INFORMACIJSKI POOBLAŠČENEC

Nova Splošna uredba o varstvu osebnih podatkov - (EU) 2016/679 (GDPR) – čas med ZVOP-1, GDPR in ZVOP-2

Mojca Prelesnik, univ. dipl. prav.
informacijska pooblaščenka
16. oktober 2018

Uredba (EU) 2016/679 EP in Sveta z dne 27.4.2016 o *varstvu posameznikov pri obdelavi OP in o *prostem pretoku OP ter o razveljavitvi Direktive 95/46/ES

Kdaj dobimo ZVOP – 2?

OP = katerakoli informacija v zvezi z „določenim ali določljivim“ posameznikom. --→>

OP: spletni identifikatorji, ID piškotkov,IP naslovi, psevdonimni podatki

((spol+datum rojstva+poštna številka))

Uporaba GDPR

1. Obdelava v celoti ali delno avtomatizirana ali zbirka OP.

2. GDPR se **NE** uporablja **(LE)** za obdelavo OP:

(a) če dejavnost izven uporabe prava EU (nacionalna varnost);

(b) ko DČ izvajajo skupno zunanjo in varnostno politiko;

(c) če fiz. oseba za popolnoma (izključno) osebno/domačo rabo;

(d) organi za preprečevanje/preiskovanje/odkrivanje/pregon KD ali izvrševanje kaz. sankcij, varovanje grožnjam javne varnosti

(e) sodišča v „dejavnosti sojenja“.

GDPR in verske skupnosti

91. člen:„Kadar v državi članici v času začetka veljavnosti GDPR cerkve in verska združenja ali skupnosti uporabljajo celovita pravila v zvezi z varstvom posameznikov pri obdelavi, ta pravila lahko veljajo še naprej, **če se uskladijo z GDPR.**

Cerkve in verska združenja, ki uporabljajo celovita pravila v skladu s 1. odstavkom, **nadzira neodvisen nadzorni organ**, ki je lahko poseben organ, če izpolnjuje pogoje iz poglavja VI GDPR (=neodvisni nadzorni organ države članice).“

r. 55: „Obdelava OP s strani državnih organov za namen doseganja ciljev uradno priznanih verskih skupnosti, **ki so določeni z ustavnim pravom ali mednarodnim javnim pravom**, se izvaja zaradi **javnega interesa.“**

r. 165: „GDPR spoštuje in ne vpliva na status cerkva in verskih združenja ali skupnosti, ki ga imajo **na podlagi veljavnega ustavnega prava** v DČ.“

Zakon o verski svobodi

4. člen

(1) Cerkve in druge verske skupnosti delujejo ločeno od države in so svobodne v svojem organiziranju ter pri izvajanju svojih dejavnosti. Država ne sme posegati v njihovo organiziranje in delovanje, razen v primerih, določenih z zakonom.

6. člen

(2) Delovanje cerkva in drugih verskih skupnosti mora biti v skladu s pravnim redom Republike Slovenije in javnosti znano. ….Delovanje cerkve ali druge verske skupnosti ne sme nasprotovati morali in javnemu redu.

(3) Registrirane cerkve in druge verske skupnosti so pravne osebe zasebnega prava. Pravico do pridobitve lastne pravne osebnosti imajo tudi njihovi sestavni deli.

11. člen (varstvo osebnih podatkov)

Zbiranje in obdelava podatkov o verskem prepričanju posameznika sta dovoljena pod pogoji, ki so za obdelavo občutljivih osebnih podatkov določeni v zakonu, ki ureja varstvo osebnih podatkov.

Ozemeljska veljavnost GDPR

1. **po sedežu upravljavca ali obdelovalca v EU**, ne glede ali obdelava poteka v EU ali ne. (=četudi obdelave sploh ni v EU)

2. **posameznikov ki so v EU**, upravljavec/obdelovalec pa nima sedeža v EU, če so dejavnosti obdelave **povezane z**:

(a) nudenjem B/S posameznikom v EU, ne glede na (ne) plačilo *((*nudenje = uporaba jezika ali valute, ki se uporablja v 1 ali več DČ, možnost naročanja B/S v tem drugem jeziku, navedba strank ali uporabnikov, ki so v EU -- → vse to jasno pokaže, da želi upravljavec nuditi B/S posameznikom v EU))*

(b) spremljanjem njihovega vedenja v EU *((*npr. se mu sledi na internetu, profiliranje – Google Earth; vedenje/obnašanje mora biti v EU, ne glede na to od kje poteka spremljanje))*

3. če upravljavec nima sedeža v EU, ampak v kraju, kjer se pravo DČ **uporablja na podlagi MJP** (npr. v DKP DČ)

Zakonitost obdelave (6.čl.)

Obdelava je zakonita le, če je izpolnjen vsaj 1 od pogojev:

a.) osebna privolitev za 1 ali več določenih namenov

„Ni prostovoljna (in s tem veljavna podlaga za obdelavo OP), če obstaja očitno neravnotežje med posameznikom in upravljavcem, zlasti kadar je ta javni organ in je zato malo verjetno, da je bila dana prostovoljno in v vseh okoliščinah te specifične situacije.“

„Za privolitev se domneva, da ni dana prostovoljno, če:

- *ne dovoljuje ločenih privolitev za različne obdelave OP,*
- *je izvajanje pogodbe, vključno z zagotavljanjem storitve, pogojeno s privolitvijo, čeprav za tako izvajanje privolitev ne bi bila potrebna.“*

---------- →>
Popravek GDPR, 23.5.2018: „specifično“ →> konkretno,
„soglasje“ →> „strinjanje“

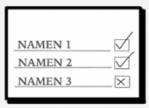
Veljavna PRIVOLITEV po Splošni uredbi

DOKAZLJIVA

Dokazljiva je privolitev, ki omogoča, da jo lahko upravljavec kadarkoli izkaže na zahtevo nadzornega organa.

PROSTOVOLJNA

Prostovoljna je privolitev, ki:
- zagotavlja resnično izbiro in nadzor,
- NE izhaja iz razmerja nesorazmerne moči med upravljavcem in posameznikom (delovno razmerje, javna oblast itd.),
- NI pogoj za sklenitev pogodbe,
- jo lahko posameznik kadarkoli umakne,
- ne prinaša škodljivih posledic za posameznika, če je ne poda ali če jo umakne.



SPECIFIČNA

Specifična je privolitev, ki je podana za konkretno opredeljen namen.

INFORMIRANA

Informirana je privolitev, ki jasno pove:
- kdo je upravljavec,
- za kakšen namen se bodo podatki obdelovali,
- kateri podatki se bodo obdelovali,
- da lahko posameznik privolitev kadarkoli umakne,
- da ima pravico, da zanj ne velja odločitev, ki temelji zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov,
- o morebitnih tveganjih pri prenosu osebnih podatkov v tretjo državo ali mednarodno organizacijo.

NEDVOUMNA

Nedvoumna je privolitev, ki je podana z izkazljivim in aktivnim dejanjem posameznika, ni domnevna.

Privolitev pridobiti PRED začetkom vsake obdelave + pridobivati NOVO, če se želi uvesti nov ali drug/spremenjen namen!

Pridobitev eksplicitne (izrecne) privolitve

Ni zahtevana vedno, pač pa npr. če obstaja velik rizik za data breach ali potreba po večji kontroli posameznika nad svojimi OP.

Izrecna privolitev pa vedno pri:

- posebnih vrstah OP (člen 9)
- prenosu OP v 3. države ali mednarodne organizacije, če ni drugih varovalk iz člena 49
- če odločanje temelji izključno na avtomatski obdelavi, vključno s profiliranjem (člen 22). -->>>>

Enostaven umik privolitve

Upravljavec zagotoviti umik privolitve enako enostavno kot dajanje in to kadarkoli – v isti obliki: klik, preko spletne strani, aplikacije, log-on račun, e-mail, vmesnik pri IoT) + brez škode: „po možnosti“ (?) brezplačno ali brez zniževanja nivoja storitve.

