

4. modul:

Pravni vidiki

Avtorica: Karin Drda-Kühn – media k GmbH – www.media-k.eu

Projekt je v okviru Erasmus + programa na področju poklicnega izobraževanja in usposabljanja financiran s strani Evropske komisije. Vsebina projekta ne odraža stališč Evropske unije, ampak zgolj stališča njenih avtorjev. Vsaka nepooblaščen uporaba in distribucija vsebin projekta v pridobitvene namene je kazniva.

Spletno izobraževanje THERAPY 2.0 : 9 tematskih modulov

1. O projektu in e-storitvah v zdravstvu

2. Spekter tehnološko podprtih informacijskih in komunikacijskih orodij in aplikacij za svetovalce in terapevte

3. Značilnosti računalniško podprte komunikacije pri svetovanju in terapiji

4. Pravni vidiki

5. Etični vidiki uporabe e-orodij/e-svetovanja

6. Ekonomski in finančni vidiki

7. Računalniška znanja, ki jih potrebuje spletni svetovalec ali terapevt

8. Psihološki vidiki

9. E-terapija za begunce, mladoletnike brez spremstva in prosilce za azil

Pregled vsebin modula

- Modul bo predstavil:
- evropski akcijski načrt, ki kot krovni dokument postavlja smernice razvoja e-storitev v zdravstvu, socialni in izobraževanju
- najpogostejše pravne ovire
- strategijo informatizacije slovenskega zdravstvenega sistema

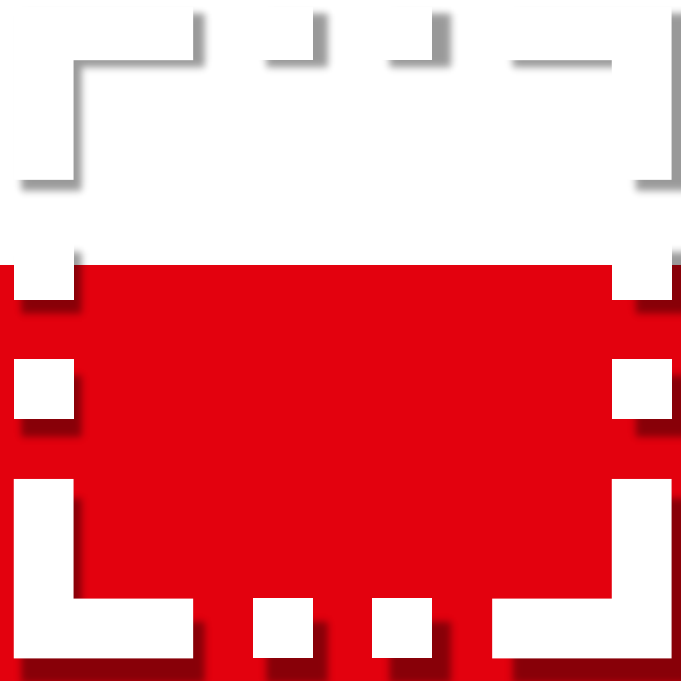
Namen modula:

- ✓ predstaviti razloge za informatizacijo zdravstvenega sistema in pomen akcijskega načrta e-zdravje za evropske državljane
- ✓ predstaviti obveze držav članic EU na področju vzpostavljanja pogojev za informatizacijo zdravstvenih sistemov;
- ✓ predstaviti rešitve za pravne ovire



Enote modula

- Enota 4.1: Pravne ovire pri implementaciji Akcijskega načrta e-zdravja
- Enota 4.2: Varnostna vprašanja povezana z uporabo podatkov v e-zdravstvu
- Enota 4.3: Nova pravila o varstvu osebnih podatkov v EU

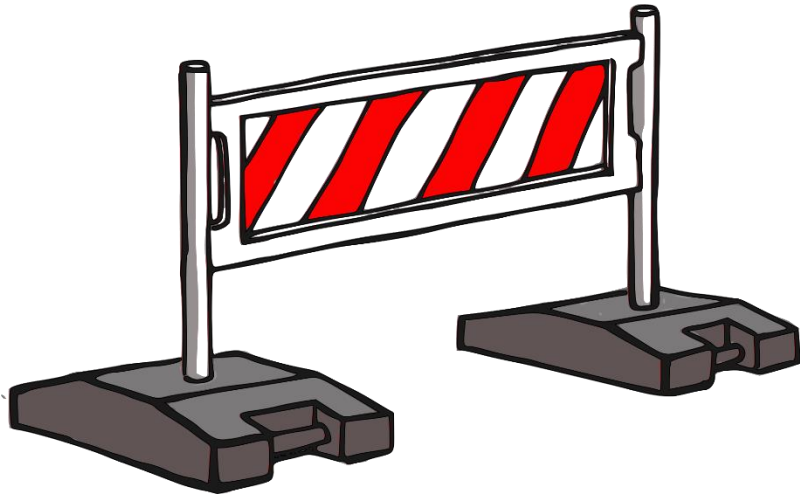


Struktura enote

- Ovire pri implementaciji akcijskega načrta v nacionalne pravne okvirje
- Odpravljanje pravnih ovir
- Nova evropska zakonodaja na področju varovanja osebnih podatkov
- Nova evropska zakonodaja na področju varovanja osebnih podatkov v Sloveniji
- Odpravljanje ovir v slovenski zakonodaji
- E-bralnik: priporočeno branje



