REPUBLIKA SLOVENIJA
INFORMACIJSKI POOBLAŠČENEC
Dunajska cesta 22, 1000 Ljubljana
T: 01 230 9730
F: 01 230 9778
gp.ip@ip-rs.si
www.ip-rs.si

Številka: 0712-6/2018/1
Datum: 9. 11. 2018

Zadeva: **Priporočila Informacijskega pooblaščenca glede delovanja pooblaščene osebe za varstvo osebnih podatkov**

Uvodna pojasnila

1. Prednosti pooblaščene osebe za varstvo podatkov (v nadaljevanju DPO) se kažejo v večjemu pomenu in večji osredotočenosti na varstvo osebnih podatkov v organizaciji, v stalnosti nadzora in preventive.
2. Ključna za uspešno delovanje DPO je ustrezna podpora vodstva, ki je prepoznalo, da DPO zasleduje iste interese kot organizacija v smislu skladnosti poslovanja in zaupanja strank.
3. Organizacija se mora zavedeti, da DPO ni odgovoren za skladnost, temveč je za skladnost odgovoren upravljavec/obdelovalec (zavezanec). Vloga DPO je nadzorno-svetovalne narave.
4. DPO ne sme postati edini, ki kaj ve/mora vedeti o varstvu osebnih podatkov v organizaciji.
5. DPO ne bi smeli biti „lastniki procesov“, ki odločajo o namenih in sredstvih obdelave, saj ne sme nadzirati samega sebe.

Splošna priporočila

1. DPO se imenuje z namenom spremljanja notranje skladnosti s Splošno uredbo o varstvu podatkov[1] in drugimi predpisi o varstvu osebnih podatkov, izvajanja izobraževalnih in svetovalnih nalog glede varstva osebnih podatkov.
2. DPO mora imeti strokovno znanje s področja varstva osebnih podatkov in poznavanje zadevnih praks.
3. DPO mora svoje dolžnosti in naloge izvajati neodvisno, ne glede na to, ali je zaposlen pri upravljavcu ali ne.
4. Ključne cilje javnosti DPO se nanašajo na njene naloge kot kontaktne točke za:
    a. posameznike,
    b. nadzorni organ,
    c. zaposlene in druge osebe znotraj same organizacije.
5. Kontakti DPO se objavijo na spletni strani družbe, v internem imeniku in sporočijo Informacijskemu pooblaščencu skladno z določbami člena 37 Splošne uredbe. Skladno s **smernicami** Evropskega odbora za varstvo podatkov[2]:
    a. naj bi objavljeni kontaktni podatki na spletni strani (neobvezno) vključevali ime DPO;
    b. se nadzornemu organu nujno sporoči ime DPO (tudi v primeru zunanjih DPO);
    c. je priporočijo svojim zaposlenim sporočiti ime in kontaktne podatke DPO (npr. na intranetu, v internem telefonskem imeniku).
6. Zaposlene je treba obvestiti o imenovanju DPO in njegovem poslanstvu ter o tem, katere naloge opravlja in kakšne pristojnosti ima.
7. V primeru najemanja zunanjih storitev DPO je treba upoštevati, da gre za pogodbene obdelovalce osebnih podatkov, s katerimi je treba ustrezno urediti pogodbeno razmerje glede na zahteve člena 28 Splošne uredbe[3].

[1] Splošna Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov; uredba).
[2] Po javni razpravi revidirane Smernice o pooblaščenih osebah za varstvo podatkov (WP 243, 5. 4. 2017; dostopno na: https://www.ip-rs.si/fileadmin/user_upload/Pdf/Mednarodno_delovanje/wp243rev01_sl.pdf).
[3] Več o (pogodbeni) obdelavi: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/pogodbena-obdelava/

