ja litsentse tuleb kohaldada. Oskab anda arvutisüsteemile arusaadavaid juhiseid.
4. Ohutus: seadmete, sisu, isikuandmete ja privaatsuse kaitsmiseks digitaalsetes keskkondades. Kaitsta füüsilist ja psühholoogilist tervist ning olla teadlik digitaaltehnoloogiatest sotsiaalse heaolu ja sotsiaalse kaasatuse tagamiseks. Olla kursis digitehnoloogiate ja nende kasutamise keskkonnamõjudega.
5. Probleemide lahendamine: Vajaduste ja probleemide väljaselgitamine ning kontseptuaalsete probleemide ja probleemsituatsioonide lahendamine digitaalses keskkonnas. Kasutada digitaalseid tööriistu protsesside ja toodete uuendamiseks. Et olla kursis digitaalse arenguga.

On olemas DigCompi kontseptuaalne võrdlusmudel, kus nendes valdkondades on 21 pädevust. Lisadimensioonid kirjeldavad oskustasemeid, teadmisi, oskusi ja hoiakuid ning kasutusjuhtumeid

# Noorsootöötajate digitaalse suveräänsuse pädevuste raamistik

Tuginedes olemasolevate raamistike küsitlusele ja analüüsile, otsustasid selle projekti partnerid keskenduda neljale DigiCompi ohutusteemale ning lisada ka noorsootöötajatele spetsiaalselt vajalikke pädevusi. Siin on DigiCompi raamistiku pädevused:

4.1 Kaitseseadmed
Seadmete ja digitaalse sisu kaitsmiseks ning digikeskkonnas esinevate riskide ja ohtude mõistmiseks. Teadma ohutus- ja turvameetmeid ning võtma nõuetekohaselt arvesse usaldusväärsust ja privaatsust.

4.2 Isikuandmete ja privaatsuse kaitsmine
Isikuandmete ja privaatsuse kaitsmiseks digikeskkondades. Et mõista, kuidas kasutada ja jagada isikut tuvastavat teavet, kaitstes ennast ja teisi kahjude eest. Mõistmaks, et digiteenused kasutavad ‚privaatsuspoliitikat", et teavitada, kuidas isikuandmeid kasutatakse.

4.3 Tervise ja heaolu kaitsmine
Suuta digitehnoloogiaid kasutades vältida terviseriske ja ohte füüsilisele ja psühholoogilisele heaolule. Suuta end ja teisi kaitsta võimalike ohtude eest digikeskkonnas (nt küberkiusamine). Olla teadlik digitaaltehnoloogiatest sotsiaalse heaolu ja sotsiaalse kaasatuse tagamiseks.

4.4 Keskkonna kaitsmine
Olla kursis digitehnoloogiate ja nende kasutamise keskkonnamõjudega.
https://joint-research-centre.ec.europa.eu/digcomp/digital-competence-framework_en#ref-4-safety

Noorsootöötajate põhiliste digipädevuste määratlemisel on kasulik mõelda nii sellest tuleneva praktilise õppimise universaalsetele (DigComp pädevused kodanikele) kui ka spetsiifilistele (igapäevased tegevused noorsootöös) tunnustele.

## Isikuandmete ja privaatsuse kaitsmise pädevus

* tehniliste digitehnoloogiate oskused,
*oskus kasutada digitehnoloogiaid mõtestatult töötamiseks, õppimiseks ja muudeks igapäevatoiminguteks,
* oskus hinnata kriitiliselt digitehnoloogiaid;
* teada põhilisi veebiturvalisuse reegleid;
* mõista, kuidas online töötab;
* mõista, mis on e-turundus ja kuidas see toimib;
* mõista privaatsust ja olla teadlik intellektuaalomandi õigustest;
* teadma, kuidas rakendada turvameetmeid;
* arendada enesetõhusust kasutades digitehnoloogiaid.

## Kaitseseadmete pädevus

Arvuti ja nutitelefoni kaitsmine tugeva ja ajakohase turvatarkvaraga. Kui arvuti või telefon on ründetarkvaraga nakatunud, pole muudest kaitsemeetmetest suurt abi, sest kurjategijatel võib juba olla kõigi võrgutoimingute võti. Samuti on oluline veenduda, et kõik operatsioonisüsteemi värskendused on installitud. Noorsootöötajad peaksid hoolitsema kõigi seadmete eest. Need peavad olema ajakohased ja tõhusa viirusetõrjetarkvaraga. Erinevad tootjad annavad välja värskendusi, mis mitte ainult ei täiusta funktsioone, vaid parandavad ka kõik turvavead, mis võivad seadmeid kahjustada.
ohus. Üldise ohutusreeglina on soovitatav mitte kasutada ühtegi teist arvutit või seadet tegevusteks, mis nõuavad teie kasutatavatesse teenustesse sisselogimist.