Primer slabe prakse: Prodaja kart po internetu in dajanje privolitev tudi za uporabo OP v marketinške namene, umik pa le po telefonu v času uradnih ur.

Obvestiti o pravici do umika + kako uresničevati to pravico in to oboje pred dajanjem privolitve (člen 7(3))!

Če umik privolitve, upravljavec ne more le enostavno „zamenjati pravno podlago“, pač pa mora biti vsaka sprememba pravne podlage posamezniku sporočena po členu 13 in 14 ter generalno zahtevo po transparentnosti.

(b) potrebna za izvajanje pogodbe ali za izvajanje ukrepov na zahtevo posameznika pred sklenitvijo pogodbe (ZVOP-1: čl. 9/3 in 10/2)

(c) potrebna za izpolnitev zakonske obveznosti upravljavca

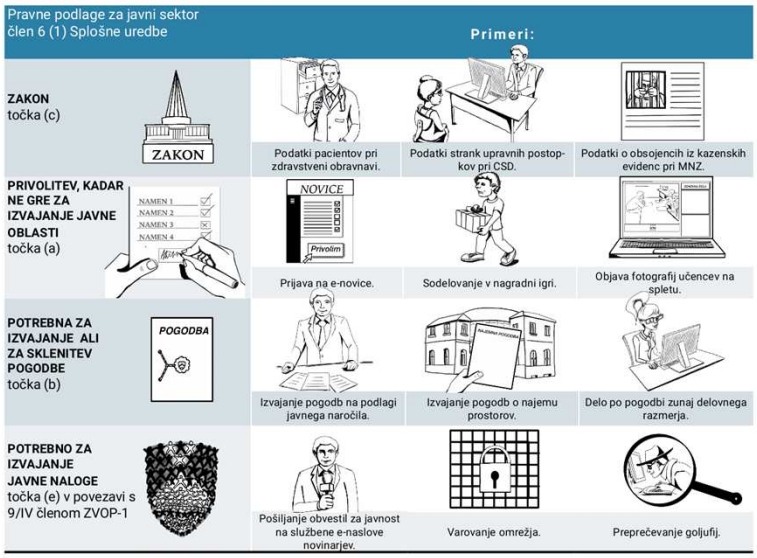
(d) potrebna za zaščito življenjskih interesov posameznika ali druge fizične osebe (včasih tudi v javnem interesu: humanitarni nameni, spremljanje epidemij, izredne humanitarne razmere, naravne nesreče ....) (ZVOP-1: 12. čl.)

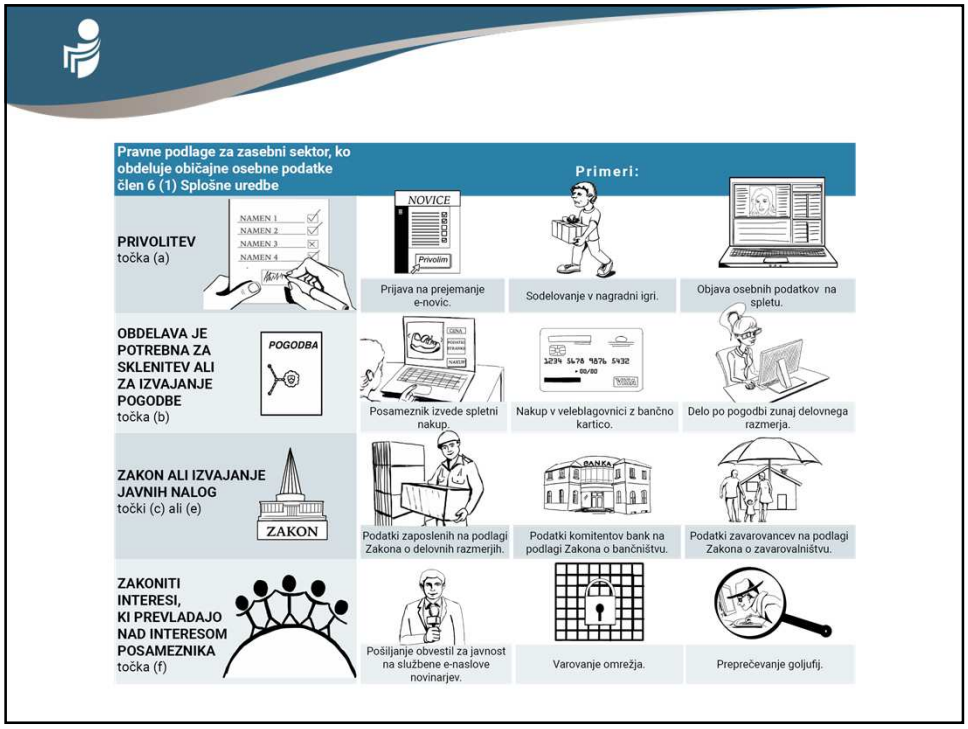
(e) potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu

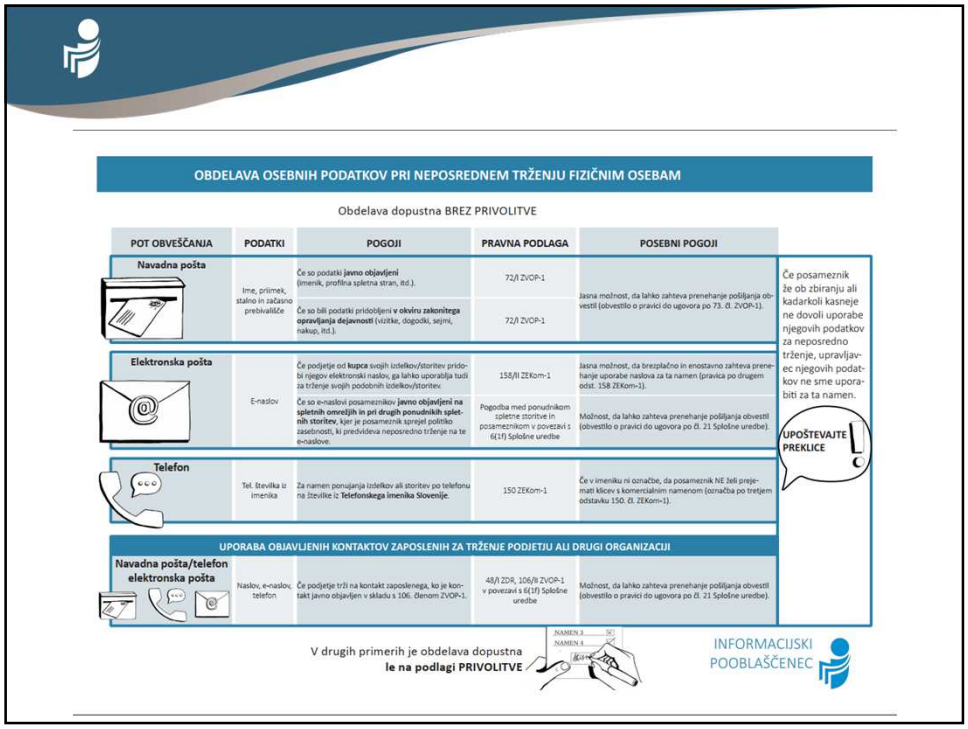
(f) potrebna zaradi zakonitih interesov za katere si prizadeva upravljavec ali 3. oseba, razen kadar prevladajo interesi ali pravice posameznika, ki zahtevajo VOP, zlasti otrok. (ZVOP-1: čl. 10/3)

Točka (f) se NE uporablja za javne organe pri njihovih nalogah, ker mora zakonodajalec z zakonom določiti podlago za obdelavo OP.

