Pooblaščena oseba za **varstvo podatkov – DPO**

Avtorici:
Maja Brajnik, dipl. prav. (UN), in Eva Langeršek, mag. prava

Splošna uredba o varstvu podatkov (v nadaljevanju: Uredba GDPR)[1] je s 25. majem 2018 na področje varstva osebnih podatkov prinesla kar nekaj novosti. Med njimi je tudi imenovanje pooblaščene osebe za varstvo podatkov, ang. Data protection officer (v nadaljevanju: DPO). DPO je nova funkcija v organizacijah, ki izpolnjujejo pogoje iz uredbe GDPR, po katerih so zavezane imenovati osebo, ki bo izvajala svetovalne in nadzorne naloge na področju varstva osebnih podatkov. Pomembno je, da obveznost imenovanja DPO ni odvisna od števila zaposlenih znotraj organizacije, ampak je obveznost njenega imenovanja odvisna izključno od dejavnosti organizacije in obsega ter narave obdelav osebnih podatkov.

Prispevek se osredotoča na določila uredbe GDPR. V delih, kjer so vključeni tudi kriteriji iz predloga Zakona o varstvu osebnih podatkov (ZVOP-2)[2], je to posebej poudarjeno. Kljub pozitivnim napovedim Ministrstva za pravosodje, da bo ZVOP-2 sprejet pred 25. 5. 2018, se to žal ni realiziralo. Kolegij predsednika Državnega zbora je 11. 4. 2018 odločil, da se ZVOP-2 ne bo sprejemal po nujnem zakonodajnem postopku, kot je predlagala Vlada Republike Slovenije, ampak po rednem zakonodajnem postopku. To pomeni, da ne bo sprejet v tem mandatu državnega zbora in ga lahko v najboljšem primeru pričakujemo v jesenskih mesecih letošnjega leta. Do takrat se še vedno uporabljajo tista določila ZVOP-1[3], ki ne odstopajo od uredbe GDPR – to pomeni, da potrebno kombinirati ZVOP-1 in uredbo GDPR.[4] Zaradi te odločitve se je lahko marsikatera organizacija znašla v nezavidljivem položaju, če je z izpolnjevanjem obveznosti iz uredbe GDPR čakala na sprejem nacionalnega predpisa. Organizacije so čakale z uvajanjem obveznosti v svoje poslovanje predvsem zato, ker je iz predloga ZVOP-2 izhaja, da bo v določenih točkah odstopal od določil uredbe GDPR.

Predlog ZVOP-2 med drugim odstopa od določil uredbe GDPR tudi v delu, ki je predmet tega prispevka, in sicer kriterijih za imenovanje DPO. Te kriterije napram uredbi GDPR definira konkretneje in postavlja pogoje, ki jih mora posameznik, ki bo opravlja funkcijo DPO, izpolnjevati.

KAJ JE DPO?[5]

V Smernicah o pooblaščenih osebah za varstvo podatkov je pojasnjeno, da pojem DPO ni nov. Pred sprejetjem GDPR je delovna skupina iz člena 29 trdila, da je DPO temelj odgovornosti in da lahko njegovo imenovanje olajša skladnost, podjetjem pa zagotovi konkurenčno prednost. Z novo ureditvijo tega področja pa Uredba GDPR to funkcijo oziroma osebo priznava kot **ključno akterko v novem sistemu** upravljanja podatkov ter določa pogoje za njeno imenovanje, položaj in naloge.

DPO je oseba s strokovnim znanjem s področja prava o varstvu podatkov in poznavanjem zadevnih praks. Njena naloga je, da upravljavcu ali obdelovalcu pomaga pri spremljanju notranje skladnosti z Uredbo GDPR.

Naloga DPO je, da upravljavcu ali obdelovalcu pomaga pri spremljanju notranje skladnosti z Uredbo GDPR.

KDO MORA IMENOVATI DPO?

V členu 39 Uredbe GDPR je določeno, da morajo nekateri upravljavci oziroma obdelovalci imenovati DPO.

Upravljavec in obdelovalec imenujeta pooblaščeno osebo za varstvo podatkov vedno, kadar:

a. obdelavo opravlja **javni organ** ali telo, razen sodišč, kadar delujejo kot sodni organ;
b. **(zasebni sektor[6])** temeljne dejavnosti upravljavca ali obdelovalca zajemajo dejanja obdelave, pri katerih je treba zaradi njihove narave, obsega in/ali namenov posameznike, na katere se osebni podatki nanašajo, redno in sistematično obsežno spremljati, ali
c. temeljne dejavnosti upravljavca ali obdelovalca zajemajo obsežno **obdelavo posebnih vrst podatkov** v skladu s členom 9 ter osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški iz člena 10 Uredbe GDPR[7].