Enota 4.1: Ovire pri implementaciji v nacionalne pravne okvirje



Kljub priložnostim in koristim so glavne ovire pri širšem uvajanju e-zdravja:

- neprimerni ali razdrobljeni pravni okvirji, vključno s pomanjkljivimi sistemi za kritje storitev e-zdravja;
- premalo pravne varnosti povezane z mobilnimi zdravstvenimi aplikacijami in aplikacijami za dobro počutje ter
- premalo preglednosti glede uporabe podatkov, ki jih zbirajo take aplikacije;
- visoki zagonski stroški pri vzpostavljanju sistemov e-zdravja;
- regionalne razlike pri dostopu do storitev IKT, omejen dostop na ogroženih območjih.

Več si lahko preberite [tukaj](#).

Enota 4.1: Odpravljanje pravnih ovir

Direktiva o uveljavljanju pravic pacientov pri čezmejnem zdravstvenem varstvu

Za vzpostavitev e-zdravja v Evropi je bistveno, da se odpravijo pravne ovire. [Direktiva o uveljavljanju pravic pacientov pri čezmejnem zdravstvenem varstvu](#) bo pripomogla k doseganju tega cilja, saj določa, da imajo pacienti pravico do čezmejnega zdravstvenega varstva tudi na daljavo s pomočjo telemedicine.

Komisija je v delovnem dokumentu o uporabi veljavnega pravnega okvira EU za telemedicinske storitve pojasnila, da se [zakonodaja EU uporablja](#) za področja, kot so kritje stroškov, odgovornost, izdajanje licenc zdravstvenim delavcem in varovanju podatkov pri čezmejnem zagotavljanju telemedicine.



Enota 4.1: Nova evropska zakonodaja na področju varovanja osebnih podatkov

*GDPR je kratica za **General Data Protection Regulation** oz. za [Splošno uredbo EU o varstvu podatkov](#), ki določa nova pravila glede varstva osebnih podatkov.*

Gre za zakonodajni sveženj, ki ga je Evropska komisija predlagala leta 2012 z namenom posodobitve in prenove določb iz [Direktive o varstvu podatkov iz leta 1995](#). V času od sprejema direktive leta 1995 je z razvojem sodobnih informacijsko-komunikacijskih tehnologij prišlo do obsežnih sprememb v obsegu, intenzivnosti in prenosih osebnih podatkov (npr. z razvojem in širitvijo uporabe računalništva v oblaku, družabnih omrežij, pametnih telefonov), ki terjajo prilagoditve in posodobitve zakonodajnega okvira.



Enota 4.1: Nova evropska zakonodaja

Splošna uredba postavlja enotna pravila za varstvo osebnih podatkov v EU, nekatera vsebinska in postopkovna vprašanja pa lahko uredijo države članice same. V Sloveniji bo ta vprašanja urejal **ZVOP-2**. Predlog ZVOP-2 je trenutno v zakonodajnem postopku, postopek pa je mogoče spremljati na povezavi [tukaj](#). Do besedila predloga zakona lahko dostopate [tukaj](#).

