

SPECIALNO E-USPOSABLJANJE ZA ZAPOSLENE V ZDRAVSTVU**VARSTVO OSEBNIH PODATKOV V SKLADU Z GDPR IN NACIONALNO ZAKONODAJO**

Najnovejše raziskave kažejo, da so zaposleni pri varstvu osebnih podatkov praviloma najšibkejši člen v verigi. Vsaka organizacija, ki obdeluje osebne podatke zaposlenih ali tretjih oseb oziroma drugih posameznikov, mora vzpostaviti ustrezne mehanizme za varstvo le-teh. Samo sprejem notranjih aktov za uskladitev z zahtevami zakonodaje, ni dovolj! GDPR od vas zahteva aktivni pristop s katerim dokazujete skladnost v praksi. Med drugim, je redno usposabljanje zaposlenih ena izmed bistvenih zahtev za zagotavljanje kakovostnega, učinkovitega in proaktivnega ravnanja na področju varstva osebnih podatkov ter izkazovanje skladnosti z zahtevami GDPR (24. in 32. člen) in nacionalne zakonodaje o varstvu osebnih podatkov.

POMEMBNO: »Veriga je močna samo toliko, kot njen najšibkejši člen«. SMARTDPO - pametni DPO - poskrbi za to, da odgovornost za varstvo osebnih podatkov v organizaciji prevzamejo vsi zaposleni in s tem zagotovi »močno verigo«, ki preprečuje varnostne incidente.

Zakaj je e-učilnica najbolj primeren način usposabljanja vaših zaposlenih?

- ✓ ker je specialno prilagojena zaposlenim v zdravstvu,
- ✓ ker jo je možno še dodatno prilagoditi potrebam konkretnega subjekta v zdravstvu,
- ✓ ker vsebuje konkretna – praktična navodila in pravila za zagotavljanje varstva, skladnosti z zakonodajo in varno obdelave podatkov,
- ✓ ker so avtorji vsebine e-učilnice priznani strokovnjaki s področja varstva osebnih podatkov in poznavanjem dejavnosti zdravstva in lekarništva, področja pravic pacientov in informacijske varnosti, med drugim mag. Renata Zatler, Jerneja Merva in mag. Andrej Tomšič (namestnik IP) ter strokovnjaki za informacijsko varnost podjetja B2 d.o.o.,
- ✓ ker poleg osnovnih pravil varstva v skladu z GDPR in nacionalno zakonodajo zajema tudi **osnovna pravila s področja informacijske varnosti** (gesla, e-pošta, splet...), ki jih mora poznati vsak zaposleni,
- ✓ ker je enostavna za uporabo, zanimiva, dostopna preko spleta in ponuja vsebine na zanimiv, interaktiven način (kviz, vprašanja in obrazložitve odgovorov ipd.),
- ✓ ker zaposleni izvede usposabljanje in testiranje znanja takrat, ko ima za to čas in
- ✓ ker omogoča, da zaposleni pridobijo dokazilo o usposobljenosti za delo z osebnimi podatki.

Vsebina in čas usposabljanja:

- ✓ I. poglavje: Osnove varstva osebnih podatkov (GDPR in nacionalna zakonodaja)
- ✓ II. poglavje: Odgovorna in varna obdelava – varnost osebnih podatkov
- ✓ III. poglavje: Osnove informacijske varnosti
- ✓ IV. poglavje: **Zaključni test – preverjanje znanja** (za pridobitev potrdila o usposobljenosti)

Opomba: Več o vsebini najdete v prilogi tega dokumenta.

Okvirni čas e-učenja: 2 uri

Okvirni čas testiranja: 30 minut

Obdobje uporabe e-učilnice (rok za izvedbo): 21 dni oz. po dogovoru.

Način izvedbe e-usposabljanja:

1. Vodstvo subjekta s področja zdravstva **naroči e-usposabljanje za zaposlene pri podjetju Dataofficer d.o.o.**, na e-naslov: info@dataofficer.si. Poleg naročila za izvedbo, **posreduje seznam zaposlenih**, ki jih želi vključiti v e-usposabljanje z njihovimi imeni in elektronskimi naslovi. V usposabljanje se vključijo vsi, ki obdelujejo osebne podatke.
2. Dataofficer d.o.o. **posameznemu zaposlenemu dodeli uporabniško ime in geslo** za uporabo **SMARTDPO** e-učilnice za zaposlene pri subjektu s področja zdravstva.
3. Na določen dogovorjeni datum **zaposleni pričnejo z usposabljanjem preko spletnega portala Dataofficer d.o.o.** (<https://www.dataofficer.si/e-usposabljanje>).
4. E-učilnica je za udeležence **»odprta« oziroma se lahko uporablja tri tedne oz. je možno časovnico prilagoditi v skladu z dogovorom**. Kadarkoli v tem obdobju (lahko pa tudi večkrat) posamezni zaposleni predela e-gradivo in opravi testiranje (zaključni test). Po uspešno opravljenem končnem testiranju, **vsak zaposleni pridobi potrdilo o opravljenem usposabljanju in uspešno opravljenem testu, s katerim dokazuje usposobljenost za delo z osebniimi podatki**.
5. Po končanem usposabljanju naročnik - subjekt s področja zdravstva - od podjetja Dataofficer d.o.o. prejme **Poročilo o izvedbi usposabljanja za zaposlene, s katerim dokazuje skladnost poslovanja z GDPR (24. in 32. člen)**.