Delovna skupina iz člena 29 priporoča, da naj upravljavci in obdelovalci **izvedejo in dokumentirajo notranjo analizo** o tem, ali so zavezani k imenovanju DPO – iz razloga, da bi lahko dokazali, da so ustrezno upoštevali ustrezne dejavnike – razen, če je očitno, da organizaciji ni treba imenovati DPO. Ta analiza je del dokumentacije v skladu z načelom odgovornosti in jo lahko zahteva nadzorni organ (Informacijski pooblaščenec). Po potrebi je potrebno analizo tudi posodobiti, na primer, če bi upravljavci ali obdelovalci pričeli izvajati nove dejavnosti ali zagotavljati nove storitve, ki bi lahko spadale pod zgoraj naštete primere, na podlagi katerih so zavezani k imenovanju DPO.[8]

V kolikor upravljavec oziroma obdelovalec ugotovi, da je zavezan k imenovanju DPO, je v skladu z Uredbo GDPR dolžan **objaviti** kontaktne podatke imenovane osebe in jih **sporočiti** nadzornemu organu.

V kolikor upravljavec oziroma obdelovalec ugotovi, da ni zavezan k imenovanju DPO, ga lahko imenuje tudi **prostovoljno**.

Uredba GDPR prav tako dopušča imenovanje **skupnega DPO**. Povezana družba lahko imenuje eno pooblaščeno osebo za varstvo podatkov, če je ta pooblaščena oseba za varstvo podatkov lahko dostopna iz vsake enote. Kadar je upravljavec ali obdelovalec javni organ ali telo, se lahko za več takšnih organov ali teles ob upoštevanju njihove organizacijske strukture in velikosti imenuje ena sama pooblaščena oseba za varstvo podatkov.

Ne nazadnje pa Uredba GDPR dopušča, da je DPO član osebja upravljavca ali obdelovalca (na primer: zaposlen v družbi – »notranji« DPO) ali pa naloge opravlja na podlagi pogodbe o storitvah (**»zunanji« DPO**).

NEODVISNOST DPO

DPO mora svoje dolžnosti in naloge izvajati neodvisno, ne glede na to, ali je pri upravljavcu zaposlen ali ne.[9]

Ključno vodilo pri izvajanju nalog pooblaščene osebe naj bo torej neodvisnost. Institut DPO zahteva celovitejši pristop in neodvisnega posameznika ali neodvisni kolegijski organ z vodjo (več posameznikov), ki mora(jo) izvrševati naloge in imeti ustrezno pozicijo, da pri tem ne pride do konflikta interesov. To predvsem pomeni, da DPO v organizaciji ne sme imeti položaja, ki bi omogočal opredelitev namenov ali storitev obdelave osebnih podatkov.

Splošno gledano lahko nasprotujoči si položaji v organizaciji vključujejo položaje višjega vodstva (kot so izvršni direktor, operativni direktor, finančni direktor, vodja zdravstvene službe, vodja oddelka za trženje, vodja službe za človeške vire ali vodja oddelkov za informacijsko tehnologijo) in tudi druge vloge na nižji ravni organizacijske strukture, če taki položaji ali vloge vodijo v določitev namenov in sredstev obdelave.[10]

Neodvisnost DPO pa ne pomeni, da njihova pooblastila za sprejemanje odločitev presegajo njihove naloge iz naslednjega poglavja. Upravljavec ali obdelovalec je še naprej **odgovoren za skladnost** s pravom o varstvu podatkov in mora biti to skladnost tudi zmožen dokazati. Če upravljavec ali obdelovalec sprejme odločitve, ki so nezdružljive s Uredbo GDPR in mnenjem DPO, bi bilo treba slednji omogočiti, da svoje odklonilno mnenje jasno posreduje najvišji upravni ravni in nosilcem odločanja. V zvezi s tem je v členu 38(3) določeno, da DPO »neposredno poroča najvišji upravni ravni upravljavca ali obdelovalca«. S takim neposrednim poročanjem zagotovi, da je višje vodstvo (npr. upravni odbor) seznanjeno z njenimi nasveti in priporočili, ki so del njenih nalog, da obvešča upravljavca ali obdelovalca ter mu svetuje.[11]