Dobre prakse glede položaja DPO

1. DPO je povabljen k rednemu udeleževanju na sestankih višjega in srednjega vodstva, kjer se sprejemajo odločitve o obdelavi osebnih podatkov.
2. Pri sprejemanju odločitev, ki vplivajo na varstvo podatkov, se zagotovi prisotnost DPO; DPO je treba pravočasno posredovati vse ustrezne informacije, da bi lahko zagotovil ustrezno svetovanje.
3. Mnenje DPO se vedno ustrezno upošteva. V primeru različnih stališč se dokumentirajo razlogi za neupoštevanje mnenja DPO.
4. DPO mora imeti dostop do drugih služb, kot so kadrovska služba, pravna služba, služba za informacijsko tehnologijo, varnostna služba itd.
5. Z DPO se opravi posvetovanje takoj, ko pride do kršitve varstva podatkov ali drugega incidenta.
6. Pri opravljanju svojih nalog DPO upošteva določbe zakonodaje, smernice nadzornih organov, standarde informacijske varnosti[4] in prakso.
7. Organizacija zagotovi, da je DPO ustrezno in pravočasno vključen v vse zadeve v zvezi z varstvom osebnih podatkov.
8. Organizacija DPO pomaga pri opravljanju nalog iz člena 39 Splošne uredbe o varstvu podatkov, tako da zagotovi sredstva, potrebna za opravljanje teh nalog, in dostop do osebnih podatkov in dejanj obdelave, ter ohranjanje njenega strokovnega znanja.
9. Organizacija zagotovi, da DPO pri opravljanju teh nalog ne prejema nobenih navodil.
10. DPO ne sme biti razrešena ali kaznovana zaradi opravljanja svojih nalog.
11. DPO neposredno poroča najvišji upravni ravni upravljavca ali obdelovalca.
12. Posamezniki, na katere se nanašajo osebni podatki, lahko z DPO stopijo v stik glede vseh vprašanj, povezanih z obdelavo njihovih osebnih podatkov, in uresničevanjem njihovih pravic.
13. DPO je pri opravljanju svojih nalog zavezan varovati skrivnost ali zaupnost v skladu s pravom Unije ali pravom države članice.
14. DPO lahko opravlja druge naloge in dolžnosti. Organizacija zagotovi, da zaradi takih nalog in dolžnosti ne pride do nasprotja interesov, tako da:
    a. se opredeli nezdružljive položaje s položajem DPO,
    b. se oblikuje notranja pravila, da bi preprečili nasprotja interesov in vključi razlago nasprotij interesov,
    c. se v sklepu o imenovanju DPO vključi izjava, da DPO ni v nasprotju interesov,
    d. se vključi ustrezne klavzule v razpise za DPO, če te naloga opravlja zunanja oseba.

Dobre prakse glede izvajanja nalog DPO

1. **DPO zaradi preprečevanja konflikta interesov ne bi smel opravljati npr. naslednjih nalog:**
    a. odločanje o pravicah posameznika,
    b. odločanje o vzpostavitvi novih zbirk osebnih podatkov, namenih in obsegih obdelave,
    c. odločanje o organizacijskih in tehničnih postopkih in ukrepih za varnost podatkov,
    d. odločanje o najemu obdelovalcev in priprava pogodb o najemu storitev obdelovalcev,
    e. odločanje o prenosu osebnih podatkov v tretje države,
    f. izvedba ocene učnikov glede varstva podatkov,
    g. priprava in ažuriranje evidenc dejavnosti obdelave,
    h. druge naloge, ki vključujejo odločanje o osebnih podatkih in kjer bi se DPO znašel v situaciji, da mora nadzirati lastne odločitve.
2. **DPO ne izvaja, temveč nadzira izvajanje naštetih nalog oziroma svetuje ustreznim službam pri izvajanju teh nalog.**
3. Priporoča se, da DPO do določenega dne v letu (npr. do 31.11. v tekočem letu) vodstvu predloži letni načrt nalog DPO, ki ga vodstvo po usklajevanjih z DPO in drugimi službami, kolikor so potrebna, odobri (npr. do 31.12. v tekočem letu).
4. Letni načrt nalog DPO naj vsebuje vsaj naslednje aktivnosti:

[4] Npr. ISO/IEC 27001:2013 Sistemi upravljanja informacijske varnosti - Zahteve.