## Rämpsposti ja pettusi märkama õppimine

Kuigi mõnda neist on lihtne tuvastada, võivad muud andmepüügikatsed meilis, suhtlusvõrgustikes või veebisaitidel tunduda väga õigustatud. Ainus viis, kuidas kunagi andmepüügipettuse alla sattuda, on mitte kunagi klõpsata saadetud lingil. Kui meilis on kirjas, et see on pangast ja sellel on kõik õiged logod ja see teab nime, võib see pärineda pärispangast või mitte. Pakutud lingi kasutamise asemel võib veebisaidi leidmine ja otsingumootori kasutamine aidata kelmust ära hoida. Nii saab kasutaja teada, kas ta sattus seaduslikule saidile, mitte võltsitud saidile.

## Mainekate veebisaitide kasutamine ostude tegemisel

Kui kasutaja ei tea selle ettevõtte mainet, millelt ta soovib osta, on oluline saiti enne seda uurida. Küsige ‚Kuidas teised kasutajad neid üle vaatavad?". Kas nad kasutavad isikliku ja finantsteabe jaoks turvalist krüpteeritud ühendust?

## Valvel püsimine

Olge avaliku WiFi suhtes ettevaatlik ja mõelge kaks korda enne turvamata võrguga liitumist. On tööriistu, mis aitavad kasutajal sirvimise ajal rohkem privaatsust ja kaitset teiste kasutajate ja veebisaitide endi poolt avalikes WiFi-võrkudes.

## Internetis turvaline püsimine

Interneti-maailmast on saanud nii kiiresti muutuv keskkond, et tänased näpunäited võivad homme vananeda. Noorsootöötajad peavad teadma, et sisu, mida nad tarbivad (ja seda võib mõnikord olla tõesti palju), tuleb filtreerida. Oluline on olla natuke kahtlustav. Internetis on suhteliselt lihtne asju võltsida. Väga lihtne on paigutada Internetti midagi, mis pole täiesti tõsi või lihtsalt hunnik valesid. Peaksime olema eriti ettevaatlikud, et mitte uskuda kõike, mida me Internetis näeme ja loeme. Hea nõuandena peaksime süvenema, et teha vahet, mis on tõsi ja mis mitte, juhuks kui milleski vähegi kahtleme. Püüdke olla veebis toimuvate asjade suhtes kriitiline ja minimeerida seega mis tahes võrgutegevusega seotud riske.

## Teabe jagamine sotsiaalvõrgustikus

"Info jagamine kirjeldab andmevahetust erinevate organisatsioonide, inimeste ja tehnoloogiate vahel" (Techopedia). Teabe jagamist on mitut tüüpi:
üksikisikute jagatud teave (nt Facebookis või YouTube'is jagatud video);
Organisatsioonide jagatud teave (nt veebipõhise ilmateate RSS-voog);
Püsivara/tarkvara vahel jagatud teave (nt saadaolevate võrgusõlmede IP-aadressid või kettaruumi saadavus)

Kõik sotsiaalsed võrgustikud (või enamik neist) võimaldavad kasutajatel luua nii üksikasjalikke profiile, kui nad soovivad. Mõnel juhul aitab see protseduur kasutajatel leida teisi ühiste huvidega kasutajaid ja nii edasi. Sotsiaalmeedias nagu Facebook on võimalik privaatsusseadeid muuta, et kontrollida, milline info on avalik ja millist infot hoitakse ainult “sõprade” jaoks. Siiski on oluline teada, et sotsiaalvõrgustikul endal on see teave olenemata privaatsusseadest.

Tavaliselt jagavad inimesed vanust, sugu, perekonda, muid huvisid, hariduslikku tausta ja oma tööga seotud üksikasju. Piltide postitamine ehk “staatus” on kiire viis tunnete, olukordade näitamiseks ja teabe jagamiseks. Enamik sotsiaalvõrgustikke on loodud selleks, et seda võimalikult kiiresti saavutada. On väga oluline olla teadlik sellest, mida kasutaja jagab. Jagamine paljastab teabe, mis võimaldab reklaamijatel jälgida potentsiaalsete tarbijate eelistusi ja maitseid.

## GDPR

GDPR-i rakendati kõikidele EL-i ja EMP liikmesriikidele alates 25. maist 2018. See on asendanud praegused privaatsust käsitlevad õigusaktid liikmesriikides, mille suhtes praegu kehtib EL-i direktiiv 95/46. GDPR on teatud valdkondades üksikasjalikum ja täpsem ning võtab arvesse väljakutseid kiiresti arenevas digimaailmas, mis põhjustab andmesubjektide privaatsusriske.

# Viited

Andmekaitse ja privaatsus võrgus
https://europa.eu/youreurope/citizens/consumers/internet-telecoms/dataprotection-online-privacy/i ndex_en.htm

Techopedia
https://www.techopedia.com/definition/24839/information-sharing

Samm-sammult juhised arvuti seadistamiseks ja kasutaja loomiseks
https://www.wikihow.com/Use-a-Computer

Privaatsusõigused
https://www.privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and -social