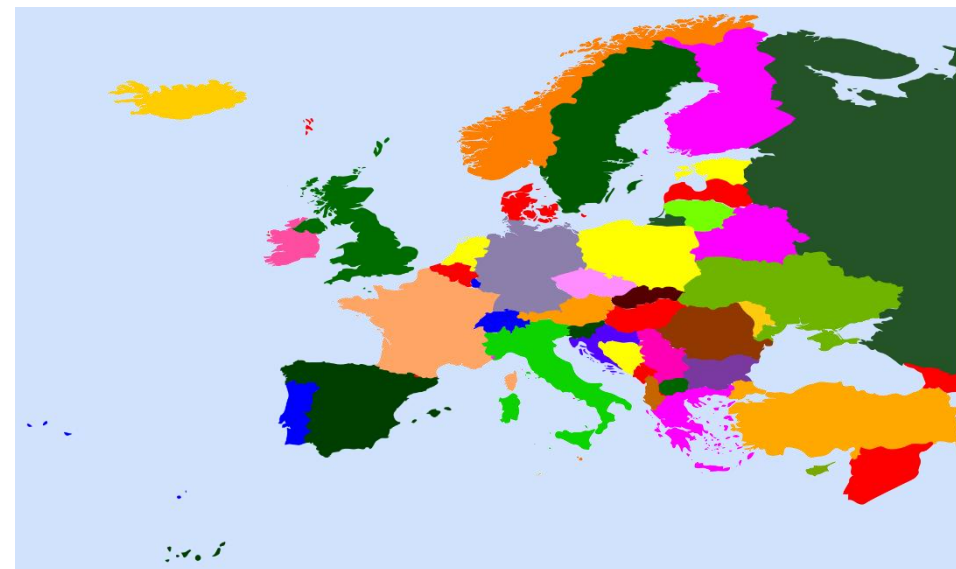
ZVOP-2 ureja določena **vsebinska področja**, kot so uporaba zdravstvenih, biometrijskih in genetskih podatkov in nekatere **postopkovne vidike** (npr. postopek izrekanja sankcij in pravna sredstva) ter **relacijo do drugih področij in pravic** (npr. dostop do javnih informacij, uporaba osebnih podatkov v znanstvene in statistične namene). Ne more pa spreminjati določb Splošne uredbe, saj se mora uredba v praksi neposredno uporabljati.



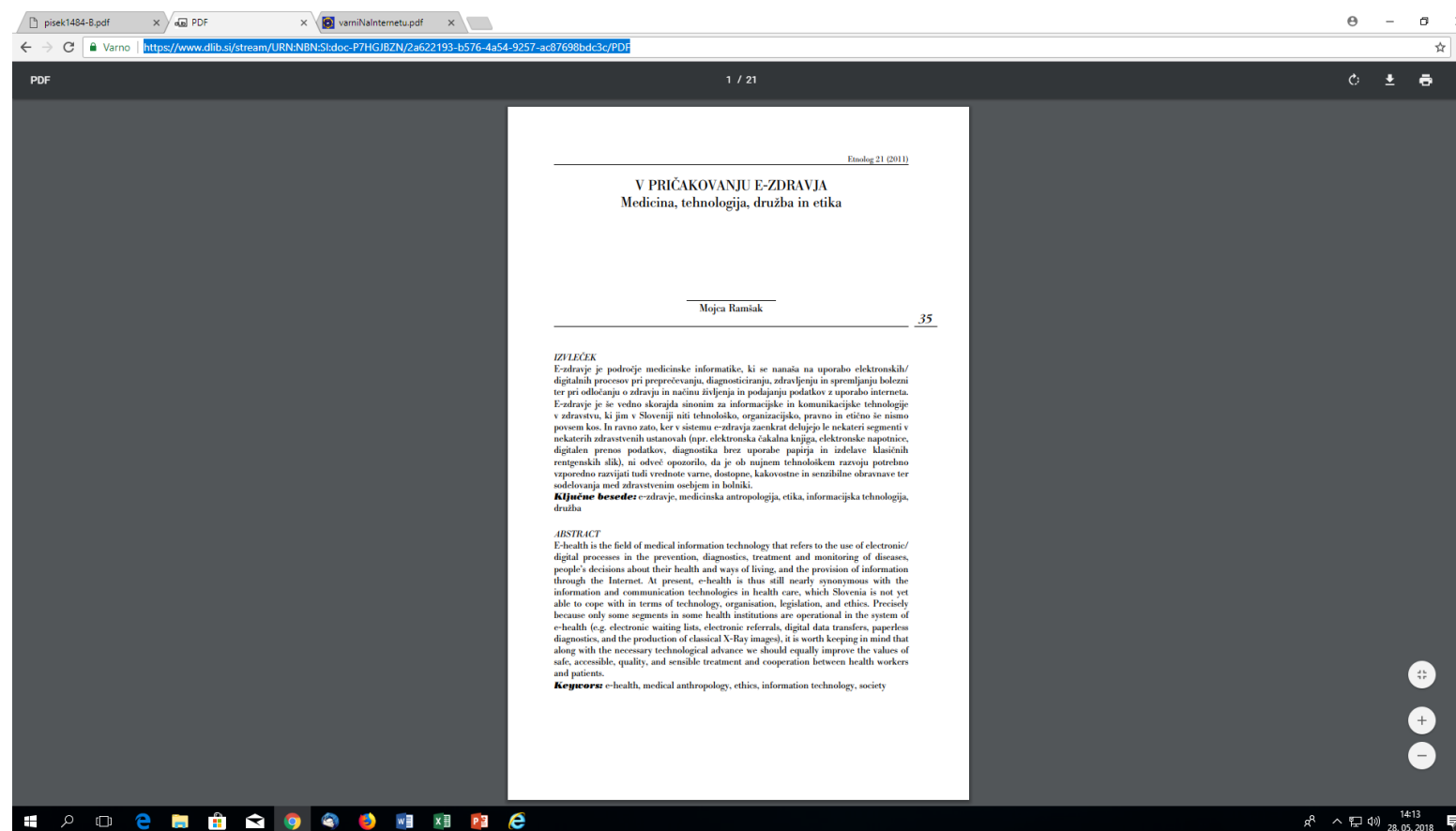
Enote 4.1: Odpravljanje ovir v slovenski zakonodaji