a. Aktivnosti na področju **obveščanja, ozaveščanja in izobraževanja** upravljavca ali obdelovalca in zaposlenih, ki izvajajo obdelavo, ter svetovanje navedenim o njihovih obveznostih v skladu s Splošno uredbo o varstvu podatkov, veljavnim Zakonom o varstvu osebnih podatkov in drugimi določbami področne zakonodaje, ki ureja ravnanje z osebnimi podatki;
b. Aktivnosti povezane s **spremljanjem skladnosti** s Splošno uredbo o varstvu podatkov, veljavnim Zakonom o varstvu osebnih podatkov in drugimi določbami področne zakonodaje, ki ureja ravnanje z osebnimi podatki ter internimi politikami upravljavca v zvezi z zagotavljanjem varnosti osebnih podatkov, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja, vključenega v dejanja obdelave, ter s tem povezanimi revizijami;
c. Aktivnosti povezane s **svetovanjem**, kadar je to zahtevano, glede ocene učinka v zvezi z varstvom podatkov in spremljanje njenega izvajanja v skladu s členom 35 Splošne uredbe;
d. Aktivnosti **povezane s sodelovanjem z Informacijskim pooblaščencem** kot nadzornim organom za varstvo osebnih podatkov in drugimi nadzornimi organi v primerih čezmejne obdelave osebnih podatkov; vključno s predhodnim posvetovanjem iz člena 36 Splošne uredbe, in, kjer je ustrezno, posvetovanje glede katere koli druge zadeve v zvezi z varstvom osebnih podatkov
e. **Sprejemanje in obravnava prijav s strani zaposlenih** in iz drugih virov glede pomanjkljivosti ali kršitev pri obdelavi osebnih podatkov pri upravljavcu ali pri pogodbenih obdelovalcih, katerih storitve najema upravljavec.
f. Aktivnosti povezane z **evidentiranjem kršitev varnosti** po členu 33 Splošne uredbe in poročanje Informacijskemu pooblaščencu. če je tako določeno z internimi akti upravljavca[5].
g. **Poročanje vodstvu** o ugotovitvah izvedenih nadzorov in drugih aktivnostih DPO.

Priporočljivo je, da se opredeli **podrobnejši opis nalog DPO z ustrezno časovnico** (letni načrt dela DPO), ki ga potrdi vodstvo.

Primer: Letni načrt nalog pooblaščene osebe za varstvo osebnih podatkov

Področje	Naloge	Časovnica	Podrobnejši opis načrtovanih aktivnosti
Obveščanje, ozaveščanje in izobraževanja upravljavca ali obdelovalca in zaposlenih, ki izvajajo obdelavo, ter svetovanje	• Izvedba izobraževanja za vse zaposlene o predpisih glede varstva osebnih podatkov. • Priprava učnih gradiv. • Priprava ozaveščevalnih vsebin za intranet. • Posvetovalni sestanki z drugimi službami (IT, kadri, trženje…). • …	Najmanj enkrat letno. Priprava gradiv in vsebin po potrebi. Pred uvajanjem novih dejavnosti obdelave ali pred drugimi spremembami, ki imajo vpliv na raven varnosti osebnih podatkov.	*Opredeli se predvidena vsebina, trajanje, ciljne publike, cilji izobraževanja.*
Spremljanje skladnosti	• Nadzor izvajanja dolžnosti upravljavca/obdelovalca po uredbi (ustreznost in ažurnost evidentiranja dejavnosti obdelave[6], ustreznost izvedbe ocen učinka, ustrezno dokumentiranje zaznanih kršitev varnosti …). • Analiziranje in preverjanje skladnosti dokumentacije (interni akti glede varnosti in upoštevanja načel vgrajenega in privzetega varstva podatkov, privolitveni obrazci, obrazci za informiranje posameznika, politike	Preverjanje skladnosti se izvede najmanj enkrat letno.	*Določi se podrobnejša časovnica posameznih preverjanja, npr.:* *- Mesec t: preverjanje pravnih podlag* *- Mesec t+1: Preverjanje evidenc dejavnosti obdelave* *…*

[5] Opomba: Naloge glede kršitev varnosti niso nujno dodeljene DPO, temveč lahko vse ali nekatere opravlja oseba ali služba, ki je odgovorna za zagotavljanje informacijske varnosti v organizaciji. V tem primeru je priporočljivo, da je DPO seznanjen s postopkom in ugotovljenimi kršitvami varstva osebnih podatkov.
[6] Več o evidencah dejavnosti obdelave: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/evidenca-dejavnosti-obdelave/