Za izvedbo je predviden **paketni pristop**. Usposabljanje se izvede v sodelovanju z vodstvom naročnika, **opravijo pa ga vsi zaposleni, ki pri naročniku obdelujejo osebne podatke**. Le na ta način lahko naročnik pridobi končno **Poročilo o izvedbi usposabljanja zaposlenih** in s tem dokazilo, ki ga potrebuje za dokazovanje skladnosti poslovanja z GDPR (24. in 32. člen).

Rok za prijavo na e-usposabljanje:

Prijave za usposabljanje **pošljite** na elektronski naslov info@dataofficer.si ali nas pokličite na št. **041 314-400**, Petra Avsec Bernot.

Termin usposabljanja je možno tudi prilagoditi vašim potrebam!

Cena na zaposlenega: 48,00 EUR

Stranke Dataofficer (DPO): **35 % popust: 31,20 EUR**

Več kot 100 udeležencev: **50 % popust: cena: 24,00 EUR**

V primeru večjega števila udeležencev se je možno dogovoriti za količinski popust, zato vas prosim, da nas pokličete. V primeru, da vas podrobneje zanima vsebina in izvedba, vam lahko pripravimo predstavitev ali vam omogočimo testni dostop.

Opomba: Navedenim cenam je treba prišteti še pripadajoči DDV.

Dataofficer d.o.o., Ljubljanska cesta 68, 1230 Domžale o MŠ: 8048291000 o ID za DDV: SI55700039

+386 41 325 479/+386 41 921 762 info@dataofficer.si www.dataofficer.si



Člani IAPP: več o certifikatu na: <https://iapp.org/certify/cippe/> .

O podjetju Dataofficer d.o.o.

Svetovalno podjetje Dataofficer d. o. o. **javnim in zasebnim poslovnim subjektom svetuje na področju izvajanja zakonodaje o varstvu osebnih podatkov, izvaja usposabljanja za vodje in zaposlene ter vodi projekte in nudi druge oblike strokovne pomoči za uskladitev subjektov z GDPR in nacionalno zakonodajo o varstvu osebnih podatkov ter nudi tudi storitev pooblaščenih oseb za varstvo osebnih podatkov (DPO).** Poleg **pravno organizacijskega svetovanja**, podjetje nudi tudi druge storitve svetovanja **na področju informacijske varnosti** in na področju dostopa do informacij javnega značaja (ZDIJZ).

Ekipo podjetja Dataofficer d. o. o. vodita **Jerneja Merva, univ. dipl. prav., CIPP/E** in **mag. Renata Zatler, CIPP/E, mednarodno certificirani pooblaščenih osebi za varstvo osebnih podatkov, svetovalki in predavateljici s področja varstva osebnih podatkov in informacij javnega značaja**. Imata bogate izkušnje in strokovno znanje ter kompetence s področja varstva osebnih podatkov (pravica do zasebnosti) in področja dostopa do informacij javnega značaja (pravica vedeti). Obe se lahko pohvalita tudi z **mednarodnim certifikatom CIPP/E** . Mednarodni certifikat **CIPP/E** dokazuje, da ima oseba, ki je certifikat pridobila, znanja in kompetence s področja varstva osebnih podatkov v skladu z najnovejšo evropsko zakonodajo (GDPR) in tako zagotavlja kompetentnega in uspešnega pooblaščenca za varstvo osebnih podatkov ter strokovnjaka s področja varovanja osebnih podatkov.

Na področju informacijske varnosti podjetje Dataofficer d. o. o. **sodeluje s strokovnjaki podjetja S&T Slovenija, Informacijske rešitve in storitve d.d.**, ki je že več kot 25 let eden vodilnih ponudnikov storitev na področju **informacijske varnosti**.