Trenutni predpisi v Sloveniji marsikdaj onemogočajo dostop do informacij z zdravstvenimi vsebinami. Eden takšnih je **Zakon o evidencah** s področja zdravstva. Tu bo potrebno na novo opredeliti zbirke podatkov, njihovo vsebino, namen in upravljavce.

Posebno pozornost je potrebno nameniti tudi **opredelitvam omejenega dostopa za posamezne skupine uporabnikov** (strokovno medicinska uporaba, finančno-upravna uporaba, dostopnost za najširšo javnost).



E-bralnik: strokovni članek Mojce Ramšak „V pričakovanju e-Zdravja“



Celoten članek je dostopen [tukaj](#).

Struktura enote

- Izhodiščna vprašanja
- Varnostna vprašanja in tveganja
- Varnostne nastavitve



4.2: Izhodiščna vprašanja

Kako dobro ste seznanjeni z
varnostnimi tvegani povezani
na spletu?

Na koga se obrniti v primeru
odkritega vdora na vaš
računalnik?

Kako lahko sami izboljšate
varnostne nastavitve?

Enota 4.2: Varnostna vprašanja in tveganja

Zdravstvene delavce veže k varovanju etični Kodeks medicinske deontologije [KMD], zakoni s področja zdravstvenega varstva [ZZVZZ] in zdravstvene dejavnosti [ZZD], zakon o varstvu osebnih podatkov [ZVOP-1], zakon o zbirkah podatkov [ZZPZV] [ZZPZV] ter drugi predpisi.

Svet Evropske unije je skupaj z Evropsko komisijo izdelal strategijo na področju informacijske varnosti, ki med drugim vključuje ISO 17799 v upravljanje varnosti informacij v privatnih in javnih organizacijah. Pri delu je potrebno upoštevati sklep Sveta Evropske unije o sprejetju predpisov o varovanju tajnosti podatkov (2001/264/ES).



Enota 4.2: Varnostna vprašanja in tveganja

- **Namen zahteve za varno izmenjavo digitalnih dokumentov** je v zagotavljanju varne in sledljive komunikacijo med različnimi deležniki, ki bo hkrati skladna z zakonodajo in standardi. Vključuje sledljivost dokumentov od naročila storitve, preko procesa svetovanja/terapije do vpisovanja v kartoteko in omogoča izboljšanje točnosti podatkov in dostopa do njih. Zadnji dve zahtevi sta skupni zahtevam standardov upravljanja z varnostjo informacij: *zagotoviti je potrebno zaupnost, celovitost in razpoložljivost informacij.*
- **Obseg zagotavljanja informacijske varnosti (scope)** določa, kje, v katerih procesih in v kakšnem obsegu se bo zagotavljala informacijska varnost.



Enota 4.2: Varnostna vprašanja

Ocena informacijskih varnostnih tveganj predstavlja metodo, s pomočjo katere se ovrednoti nivo zagotavljanja informacijske varnosti na organizacijskem nivoju. Ocena je del procesa upravljanja z informacijskimi tveganji, ki jih podaja standard ISO/IEC 27005:2008 [ISO_27005].

Vključuje:

- *identifikacijo in določitev dejanske in finančne vrednosti vseh informacijskih sredstev (oprema, programi, storitve, procesi..);*
- *identifikacijo groženj in verjetnosti njihovih uresničitvev;*
- *določitev stopenj ranljivosti informacijskih sredstev in nivoja sprejemljivega tveganja*
- *ocenitev možne škode ob uresničitvi grožnje*
- *ocenitev stroškov za odpravo posledic*
- *ocenitev stroškov za povečanje odpornosti za uresničitev najakutnejših groženj.*

Takšno oceno je potrebno izvajati periodično in po vsaki večji spremembi v IS organizacije.



Enota 4.2: Varnostna vprašanja povezana z uporabo podatkov v e-zdravstvu

Soglasja in dovoljenja pacientov: pacienti morajo imeti možnost dati soglasje in dovoljenje za obdelavo svojih podatkov in dovoljenja o obveščanju drugih oseb.

Dovoljenje za uporabo podatkov se uporablja za namene zdravljenja in kasneje za raziskovalne namene in statistiko. Obveščanje drugih oseb pa je aktualno v primeru, ko bi zaradi izrednih okoliščin ali zdravstvenega poslabšanja zdravstveno osebje moralo o tem obvestiti druge osebe (ponavadi ožje družinske člane).