	zasebnosti, druga dokumentacija). • Nadzor zakonitosti uporabe in dostopa do podatkov, ustreznosti varnostnih ukrepov (npr. spoštovanje politike čiste mize in čistega zaslona, ustreznost postopkov za varnostno kopiranje osebnih podatkov, ustreznost zagotavljanja sledljivosti obdelave osebnih podatkov, ustreznost ozaveščenosti zaposlenih…). • Nadzor spoštovanja področnih ureditev (npr. videonadzor, neposredno trženje, biometrija). • …	
Svetovanje zaposlenim in vodstvu	DPO nudi pomoč zaposlenim in vodstvu pri vprašanjih glede varstva osebnih podatkov, npr. glede ustreznosti pravnih podlag[7], postopkov in ukrepov za varnost podatkov in drugih vprašanj. DPO svetuje zadevnim službam, ki so odgovorne za izvedbo ocene učinka[8] in sicer: • ali je potrebno izvesti oceno učinka ali ne; • katero metodologijo se uporabi; • ali naj se oceno učinka izvede interno ali jo odda v zunanje izvajanje; • katere zaščitne ukrepe (vključno s tehničnimi in organizacijskimi ukrepi) je treba uporabiti in • ali je bila ocena učinka pravilno izvedena in ali so njene ugotovitve v skladu z uredbo.	V primeru zahtev po svetovanju s strani zaposlenih ali vodstva. Svetovanje glede ocene učinka se izvede pred njeno izvedbo in med samo pripravi. DPO po potrebi pregleda izdelane ocene učinka in poda mnenje.
Sodelovanje z nadzornimi organi	DPO opravlja komunikacijo z nadzornim organom in zagotovi razpoložljivost ustreznih kadrov, prostorov, opreme in podatkov, ki so potrebni za učinkovito in ekonomično izvedbo inšpekcijskega nadzora. DPO nadzornemu organu posreduje zaprosila za mnenje oziroma v postopku predhodnega svetovanje posreduje oceno učinka nadzornemu organu.	V primeru sprožitve uradnih postopkov s strani nadzornih organov. V primeru sprožitve uradnih postopkov s strani nadzornih organov ali v primeru potreb po pridobitvi mnenja nadzornih organov.
Sprejemanje in obravnava prijav glede pomanjkljivosti ali kršitev	DPO sprejema pritožbe, prijave in druga opozorila glede neskladnosti s zakonodajo s strani zaposlenih in tretjih oseb in jih ob	V primeru prijav s strani zaposlenih ali tretjih oseb.

[7] Infografike o pravnih podlagah:
- Javni sektor: https://www.ip-rs.si/fileadmin/user_upload/Pdf/infografike/pravne_podlage_javni_sektor.pdf
- Zasebni sektor: https://www.ip-rs.si/fileadmin/user_upload/png/infografike/pravne_podlage_zasebni_sektor_s_pogoji_privolitve.pdf
- Neposredno trženje: https://www.ip-rs.si/fileadmin/user_upload/Pdf/infografike/Neposredno_trzenje_infografika.pdf

[8] Več informacij o ocenah učinka: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/ocena-ucinka-v-zvezi-z-varstvom-podatkov/

pri obdelavi osebnih podatkov	ustreznem varovanju zaupnost posreduje v reševanje pristojnim službam oziroma vodstvu.	
Evidentiranje kršitev varnosti po členu 33 Splošne uredbe[9]	DPO glede na določbe internega akta o upravljanju varnostnih incidentov lahko sodeluje pri obravnavi kršitev varnosti, kar lahko vključuje: • opravljanje nalog centralne točke znotraj družbe za prejem obvestil o kršitvah varnosti, • komunikacijo s pogodbenimi obdelovalci, ko je to potrebno, • obveščanje ustreznih služb znotraj organizacije o kršitvah varnosti, • evidentiranje kršitev varnosti, • poročanje Informacijskemu pooblaščencu.	Takoj, ko je ugotovljena kršitev varnosti.
Poročanje vodstvu o ugotovitvah izvedenih nadzorov in opravljenih aktivnosti.	• DPO pripravi poročilo o ugotovitvah izvedenih nadzorov in drugih opravljenih aktivnostih (npr. obseg izobraževanja, svetovanja…).	Priporočljivo letno v primeru manjših organizacij, polletno ali mesečno v primeru večjih organizacij.

Mojca Prelesnik, univ.dipl.prav.,
informacijska pooblaščenka

[9] Več informacij o kršitvah varnosti: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/prijava-krsitev-varnosti/