Zakoniti interes upravljavca pomeni tudi obdelava OP, če je nujno potrebna za preprečevanje zlorab, ali **za neposredno trženje!** ----→>>




Pravne podlage za zasebni sektor, ko obdeluje običajne osebne podatke člen 6 (1) Splošne uredbe
Primeri:
PRIVOLITEV
točka (a)
NAMEN 1
NAMEN 2
NAMEN 3
NAMEN 4
NOVICE
Privolim
Prijava na prejemanje e-novic.
Sodelovanje v nagradni igri.
Objava osebnih podatkov na spletu.
OBDELAVA JE POTREBNA ZA SKLENITEV ALI ZA IZVAJANJE POGODBE
točka (b)
POGODBA
Posameznik izvede spletni nakup.
Nakup v veleblagovnici z bančno kartico.
Delo po pogodbi zunaj delovnega razmerja.
ZAKON ALI IZVAJANJE JAVNIH NALOG
točki (c) ali (e)
ZAKON
Podatki zaposlenih na podlagi Zakona o delovnih razmerjih.
BANKA
Podatki komitentov bank na podlagi Zakona o bančništvu.
Podatki zavarovancev na podlagi Zakona o zavarovalništvu.
ZAKONITI INTERESI, KI PREVLADAJO NAD INTERESOM POSAMEZNIKA
točka (f)
Pošiljanje obvestil za javnost na službene e-naslove novinarjev.
Varovanje omrežja.
Preprečevanje goljufij.


OBDELAVA OSEBNIH PODATKOV PRI NEPOSREDNEM TRŽENJU FIZIČNIM OSEBAM
Obdelava dopustna BREZ PRIVOLITVE
POT OBVEŠČANJA
PODATKI
POGOJI
PRAVNA PODLAGA
POSEBNI POGOJI
Navadna pošta
Ime, priimek, stalno in začasno prebivališče
Če so podatki javno objavljeni (imenik, profilna spletna stran, itd.).
72/I ZVOP-1
Jasna možnost, da lahko zahteva prenehanje pošiljanja obvestil (obvestilo o pravici do ugovora po 73. čl. ZVOP-1).
Če so bili podatki pridobljeni v okviru zakonitega opravljanja dejavnosti (vizitke, dogodki, sejmi, nakup, itd.).
72/I ZVOP-1
Elektronska pošta
E-naslov
Če podjetje od kupca svojih izdelkov/storitev pridobi njegov elektronski naslov, ga lahko uporablja tudi za trženje svojih podobnih izdelkov/storitev.
158/II ZEKom-1
Jasna možnost, da brezplačno in enostavno zahteva prenehanje uporabe naslova za ta namen (pravica po drugem odst. 158 ZEKom-1).
Če so e-naslovi posameznikov javno objavljeni na spletnih omrežjih in pri drugih ponudnikih spletnih storitev, kjer je posameznik sprejel politiko zasebnosti, ki predvideva neposredno trženje na te e-naslove.
Pogodba med ponudnikom spletne storitve in posameznikom v povezavi s 6(1f) Splošne uredbe
Možnost, da lahko zahteva prenehanje pošiljanja obvestil (obvestilo o pravici do ugovora po čl. 21 Splošne uredbe).
Telefon
Tel. številka iz imenika
Za namen ponujanja izdelkov ali storitev po telefonu na številke iz Telefonskega imenika Slovenije.
150 ZEKom-1
Če v imeniku ni označbe, da posameznik NE želi prejemati klicev s komercialnim namenom (označba po tretjem odstavku 150. čl. ZEKom-1).
UPORABA OBJAVLJENIH KONTAKTOV ZAPOSLENIH ZA TRŽENJE PODJETJU ALI DRUGI ORGANIZACIJI
Navadna pošta/telefon elektronska pošta
Naslov, e-naslov, telefon
Če podjetje tži na kontakt zaposlenega, ko je kontakt javno objavljen v skladu s 106. členom ZVOP-1.
48/I ZDR, 106/II ZVOP-1 v povezavi s 6(1f) Splošne uredbe
Možnost, da lahko zahteva prenehanje pošiljanja obvestil (obvestilo o pravici do ugovora po čl. 21 Splošne uredbe).
Če posamezniki že ob zbiranju ali kadarkoli kasneje ne dovoli uporabe njegovih podatkov za neposredno trženje, upravljavec njegovih podatkov ne sme uporabiti za ta namen.
UPOŠTEVAJTE PREKLICE
V drugih primerih je obdelava dopustna le na podlagi PRIVOLITVE
INFORMACIJSKI POOBLAŠČENEC

Obdelava posebnih vrst OP (1. odst. 9. čl.)

Prepovedana je obdelava **OP, ki razkrivajo:**

- rasno ali etnično poreklo
- politično mnenje
- versko ali filozofsko prepričanje
- članstvo v sindikatu

Prepovedana je obdelava:

- genetskih podatkov
- biometričnih podatkov za namene edinstvene identifikacije
- podatkov v zvezi z zdravjem
- podatkov v zvezi s spolnim življenjem ali spolno usmerjenostjo

----------→> **lahko pa:**

(2., 4. odst. 9. čl.) – prepoved obdelave pa ne velja, če:

a) posameznik **izrecno privoli** v obdelavo za določen namen, razen če pravo EU/DČ prepoveduje ta odstop

b) P in D iz del. prava, soc. varnosti in soc. varstva (če to dovoljuje pravo EU ali DČ ali kolektivna pogodba)

c) za **zaščito življenjskih interesov**, če fizično ali pravno ni sposoben dati privolitve

d) znotraj neprofitnih subjektov s političnim, filozofskim, verskim ali sindikalnim ciljem o svojih sedanjih ali bivših članih ali oseb v rednem stiku

e) posameznik OP sam objavi

f) za **pravne zahtevke ali ko sodišča** izvajajo sodno pristojnost

g) bistveni javni interes po pravu EU ali DČ, sorazmerno s ciljem in spoštovanjem VOP ------ >>>>

h.) **potrebno za preventivno medicino ali medicino dela, oceno delovne sposobnosti, zdravstveno diagnozo**, zdravstveno ali socialno oskrbo, **zdravljenje, upravljanje sistemov in storitev zdravstvenega** ali socialnega varstva po pravu EU ali DČ, po pogodbi z zdravstvenim delavcem - le strokovnjaki z obveznostjo varovanja poklicne skrivnosti

i.) zaradi javnega interesa na področju **javnega zdravja** po pravu EU ali DČ (npr. zaščita pred epidemijami, zagotovitev visokega standarda zdravstvenega varstva, zdravil, medicinskih pripomočkov!)

j.) za namene arhiviranja v javnem interesu, znanstveno- ali zgodovinsko-raziskovalne ali statistične namene po pravu EU/DČ

Ključni členi ustave RS:

14. člen (enakost pred zakonom)

V Sloveniji so vsakomur zagotovljene enake človekove pravice in temeljne svoboščine, ne glede na narodnost, raso, spol, jezik, vero, politično ali drugo prepričanje, …. ali katerokoli drugo osebno okoliščino. Vsi so pred zakonom enaki.

41. člen (svoboda vesti)

Izpovedovanje vere in drugih opredelitev v zasebnem in javnem življenju je svobodno.

Nihče se ni dolžan opredeliti glede svojega verskega ali drugega prepričanja.

38. člen (varstvo osebnih podatkov)

Zagotovljeno je varstvo OP. Prepovedana je uporaba OP v nasprotju z namenom njihovega zbiranja.

Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti OP določa zakon.

Vsakdo ima pravico seznaniti se z zbranimi OP, ki se nanašajo nanj in pravico do sodnega varstva ob njihovi zlorabi.

24. člen GDPR - Odgovornost upravljavca

Ob upoštevanju **narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za TČP**, ki se razlikujejo po verjetnosti in resnosti, upravljavec izvede ustrezne **tehnične in organizacijske ukrepe**, da **zagotovi** in je **zmožen dokazati, da obdelava poteka v skladu z GDPR.**

Ti ukrepi se **pregledajo in dopolnijo**, kjer je to potrebno.