Z vsebino soglasja je potrebno kliente seznaniti pred začetkom srečanj, prav tako je od njih potrebno pridobiti pred začetkom spletne terapije/svetovanja pridobiti soglasje.



Enota 4.2: Kako se zavarovati pred vdori nepooblaščenih oseb?

- **Nadgradite požarni zid** : ta prepreči dostop do storitev vašega računalnika, ki niso namenjene javni uporabi. Windows 7, Vista in XP takšno pregrado že vsebujejo, zato je ne izklaplajte (glej [navodila na straneh Microsoft Slovenija](#)). Za ostale verzije Windows operacijskega sistema pa je na voljo nekaj programov, ki so brezplačni za osebno uporabno: [ZoneAlarm Personal Firewall](#), [Outpost FirewallSunbelt Kerio Personal Firewall](#)
- **2. Posodobite svoj operacijski sistem**: od takrat, ko ste operacijski sistem namestili na računalnik (oziroma od nakupa računalnika ali operacijskega sistema), je bilo odkrito veliko število varnostnih ranljivosti, za katere je proizvajalec medtem že izdal popravke. Z namestitvijo le-teh (tj. s posodobitvijo operacijskega sistema) zakrpite varnostne luknje in občutno zmanjšate možnost zlorabe. Za Microsoft Windows pojdite na [Windows Update](#). Po možnosti aktivirajte samodejno nadgrajevanje (Automatic Updates, na voljo za Windows 2000/XP). Nekateri od popravkov so dokaj obsežni in njihov prenos po omrežju lahko traja nekaj ur, če uporabljate klicno povezavo na telefonskem omrežju. V tem primeru pokličite Microsoft Slovenija in se pozanimajte o brezplačni zgoščenki s popravki.

Enota 4.2: Kako se zavarovati pred vdori nepooblaščenih oseb?

- **3. Namestite [protivirusni program](#)**, ki omogoča samodejno in redno osveževanje seznama virusov s spleta. Oglejte si [seznam proizvajalcev](#) protivirusnih programov.
- **4. Preverite**, ali so se na vaš računalnik naselili [parazitni programi](#). Programa, ki omogočata odstranjevanje parazitnih komponent sta [Ad-Aware](#) in [Spybot Search & Destroy](#).
- Spletni brskalniki na spletnih straneh puščajo številne podatke. Zato se svetuje redno **brisanje piškotkov (cookies) in zgodovina obiskanih strani**.
- Pomembno si je zagotoviti **varnostne kopije podatkov** da ne ostanete brez ključnih podatkov v primeru okužbe z virusom ali poškodovanja strojne opreme.



Enota 4.2: Kam se obrniti po pomoč?

Uporabnikov interneta ob morebitnih varnostnih grožnjah (ob zaznavi vdora ali poskusa vdora) nudi pomoč tudi CERT (Computer Emergency Response Team), v Sloveniji pa njena nacionalna enota SI-CERT (www.arnes.si/si-cert).

Središče za pomoč organizacije Safe.si ponuja pomoč v primeru kraje osebne identitete in spletne zasvojenosti. Omogoča tudi spletno prijavo zlorab, neprimernih in nelegalnih vsebin na spletu in z njimi povezano reševanje težav. Nasveti in pomoč so dostopni na povezavi: <https://safe.si/sredisce-za-pomoc>

Tudi mobilni telefoni morajo biti ustrezno zavarovani. Več o tem pa je na voljo v zaviku *ABC varnosti in zasebnosti na mobilnih telefonih* na: https://www.ujp.gov.si/DocDir/Javne%20Objave/ABC_v_arnosti_in_zasebnosti_na_mobilnih_napravah.pdf