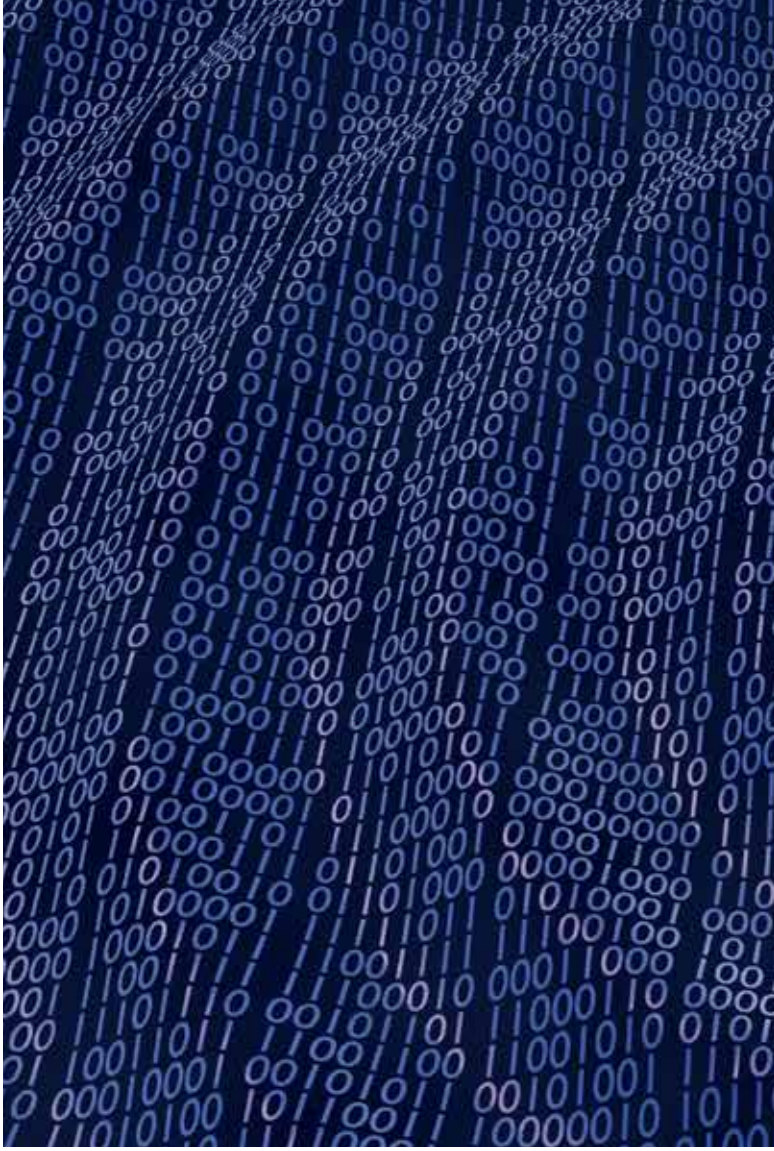
POLOŽAJ DPO

Kot že omenjeno v prehodnem besedilu, DPO **ni odgovoren za zagotavljanje skladnosti** z določbami o varstvu osebnih podatkov, pač pa sta upravljavec in obdelovalec tista, ki morata dokazati, da obdelava poteka v skladu z Uredbo.

Na podlagi tega ima DPO v skladu z Uredbo GDPR **poseben položaj**, in sicer:

a. DPO je pri opravljanju svojih nalog **zavezana varovati skrivnost ali zaupnost** v skladu s pravom Unije ali pravom države članice.

b. DPO je na **voljo tudi posameznikom**, na katere se nanašajo osebni podatki. Posamezniki lahko z DPO stopijo v stik glede vseh vprašanj, povezanih z obdelavo njihovih osebnih podatkov, in uresničevanjem njihovih pravic.