Reference: *Občine: Mestna občina Koper, Mestna občina Novo mesto, Občina Straža, Občina Piran, Občina Ajdovščina, Medobčinski inšpektorat Občina Straža in Novo Mesto, Občina Sežana, Občina Škofja Loka, Občina Trzin, Medobčinski inšpektorat Trzin, Občina Mengeš, Občina Moravče, Občina Kočevje ter druge občine; Javni zavodi: TIC Kamnik, Stanovanjski sklad Koper, Dolenjski muzej Novo mesto, Osnovna šola Jurija Vege in drugi;*
Zasebni subjekti: *Leitner & Leitner d.o.o., Assa Abloy d.o.o., Roche, farmacevtska družba d.o.o. , Episcenter d.o.o., Coloplast d.o.o., General Logistic Systems (GLS) d.o.o., Delo d.o.o., Tosama d.o.o., Lekarna Polzela d.o.o, Integral Avto d.o.o. Jesenice, Integral Brebus d.o.o. in drugi.*

Dataofficer d.o.o., Ljubljanska cesta 68, 1230 Domžale o MŠ: 8048291000 o ID za DDV: SI55700039

+386 41 325 479/+386 41 921 762 info@dataofficer.si www.dataofficer.si

SMARTDPO e-učilnica za zaposlene v zdravstvu
**VARSTVO OSEBNIH PODATKOV V SKLADU Z GDPR IN
NACIONALNO ZAKONODAJO**

POVZETEK VSEBINE



1. VARSTVO OSEBNIH PODATKOV – GDPR IN NACIONALNA ZAKONODAJA

| | |
|-------------|--|
| 1. 1. | OSEBNI PODATKI IN ZASEBNOST..... |
| 1. 2. | GDPR IN NACIONALNA ZAKONODAJA..... |
| 1. 3. | OSNOVNI POJMI..... |
| 1. 3. 1. | Kaj je osebni podatek (primeri OP – zdravstvo) |
| 1. 3. 1. 1. | Posebne vrste (občutljivi) osebnih podatkov..... |
| 1. 3. 2. | Druge definicije osnovnih pojmov..... |
| 1. 4. | PRAVNE PODLAGE ZA OBDELAVO..... |
| 1. 4. 1. | Pravne podlage za obdelavo – splošno..... |
| 1. 4. 2. | Pravne podlage za zdravstveno in lekarniško dejavnost |
| 1. 5. | NAČELA PRI OBDELAVI |
| 1. 5. 1. | Načelo vgrajenega in prevzetega varstva |
| 1. 6. | POSREDOVANJE (PRENOS) OSEBNIH PODATKOV ZUNANJIM UPORABNIKOM..... |
| 1. 7. | DOLŽNOSTI UPRAVLJAVCA OSEBNIH PODATKOV GLEDE VARSTVA OP |
| 1. 8. | POGODBENA OBDELAVA OSEBNIH PODATKOV |
| 1. 9. | PRAVICE POSAMEZNIKA..... |
| 1. 10. | ZASEBNOST IN NADZOR NA DELOVNEM MESTU |
| 1. 10. 1. | Nadzor uporabe interneta in e-pošte |
| 1. 11. | PRAVILA GLEDE KOPIRANJA OSEBNIH DOKUMENTOV |
| 1. 12. | PRAVILA GLEDE VIDEONADZORA IN DRUGIH OBLIK SNEMANJA |
| 1. 13. | VARSTVO OSEBNIH PODATKOV V PRAKSI – PRIMERI – ZDRAVSTVO |
| 1. 14. | KRŠITEV VARNOSTI OSEBNIH PODATKOV |
| 1. 14. 1. | Prijava kršitve informacijskemu pooblaščenču..... |
| 1. 15. | ODGOVORNOST IN KAZNI |
| 1.16 | VMESNO PREVERJANJE ZNANJA - KVIZ (25 vpr)..... |