Struktura enote

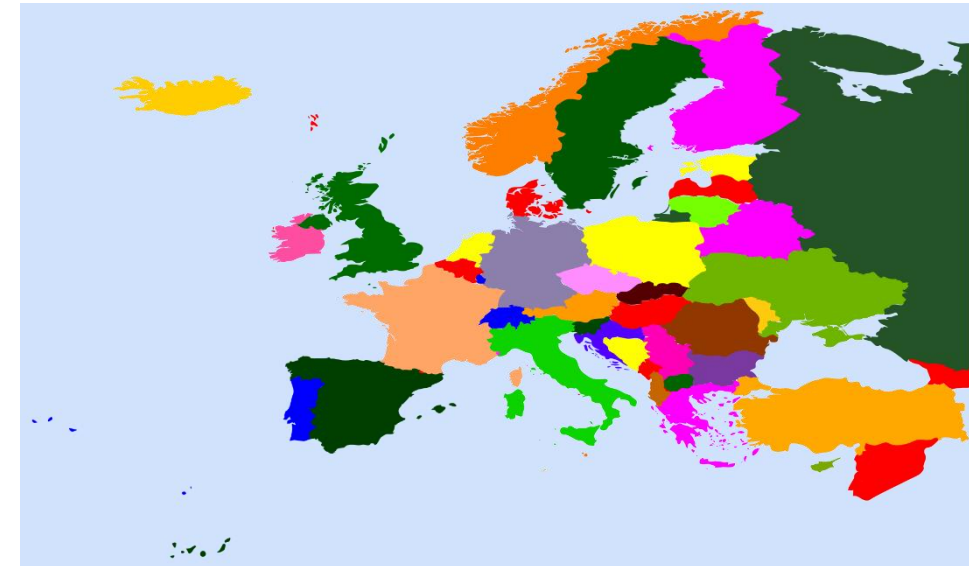
- Nova pravila o varstvu osebnih podatkov v EU
- Pomembne novosti
- Nadaljnji koraki
- Razmislek
- Izhodišče za končno diskusijo
- Naloga ob koncu enote



Enote 4.3: Nova pravila o varstvu osebnih podatkov v EU

Splošna uredba o varstvu podatkov (angl. General Data Protection Regulation – GDPR; v nadaljevanju uredba) je začela veljati **25.5.2016**, njene določbe pa se bodo morale neposredno uporabljati v vseh državah članicah od **25. 5. 2018.**

Priporoča se pregled [smernic](#) o ključnih temah, kot so pooblašcene osebe, ocene učinkov ali pravila glede profiliranja posameznikov, ki jih skupaj **pripravljamo vsi nadzorni organi v EU.**

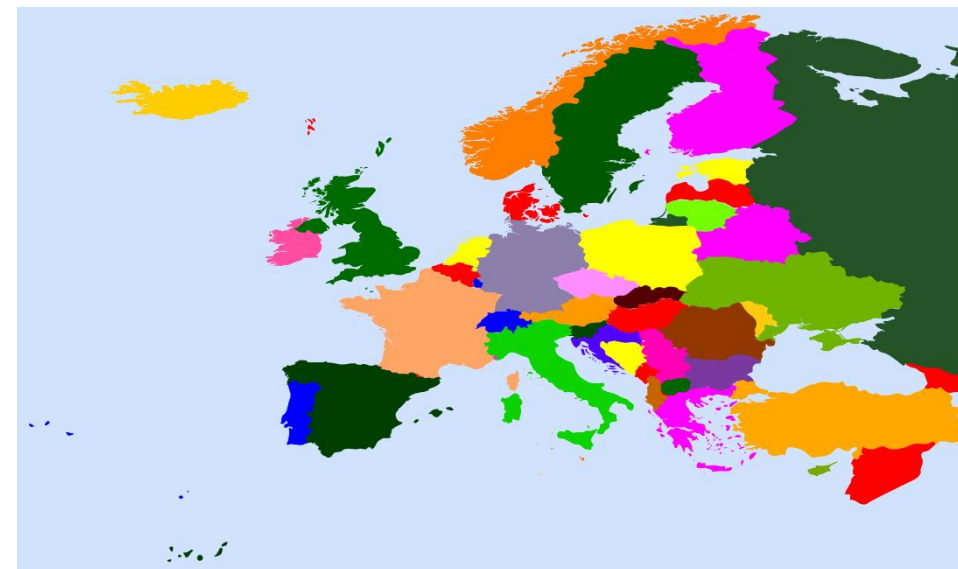


Enote 4.3: Pomembne novosti

Obveznosti upravljavcev in obdelovalcev podatkov

V skladu z uredbo bodo javni sektor ter podjetja, katerih temeljne dejavnosti zajemajo ali dejanja obdelave, ki pomenijo redno in sistematično obsežno spremljanje posameznikov, ali pa obsežno obdelavo posebnih vrst podatkov, morali imenovati **uradno (odgovorno) osebo za varstvo podatkov**.

Večji poudarek daje uredba tudi **(predhodnim) izvedbam analiz učinkov** na varstvo osebnih podatkov, v primeru varnostnih incidentov, kot je npr. izguba osebnih podatkov, pa se **uvaja obveznost poročanja nadzornemu organu in v določenih primerih** tudi obveščanja **vseh prizadetih posameznikov**.