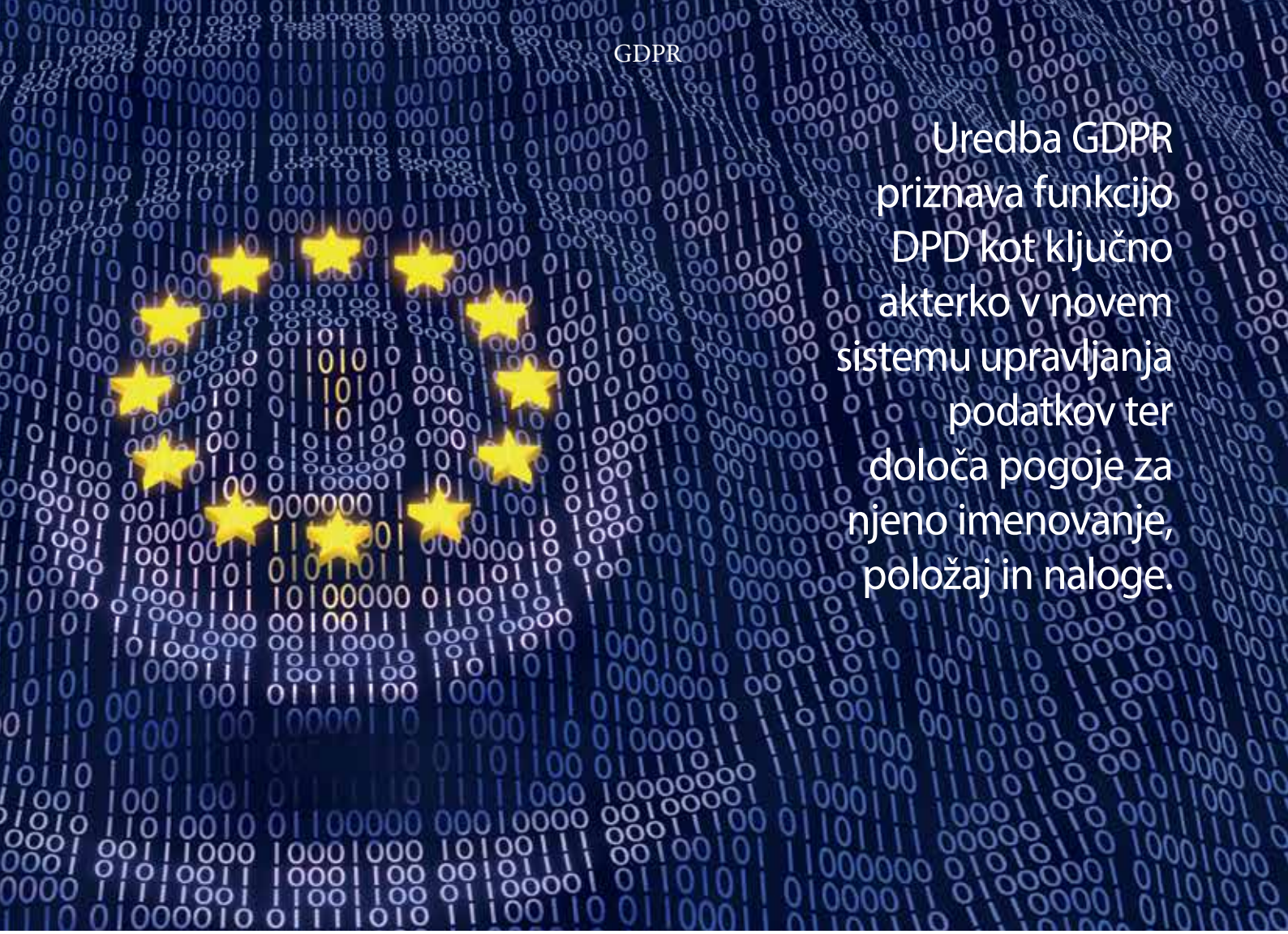
c. **Upravljavec in obdelovalec:**

- sta dolžna zagotoviti, da je DPO ustrezno in pravočasno **vključen v vse zadeve** v zvezi z varstvom osebnih podatkov;
- DPO-ju pomagata pri opravljanju nalog iz člena 39, tako da **zagotovita sredstva,** potrebna za opravljanje teh nalog, dostop do osebnih podatkov in dejanj obdelave ter ohranjanje njegovega strokovnega znanja;
- zagotovita, da DPO pri opravljanju teh nalog **ne prejema nobenih navodil**. DPO ne sme biti razrešen ali kaznovan zaradi opravljanja svojih nalog.