Kadar je to sorazmerno glede na dejavnosti obdelave, ukrepi vključujejo **izvajanje ustreznih politik** za varstvo podatkov s strani upravljavca.

Spoštovanje odobrenih **kodeksov ravnanja** ali izvajanje **odobrenega mehanizma potrjevanja** se lahko uporabi za **dokazovanje izpolnjevanja obveznosti upravljavca**. --→> **POSAMEZNI INSTITUTI**

30. člen - Evidenca dejavnosti obdelave („katalogi“)

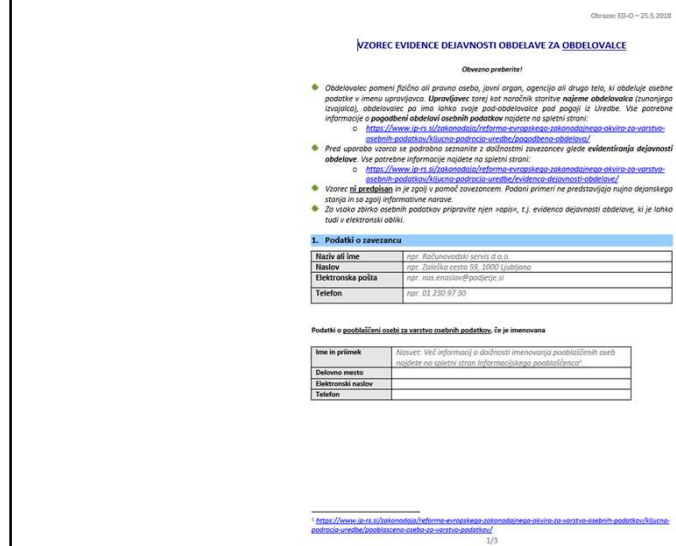
Upravljavci, **obdelovalci in njihov predstavniki**, kadar obstajajo, vodijo evidenco vseh vrst dejavnosti obdelave.

Evidenca predstavlja **opis zbirk**, ki jih vodijo (vsebino zbirk, namene, pravne podlage, varnostne postopke…).

Register zbirk (prijava zbirk) OP pri IP **se ukinja, katalogi pa ostajajo!**

- Evidence so v **pisni**, **vključno v elektronski obliki**.
- **Nadzorni organ ima na zahtevo dostop do evidenc**.
- Izjema: zaposluje **manj kot 250 oseb**, razen če *visoka tveganja ali *ni občasne obdelave, ali *posebne vrste podatkov.

Vzorec evidence dejavnosti obdelav – ZA OBDELOVALCE



Obrazec ED-O – 25.5.2018

VZOREC EVIDENCE DEJAVNOSTI OBDELAVE ZA OBDELOVALCE

Obvezno preberite!

- *Obdelovalec pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca. **Upravljavec** torej kot naročnik storitve **najeme obdelovalca** (zunanjega izvajalca), obdelovalec pa ima lahko svoje pod-obdelovalce pod pogoji iz Uredbe. Vse potrebne informacije o **pogodbeni obdelavi osebnih podatkov** najdete na spletni strani:*
  - *https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/pogodbena-obdelava/*
- *Pred uporabo vzorca se podrobno seznanite z določbami zavezanceve glede **evidentiranja dejavnosti obdelave**. Vse potrebne informacije najdete na spletni strani:*
  - *https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/evidenca-dejavnosti-obdelave/*
- *Vzorec **ni predpisan** in je zgolj v pomoč zavezancem. Podani primeri ne predstavljajo nujno dejanskega stanja in so zgolj informativne narave.*
- *Za vsako zbirko osebnih podatkov pripravite njen »opis«, t.j. evidenco dejavnosti obdelave, ki je lahko tudi v elektronski obliki.*

1. Podatki o zavezancu

Naziv ali ime	*npr. Računovodski servis d.o.o.*
Naslov	*npr. Zaloška cesta 59, 1000 Ljubljana*
Elektronska pošta	*npr. nas.enaslov@podjetje.si*
Telefon	*npr. 01 230 97 30*

Podatki o pooblaščeni osebi za varstvo osebnih podatkov, če je imenovana

Ime in priimek	*Nasvet: Več informacij o določitvi imenovanja pooblaščenih oseb najdete na spletni strani Informacijskega pooblaščenca[1].*
Delovno mesto	
Elektronski naslov	
Telefon	

[1] https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/pooblascena-oseba-za-varstvo-podatkov/

1/3

Vzorec evidence dejavnosti obdelav – ZA UPRAVLJAVCE

2. Podatki o zbirki osebnih podatkov

Naziv zbirke	*Nasvet: Zbirke osebnih podatkov najlažje ločite, če so zanje predpisane določene zakonske podlage (npr. Evidenca delovnega časa), sicer pa jih smiselno ločite predvsem po namenih uporabe. Podjetja imajo v povprečju med 5 in 50 zbirk osebnih podatkov, ki jih vodijo na različnih pravnih podlagah (npr. zaradi zahtev delovno-pravne zakonodaje, na podlagi privolitve posameznika itd.), v javnem sektorju pa praviloma zbirke osebnih podatkov določa zakonodaja. Isti osebni podatki se lahko nahajajo tudi v različnih zbirkah (npr. ime in priimek zaposlenega, ki je hkrati tudi imetnik kartice zvestobe).* *Deloma si lahko pomagate tudi s primeri zbirk, ki so jih zavezanci po ZVOP-1 prijavljali v register zbirk do 25.5.2018:* *https://www.ip-rs.si/varstvo-osebnih-podatkov/register-zbirk/* *Primeri:* • *Osebnih podatki zaposlenih, ki se obdelujejo ob uporabi službenih sredstev* • *Evidenca delovnega časa* • *Evidenca videonadzora* • *Zbirka podatkov o članih kluba zvestobe*
Namen obdelave osebnih podatkov	*Nasvet: Namene obdelave osebnih podatkov določa bodisi zakonodaja bodisi upravljavec sam. Posamezna zbirka osebnih podatkov ima lahko en ali več namenov (pri klubu zvestobe so verjetni namene izvajanje neposrednega trženja, izvajanje profiliranja, prilagajanje ponudbe itd.)* *npr. Urejanje pravic in obveznosti javnih uslužbencev iz delovnega razmerij, izvedba novoletnega obdarovanja otrok zaposlenih, pošiljanje e-navic podjetja ...*
Kategorije posameznikov, na katere se nanašajo osebni podatki v zbirki	*Nasvet: Premislite, na katere posameznike se nanašajo podatki. Lahko gre za zaposlene, pripravnike, stranke, komitente, učence, zavarovance, obiskovalce itd.*
Vrste osebnih podatkov v zbirki	*Nasvet: Pomislite, kateri vse vrste osebnih podatkov imate. Naštejte vse vrste osebnih podatkov, ki se hranijo v zbirki in ne pozabite, da se osebni podatki nanašajo na določljive posameznike.* *Primeri:* *Na primeru zbirke «Osebni podatki zaposlenih, ki se obdelujejo ob uporabi službenih sredstev», ki jo organizacije pogosto spregledajo, preverite, kaj se*

EVIDENCA UPORABE VIDEONADZORNEGA SISTEMA

Vzorec informativne narave.

EVIDENCA UPORABE VIDEONADZORNEGA SISTEMA

Naziv in naslov upravljavca: _____

Objekt, kjer se izvaja videonadzor: _____

Pooblaščene osebe (osebe, ki lahko obdelujejo oz. imajo dostop do zbirke videoposnetkov):_____

Odgovorna oseba za zbirko videoposnetkov: _____

Videonadzor uveden s sklepom št. _____ z dne _____

OPOZORILO

- Vpogled v posnetke snemalnika, presnemavanje, brisanje in ostala obdelava videoposnetkov je dovoljena izključno pooblaščenim osebam v skladu z veljavno zakonodajo in internimi pravili (oziroma zunanjim pogodbenim izvajalcem po nalogu pooblaščene osebe).
- Vsak dostop, uporaba, kopiranje ali druga vrsta obdelave videoposnetkov mora biti zabeležena.
- Evidenca uporabe videonadzornega sistema se hrani skladno z določbami 24. člena Zakona o varstvu osebnih podatkov.