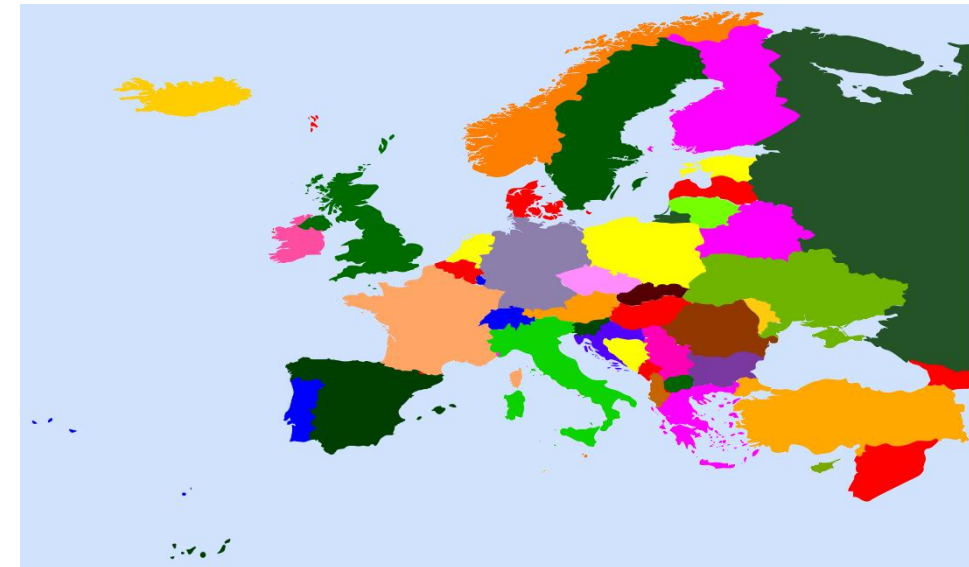


Enote 4.3: Pomembne novosti

Pravice posameznika

V uredbi so navedene pravice posameznika, na katerega se nanašajo osebni podatki, tj. posameznika, katerega osebni podatki se obdelujejo. Med temi pravicami so pravica do dostopa do osebnih podatkov ter pravice do popravka, pozabe, izbrisa, omejitve obdelave, ugovora in prenosljivosti podatkov.

Določena je tudi obveznost upravljavcev (oseb, odgovornih za obdelavo podatkov) glede zagotavljanja preglednih in lahko dostopnih informacij posameznikom, na katere se nanašajo osebni podatki, o obdelavi njihovih podatkov.



Enote 4.3: Nadaljnji koraki

- **PREVERITE VELJAVNOST OBSTOJEČIH PRIVOLITEV.** Privolitev mora biti jasna in razumljiva izjava, dana z nedvoumnim pritrdilnim dejanjem in dokazljiva. **Glej člene 6, 7 in 8, uvedne določbe: 32, 42, 43, 171.**
- **PREVERITE NAČIN PRIDOBIVANJA PRIVOLITEV V BODOČE.** Je posameznik ustrezno obveščen, komu daje podatke, katere in zakaj ter kakšne pravice ima? **Glej člene 12, 13 in 14.**
- **PRILAGODITE POGODBE S POGODBENIMI OBDELOVALCI.** Določene klavzule v pogodbah z zunanji izvjalci (računovodski servisi, IT ponudniki ...) bodo obvezne. **Glej člen 28.**
- **PREVERITE IN PRILAGODITE POPIS ZBIRK OSEBNIH PODATKOV – EVIDENCE DEJAVNOSTI OBDELAVE.** Če želimo podatke ustrezno varovati, moramo vedeti kje in katere imamo. **Glej člen 30.**
- **PREGLEJTE VAŠE POSTOPKE ZA ZAGOTAVLJANJE PRAVIC POSAMEZNIKA.** Posameznik ima pravico do seznanitve, omejitve, izbrisa, popravka, prenosljivosti in do ugovora. **Glej člene 12 - 22.**

Enote 4.3: Nadaljnji koraki

- **PRIPRAVITE SE NA IZVAJANJE NAČELA ODGOVORNOSTI.** Če so osebni podatki temelj vašega poslovanja, ne čakajte na obisk inšpekcije in pravočasno preverite:
 - **ALI BOSTE MORALI IZVAJATI OCENE UČINKA?** Glej člen 35.
 - **ALI BOSTE MORALI IMENOVATI ODGOVORNO OSEBO ZA VARSTVO OSEBNIH PODATKOV (»DPO«)?** Glej člen 37.
 - **VAŠE POSTOPKE ZA MINIMIZACIJO (NAČELO VGRAJENEGA IN PRIVZETEGA VARSTVA PODATKOV.** Minimizirajte 1) količino zbranih podatkov, 2) obseg njihove obdelave, 3) obdobje njihove hrambe in 4) kdo jih obdeluje. **Glej člen 25.**
- **PREGLEJTE IN PRILAGODITE VAŠE VARNOSTNE POLITIKE IN NJIHOVO IZVAJANJE.** Več o varnosti za mala podjetja na varninainternetu.si. Glej člen 24.
- **DOLOČITE, KDO BO POROČAL V PRIMERU VARNOSTNEGA INCIDENTA.** Če izgubite podatke ali pridejo v roke nepooblaščenim osebam, boste morali o tem poročati v 72-ih urah. **Glej člen 33.**
- **RAZMISLITE, ALI BI RADI DOBILI CERTIFIKAT, DA ZA OSEBNE PODATKE USTREZNO SKRBITE?** Certificiranje bo možno čez nekaj časa, bo prostovoljno, a plačljivo. **Glej člen 42.**

Razmislek

Kako učinkovito zaščiti vsebine in posnetke pogovorov, ki bodo nastajali v okviru e-svetovanja/terapije?