NALOGE DPO

DPO pri opravljanju svojih nalog upošteva tveganje, povezano z dejanji obdelave, ter naravo, obseg, okoliščine in namene obdelave in ima vsaj naslednje naloge:

- obveščanje upravljavca ali obdelovalca in zaposlenih, ki izvajajo obdelavo, ter svetovanje navedenim o njihovih obveznostih v skladu s to uredbo in drugimi določbami prava Unije ali prava države članice o varstvu podatkov;
- spremljanje skladnosti s to uredbo, drugimi določbami prava Unije ali prava države članice o varstvu podatkov in politikami upravljavca ali obdelovalca v zvezi z



Uredba GDPR priznava funkcijo DPD kot ključno akterko v novem sistemu upravljanja podatkov ter določa pogoje za njeno imenovanje, položaj in naloge.

varstvom osebnih podatkov, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja, vključenega v dejanja obdelave, ter s tem povezanimi revizijami;

- svetovanje, kadar je to zahtevano, glede ocene učinka v zvezi z varstvom podatkov in spremljanje njenega izvajanja v skladu s členom 35;
- sodelovanje z nadzornim organom;
- delovanje kot kontaktna točka za nadzorni organ pri vprašanjih v zvezi z obdelavo, vključno s predhodnim posvetovanjem iz člena 36, in, kjer je ustrezno, posvetovanje glede katere koli druge zadeve.

STROKOVNA USPOSOBLJENOST DPO

Uredba GDPR določa, da se DPO imenuje na podlagi poklicnih odlik ter zlasti strokovnega znanja o zakonodaji in praksi na področju varstva podatkov ter zmožnosti za izpolnjevanje nalog, ki so opredeljene v prejšnjem poglavju. Uredba GDPR pri definiranju kriterijev, ki jih mora izpolnjevati DPO, ni določna.

Delovna skupina iz člena 29 pa je zavzela stališče, da mora biti raven strokovnega znanja sorazmerna z občutljivostjo, zapletenostjo in količino podatkov, ki jih organizacija obdeluje. DPO mora imeti strokovno znanje o nacionalni in evropski zakonodaji in praksi na področju varstva podatkov ter poglobljeno razumevanje, hkrati pa mora poglobljeno razumeti vsebino uredbe GDPR. DPO mora dobro razumeti tudi dejanja obdelave, ki se izvajajo, in informacijske sisteme, pa tudi potrebe upravljavca v zvezi z varnostjo in varstvom podatkov. V primeru javnega organa ali telesa bi morala dobro poznati tudi upravna pravila in postopke organizacije.[12]

Natančnejše zahteve glede stopnje strokovne izobrazbe in delovnih izkušenj predpisuje predlog ZVOP-2. Glede na to, da ZVOP-2 še ni sprejet, niti ne moremo pričakovati, da se vsebina njegovih členov v zakonodajnem postopku ne bo spremenila, ni mogoče trditi, da bodo v sprejeti in potrjeni verziji ZVOP-2 kriteriji ostali enaki.

Glede na predlog ZVOP-2 mora DPO upravljavca ali obdelovalca v zasebnem sektorju izpolnjevati naslednje pogoje:

- biti mora poslovno sposoben,
- dosegati mora vsaj VII. stopnji izobrazbe (magisteriji stroke (2. bolonjska stopnja), univerzitetni programi pred bolonjsko reformo),
- imeti mora vsaj tri leta delovnih izkušenj s področja varstva osebnih podatkov,[13]
- v preteklosti ni bil pravnomočno obsojen na kazen najmanj šestih mesecev zapora oziroma ni bil pravnomočno obsojen za kaznivo dejanje glede zlorabe osebnih podatkov ali kraje identitete in obsodba še ni bila izbrisana.

Če je DPO imenovan v javnem sektorju, bo moral poleg prej navedenih kriterijev izpolnjevati še dodatni kriterij, in sicer bo moral biti državljan Republike Slovenije ali države članice Evropske unije ali države članice Evropskega gospodarskega prostora in aktivno obvladati slovenski jezik.

ZAKLJUČEK

V kolikor organizacija skozi analizo ugotovi, da je zavezana imenovati DPO, je priporočljivo, da DPO-ja imenuje začasno, saj v tem trenutku še ni jasno, ali bo sprejeti ZVOP-2 določal enake kriterije, kot so predvideni v predlogu ZVOP-2. Lahko se zgodi, da DPO, ki ga bo organizacija imenovala, ne bo izpolnjeval kriterijev iz ZVOP-2.