SEZNAM LISTOV DNEVNIKA:

List 1 Seznam kamer
List 2 Evidenca prekinitev snemanja
List 3 Evidenca uporabe videoposnetkov
List 4 Evidenca posredovanja videoposnetkov
List 5 Evidenca brisanja videoposnetkov oziroma uničenja medijev

Na Listu 1 se vodi ažuren seznam kamer, ki vsebuje oznake in področje pokrivanja posamezne kamere.
Na Listu 2 se evidentirajo prekinitve snemanja.
Na Listu 3 se evidentirajo vse uporabe oziroma obdelave videoposnetkov (pregledovanje, kopiranje).
Na Listu 4 se evidentirajo vsa posredovanja videoposnetkov zunanjim uporabnikom.
Na Listu 5 se evidentira brisanje oziroma uničenje posnetkov, če je do tega prišlo pred potekom roka hrambe.

Sodbe sodišča EU

1.) Bodil Linquist v. EK: ga. Bodil Linquist je za potrebe svoje cerkve (Švedska) naredila spisek sodelavcev z njihovimi OP (ime, tel. št., podatke o zdravstvenem stanju sodelavca) in ga dala na internet.

Avtomatska obdelava OP + posredovanje OP v 3. države, četudi švedski strežnik, saj pri uporabi interneta obstaja možnost, da OP dobi oseba iz 3. države.

2.) Člani skupnosti Jehovih prič (C-25/17, 10.7.2018)

Finski DPA je leta 2013 članom skupnosti Jehovih prič prepovedala zbiranje in obdelavo OP med oznanjevanjem od vrat do vrat, saj niso bili spoštovani zakonski pogoji za obdelavo OP. Delali so zapiske o osebah, beležili imena+priimke, podatke o njihovem verskem prepričanju in družinskih razmerah, posledično naj bi župnije izdelale seznam oseb, ki so izrazile željo, da jih člani Jehovih prič ne bi več obiskovali na domu →> **pritožba→ Finsko upravno sodišče**: odpravilo odločbo DPA, ker da verska skupnost ni upravljavec OP →> DPA izpodbija na **vrhovnem upravnem sodišču** →> to na SEU naslovi predlog za predhodno odločanje.

SEU: ne gre za popolnoma domačo ali osebno rabo,

gre za zbirko OP, verska skupnost je upravljavec OP.

Pooblaščena oseba za VOP

Upravljavec/obdelovalec imenujeta DPO, če:

1.) obdelavo izvaja javni organ;

2.) je obdelava OP njuna temeljna dejavnost, kjer je zaradi narave obsega ali namenov obdelave, treba posameznike redno in sistematično obsežno spremljati (npr. direktni marketing, segmentiranje, analitika….);

3.) njune temeljne dejavnosti zajemajo obsežno obdelavo posebnih vrst OP (t.i. „občutljivi OP“) in OP v zvezi s KE/PE

Lahko *en DPO za (pod)družbe/enote organa, * več organov enega, *zaposlen, *najet.

Upravljavec kontaktne podatke DPO objavi + sporoči IP.

Ustrezno strokovno znanje in poklicne odlike - npr. integriteto.

Ocena: 75.000 DPO-jev v EU

Naloge:

- obvešča upravljavca+ svetuje o VOP in zahtevah GDPR,
- spremlja skladnosti obdelave OP po GDPR idr. predpisi,
- izvaja izobraževanja za zaposlene in sodeluje pri revizijah,
- sodeluje z IP,
- kontaktna točka glede obdelave OP.

„TEMELJNE DEJAVNOSTI UPRAVLJAVCA“

R97: So **osnovne dejavnosti (ne obdelava OP kot postranska dejavnost)**. So **ključne dejavnosti, potrebne za dosego ciljev** upravljavca/obdelovalca.

- Npr.: temeljna dejavnost bolnišnice je zagotavljanje zdravstvenega varstva, česar **bi ne more varno in učinkovito zagotavljati brez obdelave OP**.
- Varnostna družba **nadzoruje več nakupovalnih centrov in javnih prostorov**. Nadzor je temeljna dejavnost družbe, neločljivo povezana z obdelavo OP.
- HR in IT **so podporne funkcije in ne temeljne dejavnosti.**

29

„VELIK OBSEG“

- R91: Obd*elava **precejšnje količine OP** na regionalni, nacionalni, nadnacionalni ravni in **bi lahko vplivala na veliko število posameznikov**, na katere se nanašajo OP ter za katere je **verjetno, da bodo povzročila veliko tveganje**.*
- Izpostavljeno: **NE**, če *obdelava OP pacientov/strank s strani **posameznega zdravnika, drugega zdravstvenega delavca ali odvetnika**“.*

Ni mogoče navesti točnega števila, ki bi veljalo v vseh primerih.

29 WP kriteriji za „obsežno obdelavo“:

- **število** posameznikov - število ali **delež** ustrezne populacije;
- **količina podatkov** in/ali **obseg** različnih podatkovnih postavk;
- **trajanje ali stalnost** dejavnosti obdelave in
- **geografska razsežnost** dejavnosti obdelave.

30

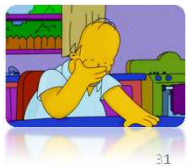
„REDNO IN SISTEMATIČNO SPREMLJANJE“

R24: „**spremljanje vedenja“** = **vse oblike sledenja posameznikom in oblikovanja njihovega profila** na internetu, tudi zaradi oglaševanja na podlagi vedenjskih vzorcev.

29 WP„**redno**“: **poteka v določenih intervalih in določenem obdobju ali se izvaja večkrat ali se ponavlja ob določenem času ali** se izvaja **stalno ali periodično**.

„**sistematično**“: **vnaprej določeno, organizirano ali metodično ali** poteka kot del splošnega načrta zbiranja OP, se izvaja kot **del strategije**

---------->



31

Dejavnosti, ki so lahko **redno in sistematično spremljanje:**

- upravljanje **telekomunikacijskega omrežja**,
- zagotavljanje **telekomunikacijskih storitev**,
- **dejavnosti trženja, ki temeljijo na *(več kot le kontaktnih)* OP**,
- **oblikovanje profilov** in točkovanje za namene ocene tveganja (npr. zaradi kreditnega točkovanja, določitve zavarovalnih premij, preprečevanja goljufij, odkrivanja pranja denarja),
- **sledenje** geografskemu položaju, npr. z mobilnimi napravami,
- **programi zvestobe**,
- oglaševanje na podlagi **vedenjskih vzorcev**,
- spremljanje podatkov o **počutju, telesni pripravljenosti in zdravju** prek nosljivih naprav („wearables“),
- (**obsežni) videonadzorni sistemi**, **povezane naprave, npr. pametni števci, pametni avtomobili, povezani sistemi za avtomatizacijo doma itd.**

