»PREVZEMITE NADZOR NAD PODATKI IN PREPREČITE KRŠITVE«

SPECIALNO E-USPOSABLJANJE ZA ZAPOSLENE NA OBČINAH

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 (občanov, pacientov, šolarjev…) mora vzpostaviti ustrezne mehanizme za varstvo** le-teh. Samo sprejem notranjih aktov za uskladitev z zahtevami zakonodaje, ni dovolj! GDPR od vas zahteva aktivni in kontinuiran 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 oziroma pametni DPO poskrbi za to, da **odgovornost za varstvo osebnih podatkov v organizaciji prevzamejo vsi zaposleni** in s tem zagotovi »močno verigo« za varnost podatkov.

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

- ✓ ker je specialno **prilagojena zaposlenim na občinah**,
- ✓ 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 informacijske varnosti, med drugim mag. Renata Zatler in mag. Andrej Tomšič),
- ✓ 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,**
- ✓ 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
- ✓ 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 (Vsebina e-učilnice za zaposlene na občinah)*

Okvirni čas e-učenja: 2 uri

Čas testiranja: 30 minut

Obdobje uporabe e-učilnice (rok za izvedbo): 21 dni

Način izvedbe e-usposabljanja:

1. Vodstvo občine **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 na občinah.
3. Na določen dogovorjeni datum (prvi je predviden **20. marca**) **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**. 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 osebnimi podatki.**
5. Po končanem usposabljanju občina 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** in ne posamični pristop. Usposabljanje se izvede v sodelovanju z vodstvom občine, **opravijo pa ga vsi zaposleni, ki v občini obdelujejo osebne podatke**. V praksi to pomeni približno 80 (pri manjših občinah je ta odstotek lahko tudi nižji) odstotkov zaposlenih. Le na ta način lahko občina 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 prvo e-usposabljanje:

Prijave za usposabljanje, ki bo potekalo od **10. aprila 2019 do 5. maja (zaradi prvomajskih praznikov je termin za teden dni podaljšan) aprila 2019**, **pošljite do 5. aprila 2019**, na elektronski naslov petra.avsec@dataofficer.si ali nas pokličite na št. 041 314-400, Petra Avsec Bernot.

Cena na zaposlenega:

Redna cena: 48,00 EUR

Članice SOS: **15 % popust**: **40,80 EUR**

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

Več kot 50 udeležencev iz ene občine: dodatni količinski popust (v skladu z dogovorom).

Opomba: Navedenim cenam je treba prišteti še pripadajoči DDV.

Direktorica:

Mag. Renata Zatler

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

SMARTDPO e-učilnica za zaposlene na občinah

POVZETEK VSEBINE

Okvirni čas e-učenja: 2 uri

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

PRIMER GRADIVA IZ SPLETNE E-UČILNICE –

KRŠITEV VARNOSTI OSEBNIH PODATKOV [E] [S]

- 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, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

Tipi kršitev:

Kršitev zaupnosti (nepooblaščena seznanitev z osebnimi podatki),
Kršitev celovitosti (nepooblaščeno 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 v javnem sektorju. 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 delavec, ki ni pooblaščen za kadrovske zadeve oziroma obdelavo osebnih podatkov zaposlenih, z vpogledom v personalno mapo, seznani 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 na eni izmed občin): »*začasna nedosegljivost osebnih podatkov v občini ima večjo škodo (lahko tudi odpoved »poslovanja z občani«) kot pa na primer nedosegljivost osebnih podatkov v zasebnem podjetju, kjer vodijo osnovne podatke o kupcih. Zaradi morebitnih težjih posledic kršitev, mora občina zagotoviti višji standard varnosti (fizične in elektronske) podatkov.* »

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 **pooblaščene osebe za varstvo osebnih podatkov (DPO)**. Poleg **pravno organizacijskega svetovanja**, podjetje nudi tudi druge storitve svetovanja **na področju informacijske varnosti** in svetovanje 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, mednarodno certificirani pooblaščeni 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, 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, Lekarna Polzela, Dolenjski muzej Novo mesto, Osnovna šola Jurija Vege in drugi;* ***Zasebni subjekti****: Delo d.o.o., Tosama d.o.o., Assa Abloy d.o.o. , Coloplast d.o.o., General Logistic Systems d.o.o., TSC Laba d.o.o., Integral Avto d.o.o. Jesenice, Integral Brebus d.o.o. in drugi.*

DATAOFFICER