Katere pomembne novosti boste morali uvesti na področju varstva osebnih podatkov?



Naloga:

Preglejte in
prilagodite vaše
varnostne politike in
njihovo izvajanje.



Vprašanja ob koncu enote:

1. Kaj pomembnega prinaša Direktiva o uveljavljanju pravic pacientov v čezmejnem zdravljenju?
2. Katera varnostna vprašanja so povezana z uporabo osebnih podatkov v zdravstvenih sistemih?
3. Kako lahko poskrbite za zaščito strojne in programske opreme?
4. Katere pomembne novosti prinaša nov evropski zakon o varstvu osebnih podatkov za pacienta in katere obveznosti za ponudnike e-zdravstvenih storitev?

Viri:

- Global diffusion of eHealth: making universal health coverage achievable. Report of the third global survey on eHealth. World Health Organization 2016, ISBN 978-92-4-151178-0, also <http://www.who.int/goe/en> , assessed 26 February 2018
- Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services. Final report and recommendations. Brussels: European Commission; 2013 (http://ec.europa.eu/health/ehealth/docs/laws_report_recommendations_en.pdf , accessed 26 February 2018).
- European eHealth Action Plan <https://ec.europa.eu/digital-single-market/en/news/ehealth-action-plan-2012-2020-innovative-healthcare-21st-century> , assessed 26 February 2018
- Spletna stran Informacijskega pooblaščenca: <https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebni-podatkov/>
- Informatica Medica Slovenica (2005): Zaključki strokovnega srečanja E-zdravje za boljše zdravje v Sloveniji. Zreče (e-prispevek), dostopen na: [http://ims.mf.uni-lj.si/archive/10\(1\)/09.pdf](http://ims.mf.uni-lj.si/archive/10(1)/09.pdf)

Podatki o projektu:

Projekt: Therapy 2.0

Projektni koordinator: media k GmbH, Goethestr. 10, D-97980 Bad Mergentheim,
tel.: +497931 99 27 30, fax +49 7931 99 27 31

URL: <https://www.ecounselling4youth.eu>

Številka projekta: 2016-1-DE02-KA202-003245

Program financiranja: Erasmus+

Avtorica 4. modula – Pravni vidiki v spletnih intervencijah

Dr. Karin Drda-Kühn– kontakt: therapy2.0@media-k.eu

© **Fotografije:**

- Pixabay CC0 Creative Commons



Spletni tečaj je avtorsko zaščiten z licenco Creative Commons. Priznanje avtorstva-Nekomercialni namen-ShareAlike 4.0 International



Projekt je financiran s strani Evropske komisije v okviru programa Erasmus+. Vsebine spletnega tečaja ne odražajo stališč Evropske komisije, ampak stališča njenih avtorjev.

Partnerski konzilij:

Germany		media k GmbH (Koordinator) Dr. Karin Drda-Kühn / Hans-Jürgen Köttner • Therapy2.0@media-k.eu • + 49 7931 99 27 30
Germany		Innovation in Learning Institute – University of Erlangen-Nuremberg Evelyn Schlenk • Evelyn.Schlenk@ili.fau.de • + 49 9131 856 1111
Slovenia		Integra Institut, Institut za razvoj clovekovih potentialov Sonja Bercko Eisenreich • sonja.bercko@eu-integra.eu • + 38 659 013 2641
Croatia		Sveuciliste u Rijeci, Medicinski Fakultet Dr. Tanja Franciskovic / Dr. Marina Crepulja • tanja.franciskovic@medri.uniri.hr • + 38 591 2000 000
Iceland		Iceland Academy of the Arts Björg Jóna Birgisdóttir • bjorg@lhi.is • + 354 552 4000
Austria		Wissenschaftsinitiative Niederösterreich Dr. Wolfgang Eisenreich • office@wissenschaftsinitiative.at • + 43 676 944 5447
Portugal		Instituto Politecnico do Porto Dr. Regina Silva • ras@eu.ipp.pt • + 351 222 061
Greece		GUnet Akadimaiko Diadiktyo Pantelis Balaouras / Constantinos Tsibanis • costas@noc.uoa.gr • + 30 210 7275603

Zadnja drsnica



Modul je zaključen.