32

Varovan položaj DPO

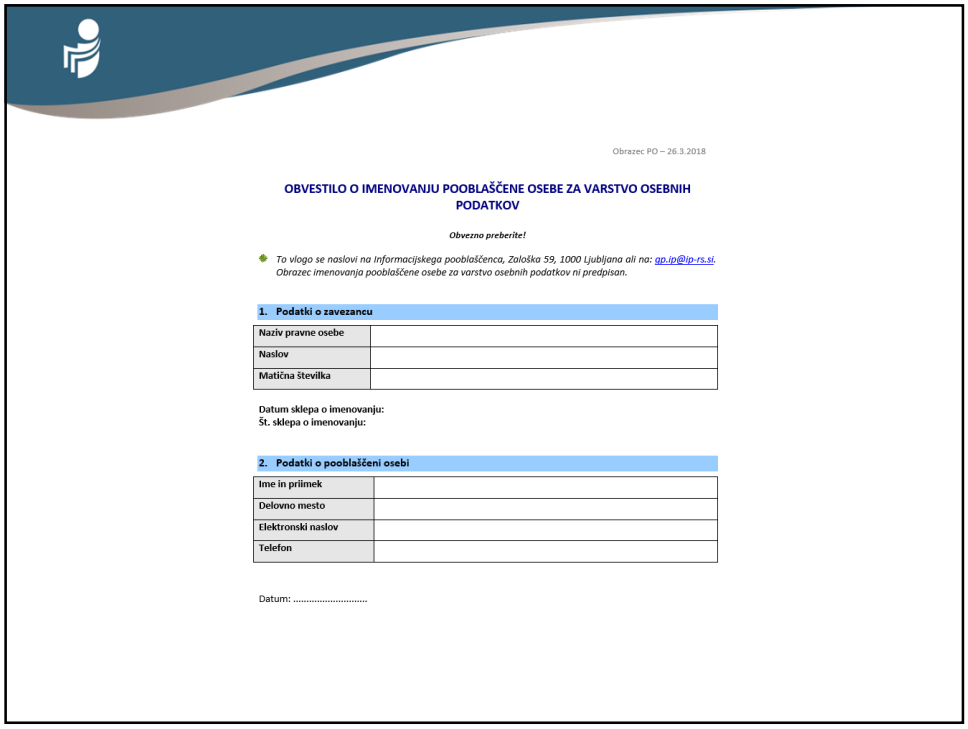
1. **ustrezno + pravočasno vključen** v vse zadeve VOP,
2. zagotovljeno**: *sredstva,** *dostop do **OP in dejanj obdelave**, ***ohranjanje strokovnega znanja,**
3. pri opravljanju nalog **ne sme prejemati nobenih navodil,**
4. **ne razrešen** ali **kaznovan** zaradi opravljanja nalog,
5. **neposredno poroča najvišji upravi** upravljavca/obdelovalca,
6. p**osamezniki** lahko **z DPO stopijo v stik** glede vseh vprašanj glede obdelave njihovih OP, in uresničevanjem njihovih pravic,
7. dolžnost **varovati skrivnost ali zaupnost** po pravu EU ali DČ.
8. **druge naloge,** če upravljavec zagotovi, da **ni nasprotja interesov.**

33

Nasprotje interesov (38. člen)

- DPO ne sme imeti položaja, kjer **določa namene + sredstva obdelave**
- **NE: položaji višjega vodstva (izvršni direktor, operativni direktor, finančni direktor, vodja interne 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.

34



Obrazec PO – 26.3.2018

OBVESTILO O IMENOVANJU POOBLAŠČENE OSEBE ZA VARSTVO OSEBNIH PODATKOV

Obvezno preberite!

- *To vlogo se naslovi na Informacijskega pooblaščenca, Zaloška 59, 1000 Ljubljana ali na: gp.ip@ip-rs.si. Obrazec imenovanja pooblaščene osebe za varstvo osebnih podatkov ni predpisan.*

1. Podatki o zavezancu

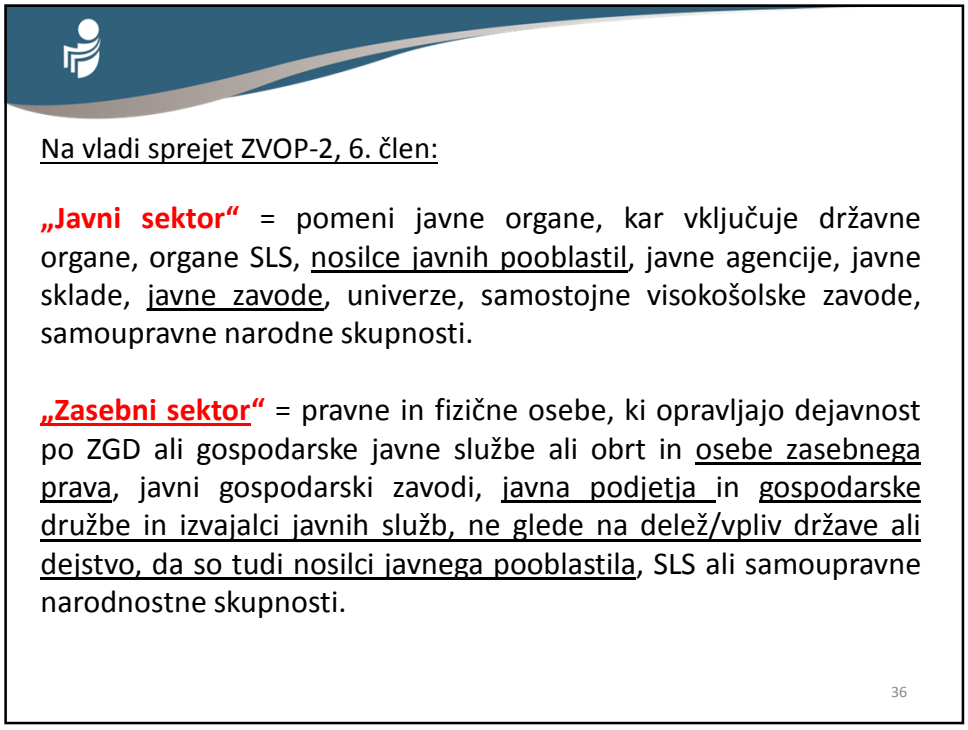
Naziv pravne osebe	
Naslov	
Matična številka	

Datum sklepa o imenovanju:
Št. sklepa o imenovanju:

2. Podatki o pooblaščeni osebi

Ime in priimek	
Delovno mesto	
Elektronski naslov	
Telefon	

Datum: .....



Na vladi sprejet ZVOP-2, 6. člen:

„Javni sektor“ = pomeni javne organe, kar vključuje državne organe, organe SLS, nosilce javnih pooblastil, javne agencije, javne sklade, javne zavode, univerze, samostojne visokošolske zavode, samoupravne narodne skupnosti.

„Zasebni sektor“ = pravne in fizične osebe, ki opravljajo dejavnost po ZGD ali gospodarske javne službe ali obrt in osebe zasebnega prava, javni gospodarski zavodi, javna podjetja in gospodarske družbe in izvajalci javnih služb, ne glede na delež/vpliv države ali dejstvo, da so tudi nosilci javnega pooblastila, SLS ali samoupravne narodnostne skupnosti.

36

Ocena učinka v zvezi z varstvom podatkov *PIA* *(35. čl)*

1. Če je možno, da bi lahko obdelava, zlasti z novimi tehnologijami, ob upoštevanju narave/obsega/okoliščin/namenov obdelave povzročila **veliko tveganje za TČP**, upravljavec **pred obdelavo opravi PIA-o** predvidenih dejanj obdelave na VOP.

2. Upravljavec pri izvedbi ocene **za mnenje zaprosi DPO**.

3. Ocena učinka se zahteva zlasti v primeru:

a) **sistematičnega in obsežnega vrednotenja osebnih vidikov,** ki temelji na **avtomatizirani obdelavi**, vključno s **profiliranjem**, in je osnova za odločitve, ki imajo pravne učinke na posameznika ali nanj znatno vplivajo;

b) **obsežne obdelave posebnih vrst podatkov** ali OP v zvezi s KE/PE;

c) **obsežnega sistematičnega spremljanja javno dostopnega območja**. -->

37

PIA zajema vsaj:

a) **sistematičen opis dejanj + namenov** obdelave,

b) oceno **potrebnosti** in **sorazmernosti** obdelave glede na **namen,**

c) **oceno tveganj** za TČP,

d) **ukrepe za obravnavanje tveganj**, **zaščitne in varnostne ukrepe** ter mehanizme za zagotavljanje VOP in za **dokazovanje skladnosti** s to uredbo, ob upoštevanju pravic in zakonitih interesov posameznikov ter drugih oseb, ki jih to zadeva.