DPO se lahko v vmesnem obdobju določi že glede na določbe členov 37 – 39 uredbe GDPR, ampak naj bo to začasno oziroma v samo imenovanje vključite klavzulo, s katero boste izpolnjevanje kriterijev po sprejemu ZVOP-2 ponovno presojali ter posameznika s položaja razrešili, če se bo ugotovilo, da dodatnih kriterijev iz slovenske nacionalne zakonodaje ne izpolnjuje.

Potrebno je dodati tudi, da v vmesnem obdobju (do sprejetja novega ZVOP-2) ni kaznovalne funkcije Informacijskega pooblaščenca (globe za prekrške), je pa možen inšpekcijski nadzor.

Ministrstvo za pravosodje je izdalo mnenje[14], **v katerem je zavzelo stališče, da Informacijski pooblaščenec v smislu izrekanja upravnih glob in drugih sankcij ne bo pristojen za obravnavo kršitev določb uredbe GDPR**. Informacijski pooblaščenec bo lahko izrekal globe in druge sankcije po uredbi GDPR šele po sprejemu ZVOP-2.

Kljub temu pa bodo kršitve določb uredbe GDPR, storjene med 25. 5. in do sprejema ZVOP-2, še vedno (materialnopravno) kaznive ter bodo kršitelji po ureditvi pristojnosti Informacijskega pooblaščenca za njih lahko kaznovani, v kolikor se bodo ti postopki začeli oz. končali v okviru splošnih domačih zastaralnih rokov za obravnavo prekrškov.[15]

Opombe

1 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.
2 Predlog Zakona o varstvu osebnih podatkov, Generalni sekretariat Vlade Republike Slovenije, z dne 4. 4. 2018.
3 Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07), z dne 15. 7. 2014.
4 Prva sistemska pojasnila Ministrstva za pravosodje ob začetku razvoja uporabe nove evropske zakonodaje o varstvu osebnih podatkov, z dne 28. 5. 2018
5 Povzeto po: Delovna skupina za varstvo podatkov iz člena 29, Smernice o pooblaščenih osebah za varstvo podatkov (v nadaljevanju: Smernice o pooblaščenih osebah za varstvo podatkov) dostopno na: https://www.ip-rs.si/fileadmin/user_upload/Pdf/Mednarodno_delovanje/wp243rev01_sl.pdf, str. 5 in 6.
6 Na primer: banke, zavarovalnice, operaterji elektronskih komunikacij, trgovci s klubi zvestobe, kadrovske agencije, spletne trgovine in IT podjetja, ki vzdržujejo rešitve CRM, …
7 Na primer: klinični centri, bolnišnice in klinike, zdravstveni in socialno-varstveni zavodi, zapori in prevzgojni zavodi.
8 Povzeto po: Smernice o pooblaščenih osebah za varstvo podatkov, str. 6 in 7.
9 Uvodna določba 97 Uredba GDPR.
10 Povzeto po: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/pooblascena-oseba-za-varstvo-podatkov/.
11 Povzeto po: Smernice o pooblaščenih osebah za varstvo podatkov, str. 17.
12 Povzeto po: Smernice o pooblaščenih osebah za varstvo podatkov, str. 12 in 13.
13 Predlog ZVOP-2, 138. člen (prehodne in končne določbe): »Ne glede na pogoja izobrazbe iz 3. točke in vsebine in trajanja delovnih izkušenj iz 4. točke prvega odstavka 46. člena tega zakona se do 25. maja 2020 za pooblaščeno osebo lahko določi osebo, ki ima najmanj eno leto delovnih izkušenj s primerljivih področij informacijske varnosti, varstva poslovne skrivnosti po zakonu, ki ureja gospodarske družbe, ali varstva zaupnih podatkov po zakonu, ki ureja bančništvo.«
14 Ministrstvo je zavzelo to mnenje v Prvih sistemskih pojasnilih Ministrstva za pravosodje ob začetku razvoja uporabe nove evropske zakonodaje o varstvu osebnih podatkov.
15 Povzeto po Prvih sistemskih pojasnilih Ministrstva za pravosodje ob začetku razvoja uporabe nove evropske zakonodaje o varstvu osebnih podatkov, str. 5.

V kolikor organizacija skozi analizo ugotovi, da je zavezana imenovati DPO, je priporočljivo, da **DPO-ja imenuje začasno**, saj v tem trenutku še ni jasno, ali bo sprejeti ZVOP-2 določal enake kriterije, kot so predvideni v predlogu ZVOP-2. Lahko se zgodi, da DPO, ki ga bo organizacija imenovala, ne bo izpolnjeval kriterijev iz ZVOP-2.