| | | |
|----------|--|--|
| 2. | ODGOVORNA IN VARNA OBDELAVA OSEBNIH PODATKOV | |
| 2.1 | UKREPI ZA ZAGOTAVLJANJE VARNOSTI PODATKOV | |
| 2.1.1 | Interna pravila za zavarovanje..... | |
| 2.2. | VARNOST PODATKOV IN NAPRAV | |
| 2.2.1. | Izpostavljenost podatkov | |
| 2.2.2. | Varnost informacij v pisarni..... | |
| 2.2.3. | Skrb za dostopne elemente | |
| 2.2.4. | Brisanje digitalnih podatkov | |
| 2.2.5. | Varnost opreme in dostopnost..... | |
| 2.2.5.1. | Fizična varnost | |
| 3. | OSNOVE INFORMACIJSKE VARNOSTI | |
| 3.1. | NAJŠIBKEJŠI ČLEN | |
| 3.2. | VARNOSTNI INCIDENTI..... | |
| 3.3. | GESLA IN DOSTOPI DO PODATKOV | |
| 3.3.1. | Dostop do informacijskih sistemov | |
| 3.3.2. | Prijava v operacijski sistem..... | |
| 3.3.3. | Dostop do poslovnih sistemov, podatkovnih zbirk in aplikacij | |
| 3.3.4. | MOČNA GESLA – 10 priporočil za varna gesla | |
| 3.3.4.1. | Metode za pridobivanje gesel..... | |
| 3.4. | NEVARNOSTI E-POŠTE IN SPLETA | |
| 3.4.1. | (Ne)varna e-pošta..... | |
| 3.4.2. | Nezaželena in verižna pošta | |
| 3.4.3. | Nigerijsko pismo | |
| 3.4.4. | Zavajajoča sporočila | |
| 3.4.5. | Sporočila s priponkami | |
| 3.4.6. | Izsiljevalski virusi (vdori) | |
| 3.4.7. | (Ne)varen splet | |
| 3.8. | VMESNO PREVERJANJE ZNANJA – KVIZ (18 vpr.)..... | |
| 4. | ZAKLJUČNI TEST (formalno – 25 vpr.) | |
| 5. | ZAKLJUČEK (izpis potrdila o opravljenem testu) | |

Okvirni čas e-učenja: 2 uri

Testiranje: 30 minut, 22 vprašanj (za pozitivno 60 %)

PRIMER UČNEGA LISTA IZ GRADIVA – E-USPOSABLJANJE S PODROČJA VARSTVA OSEBNIH PODATKOV ZA ZAPOSLENE V ZDRAVSTVU

KRŠITEV VARNOSTI OSEBNIH PODATKOV

Tipi kršitev

- [Primeri kršitev](#)
- [Iz prakse](#)

Vsaka kršitev varnosti osebnih podatkov je **VARNOSTNI INCIDENT**. Ključni namen izvajanja vseh aktivnosti za skladnost upravljavca z zakonodajo o varstvu osebnih podatkov (GDPR in ZVOP), je usmerjen v **preprečevanje kršitev varnosti** osebnih podatkov.

Kršitev varnosti osebnih podatkov pomeni kršitev, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščen razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

Tipi kršitev:

Kršitev zaupnosti (nepooblaščen seznanitev z osebnimi podatki),

Kršitev celovitosti (nepooblaščen spreminjanje)

Kršitev dostopnosti (nezmožnost dostopa do podatkov)

V zadnjem času beležimo največ kršitev dostopnosti. Napadalci vdirajo v računalnike in IT omrežja, motijo poslovanje, vohunijo za podatki, povzročajo škodo ali onemogoča delovanje sistema. V praksi se to že pogosto dogaja tudi na področju zdravstvene in lekarniške dejavnosti. Vzrokov za ranljivost je več, **najpogosteje pa je kriv nepoučen in predvsem naiven uporabnik**, ki ne prepozna nevarnosti (npr. sumljive elektronske pošte ali uporablja neustrezna gesla za dostope).

Kršitev v praksi pomeni že dejstvo, da se zaposleni, ki ni pooblaščen za kadrovske zadeve oziroma obdelavo osebnih podatkov zaposlenih, v pogledu v personalno mapo, seznaneni z zdravstvenim stanjem sodelavca, npr. invalidnost. Če te podatke posreduje drugim oziroma jih razširja lahko posamezniku povzroči veliko škodo. Poleg kazenskih sankcij po GDPR lahko kršitelja doleti tudi odškodninska odgovornost.

zavihek: **1 2 3**

Posledice kršitev: izguba nadzora nad osebnimi podatki, diskriminacija, kraja ali zloraba identitete, finančne posledice, izguba ugleda, zaupanja...

Primer »težje« kršitve načela dostopnosti (primer, ki se je že zgodil pred kratkim): »Začasna nedosegljivost osebnih podatkov v javnem sektorju (npr. v bolnišnici, lekarni, zdravstvenem domu...) ima praviloma bistveno večjo škodo kot pa na primer nedosegljivost osebnih podatkov v zasebnem podjetju, kjer se vodijo le osnovni podatki o kupcih in le ti niso občutljive narave. Zaradi težjih posledic kršitev, mora subjekt javnega sektorja zagotoviti bistveno višji standard varnosti podatkov. Med drugim to zagotovi tudi z ustrezno stopnjo osveščenosti in usposobljenosti zaposlenih za zagotavljanje varnosti obdelave.»