(analiza tveganj na področju VOP)

38

Primer PIA-e:

Obrazec ocene učinkov v zvezi z VOP

(priloga k Uredbi o brezpilotnih letalnikih – poslati IP)

Nabor OP, ki bodo zajeti, shranjeni ali drugače obdelani

Fotografije posameznikov	Sistematičen nadzor javnih površin	Posebne vrste osebnih podatkov (občutljivi osebni podatki)	
Video posnetki posameznikov	RFID oznake	Podatki o verski pripadnosti posameznikov	Podatki o članstvu v sindikatu
Avdio posnetki posameznikov	Podatki o električnih, vodnih ali plinskih odjemnih mestih	Podatki o zdravstvenem stanju posameznikov	Genetski podatki
Registrske tablice avtomobilov ali drugih vozil posameznikov	Lokacijski podatki posameznikov	Podatki o rasnem ali etničnem poreklu	Biometrični podatki za namene avtentikacije ali identifikacije posameznika
Identifikatorji naprav posameznikov (*obkroži ustrezno*): IMEI/IMSI, bluetooth, IP, MAC naslovi, SSID ipd.	Podatki o gibanju posameznikov (npr. podatki o lokacijah in hitrosti vožnje, potovalnih vzorcih)	Podatki o političnem prepričanju	Podatki v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo
Drugi podatki o posameznikih (*navedi):* _____ _____		Podatki o verskem ali filozofskem prepričanju	

ali

❑Ne bomo zajemali, shranjevali ali kakor koli drugače obdelovali nobenih osebnih podatkov.

Sorazmernost - najmanjši obseg podatkov

Za zmanjšanje obsega zbranih OP bomo uporabili naslednje postopke in ukrepe (*označi ustrezno*):

- ❑ prilagajanje urnikov letenja in poti (npr. izogibanje zasebnim zemljiščem in prostorom, terminom, ko je pričakovati več oseb);
- ❑ izbor samo nujnih senzorjev (npr. brez zajema videoposnetkov, če to ni potrebno);
- ❑ časovno omejevanje zajema podatkov (npr. šele ob prihodu na ciljno lokacijo oz. ob opravljanju naloge in ne ves čas letenja);
- ❑ uporaba tehnologij za anonimizacijo (npr. zameglitev obrazov, registrskih tablic);
- ❑ sprotno in naknadno pregledovanje/urejanje posnetkov in zajetih podatkov ter čimprejšnje naknadno izločanje oz. brisanje nepotrebnih OP.

Kako se najbolje izognemo kršitvam?

- razvijati PIA (Privacy Impact Assessment) pred uvedbo vsakega posega v zasebnost (zlasti ob novem tehničnem sredstvu, aplikaciji)

- Razvoj in evalvacija novih varnostnih tehnologij:

a.) **SIA** = Surveillance Impact Assesment (impacts: privacy, legal, psychological, ethical, financial)

b.) **DESSI** = Decision Support System on security Investments (kaj je problem, učinkovite rešitve zanj, varnost + in -, družbena sprejemljivost, socialna implikacija, etični vidik, stroški, pravni vidik)

c.) **STEFI** = Security, Trust, Efficiency, Freedom infringement **(CRISP)**

Predhodno posvetovanje z IP (36. čl.)

Če **iz ocene učinka izhaja**, da bo obdelava OP **veliko tveganje**, **se upravljavec predhodno posvetuje z IP**.

Pri posvetovanju mora upravljavec IP **predložiti**:

- dolžnosti upravljavca, skupnih upravljavcev in obdelovalcev,
- namene in sredstva predvidene obdelave,
- ukrepe in zaščitne ukrepe za zaščito TČP posameznikov,
- kontaktne podatke pooblaščene osebe za VOP,
- oceno učinka v zvezi z varstvom podatkov,
- vsakršne druge informacije, ki jih zahteva IP.

„Pod"-obdelovalec (28. čl.)

1. Če obdelava v imenu upravljavca, ta sodeluje le z obdelovalci, ki **zagotovijo zadostna jamstva za izvedbo ustreznih tehničnih in organizacijskih ukrepov** (obdelava izpolnjuje zahteve GDPR + zagotavlja varstvo pravic posameznika).

2. **Obdelovalec lahko zaposli drugega obdelovalca le ob predhodnem posebnem ali splošnem pisnem dovoljenju upravljavca –** mu **omogoči, da nasprotuje.**

3. Podpišeta **pogodbo ali drug pravni akt: obveznosti obdelovalca**, **vsebino in trajanje obdelave**, **naravo** in **namen** obdelave, **vrste OP**, **kategorije posameznikov OP**, **P+D upravljavca**.

((Pozor: kadar pogodbeni obdelovalec **v tujini**: iznos OP v 3. države; Privacy Shield))

44

Pravice posameznika (12. čl. in nasl.)

Upravljavec mora **zagotoviti posamezniku informacije o njegovih pravicah in sprejetih ukrepih** (glede potrditve obdelave, popravka, RTBF, omejitve obdelave, Data portability, ugovora, ugovora zoper avtomatizirano odločitev) v jedrnati, pregledni, razumljivi in lahko dostopni obliki + jasnem in preprostem **jeziku**, pisno ali v e-obliki. Na zahtevo posameznika lahko ustno, a le če se identiteta posameznika izkaže kako drugače.

Zahteve glede pravic uresničuje brez odlašanja v 1 mesecu.
+ dodatno **največ 2 meseca** ob upoštevanju kompleksnosti in števila zahtev, a ga mora v 1 mesecu obvestiti o podaljšanju in razlogih.

Če zahtevo predloži z **e-sredstvi, zagotovi** odgovor, če je mogoče, tudi z e-sredstvi. Možnosti vložitve **pritožbe pri IP** in **možnosti uveljavljanja pravnih sredstev.**

45

Vse informacije se zagotovijo **brezplačno**! (ne več zaračunavanja po Pravilniku o materialnih stroških!) -→ vendar:

Če pa so **zahteve očitno neutemeljene ali pretirane** zlasti **ponavljajoče**, **lahko upravljavec (=šikanoznost)**:

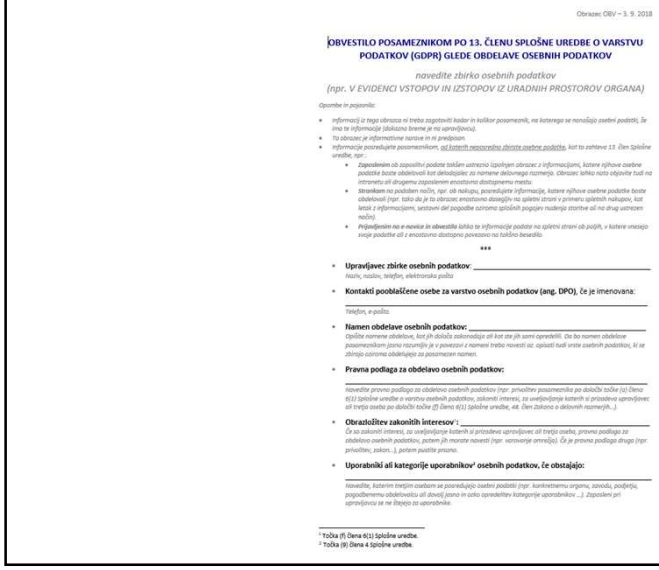
a) **zaračuna razumno pristojbino**, pri čemer upošteva upravne stroške posredovanja informacij ali sporočila ali izvajanja zahtevanega ukrepa,

b) **zavrne ukrepanje** v zvezi z zahtevo.

Upravljavec nosi dokazno breme!

46

OBVESTILO POSAMEZNIKOM PO 13. ČLENU SPLOŠNE UREDBE O VARSTVU PODATKOV (GDPR) GLEDE OBDELAVE OSEBNIH PODATKOV



Obrazec OBV – 3. 9. 2018

OBVESTILO POSAMEZNIKOM PO 13. ČLENU SPLOŠNE UREDBE O VARSTVU PODATKOV (GDPR) GLEDE OBDELAVE OSEBNIH PODATKOV

navedite zbirko osebnih podatkov
(npr. V EVIDENCI VSTOPOV IN IZSTOPOV IZ URADNIH PROSTOROV ORGANA)

Opombe in pojasnila:

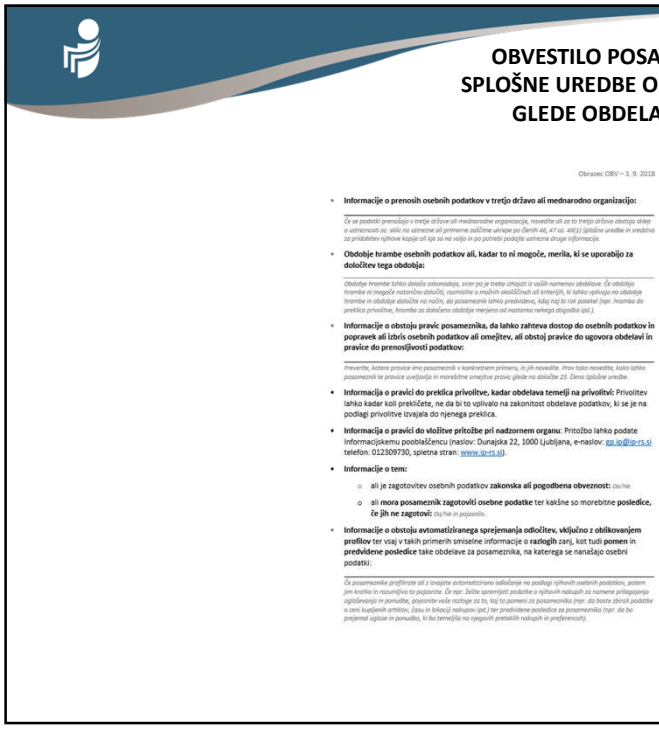
- *Informacij iz tega obrazca ni treba zagotoviti kadar in kolikor posameznik, na katerega se nanašajo osebni podatki, že ima te informacije (dokazno breme je na upravljavcu).*
- *Ta obrazec je informativne narave in ni predpisan.*
- *Informacije posredujete posameznikom, od katerih neposredno zbirate osebne podatke, kot to zahteva 13. člen Splošne uredbe, npr.:*
  - *Zaposlenim ob zaposlitvi podate takšen ustrezno izpolnjen obrazec z informacijami, katere njihove osebne podatke boste obdelovali kot delodajalec za namene delovnega razmerja. Obrazec lahko nato objavite tudi na intranetu ali drugemu zaposlenim enostavno dostopnemu mestu.*
  - *Strankam na poddelen način, npr. ob nakupu, posredujete informacije, katere njihove osebne podatke boste obdelovali (npr. tako da je ta obrazec enostavno dosegljiv na spletni strani v primeru spletnih nakupov, kot letak z informacijami, sestavni del pogodbe oziroma splošnih pogojev rudenja storitve ali na drug ustrezen način).*
  - *Prijavljenim na e-novice in obvestila lahko te informacije podate na spletni strani ob pošiji, v katere vnesejo svoje podatke ali z enostavno dostopno povezavo na tiskano besedilo.*

***

- **Upravljavec zbirke osebnih podatkov:** _____
  Naziv, naslov, telefon, elektronska pošta
- **Kontakti pooblaščene osebe za varstvo osebnih podatkov (ang. DPO),** če je imenovana:
  _____
  Telefon, e-pošta.
- **Namen obdelave osebnih podatkov:** _____
  Opišite namene obdelave, kot jih določa zakonodaja ali kot ste jih sami opredelili. Do bo namen obdelave posameznikom jasno razumljiv je v povezavi z nameni treba navesti oz. opisati tudi vrste osebnih podatkov, ki se zbirajo oziroma obdelujejo za posamezen namen.
- **Pravna podlaga za obdelavo osebnih podatkov:**
  _____
  Navedite pravno podlago za obdelavo osebnih podatkov (npr. privolitev posameznika po določbi točke (a) člena 6(1) Splošne uredbe o varstvu osebnih podatkov, zakoniti interesi, za uveljavljanje katerih si prizadeva upravljavec ali tretja oseba po določbi točke (f) člena 6(1) Splošne uredbe, 48. člen Zakona o delovnih razmerjih...).
- **Obrazložitev zakonitih interesov[1]:** _____
  Če so zakoniti interesi, za uveljavljanje katerih si prizadeva upravljavec ali tretja oseba, pravna podlaga za obdelavo osebnih podatkov, potem jih morate navesti (npr. varovanje premoženja). Če je pravna podlaga drugo (npr. privolitev, zakon...), potem pustite prazno.
- **Uporabniki ali kategorije uporabnikov[2] osebnih podatkov, če obstajajo:**
  _____
  Navedite, katerim tretjim osebam se posredujejo osebni podatki (npr. konkretnemu organu, zavodu, podjetju, pogodbenemu obdelovalcu ali dovolj jasno in zelo opredeljeno kategorijo uporabnikov ...). Zaposleni pri upravljavcu se ne štejejo za uporabnike.

[1] Točka (f) člena 6(1) Splošne uredbe.
[2] Točka (9) člena 4 Splošne uredbe.

OBVESTILO POSAMEZNIKOM PO 13. ČLENU SPLOŠNE UREDBE O VARSTVU PODATKOV (GDPR) GLEDE OBDELAVE OSEBNIH PODATKOV



Obrazec OBV – 3. 9. 2018

- **Informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo:**
  _____
  Če se podatki prenašajo v tretje države ali mednarodne organizacije, navedite ali za to tretjo državo obstaja sklep o ustreznosti oz. sklic na ustrezne ali primerne zaščitne ukrepe po členih 46, 47 oz. 49(1) Splošne uredbe in sredstva za pridobitev njihove kopije ali kje so na voljo in po potrebi podajte ustrezne druge informacije.
- **Obdobje hrambe osebnih podatkov ali, kadar to ni mogoče, merila, ki se uporabijo za določitev tega obdobja:**
  _____
  Obdobje hrambe lahko določa zakonodaja, sicer pa je treba izhajati iz vaših namenov obdelave. Če obdobja hrambe ni mogoče natančno določiti, razmislite o možnih okoliščinah ali kriterijih, ki lahko vplivajo na obdobje hrambe in obdobje določite na način, da posameznik lahko predvideva, kdaj naj bi rok potekel (npr. hramba do preklica privolitve, hramba za določeno obdobje merjeno od nastanka nekega dogodka (pd.).
- **Informacije o obstoju pravic posameznika, da lahko zahteva dostop do osebnih podatkov in popravek ali izbris osebnih podatkov ali omejitev, ali obstoj pravice do ugovora obdelavi in pravice do prenosljivosti podatkov:**
  _____
  Preverite, katere pravice ima posamezik v konkretnem primeru, in jih navedite. Prav tako navedite, kako lahko posamezik te pravice uveljavlja in morebitne omejitve pravic glede na določbe 23. člena Splošne uredbe.
- **Informacija o pravici do preklica privolitve, kadar obdelava temelji na privolitvi:** Privolitev lahko kadar koli prekličete, ne da bi to vplivalo na zakonitost obdelave podatkov, ki se je na podlagi privolitve izvajala do njenega preklica.
- **Informacija o pravici do vložitve pritožbe pri nadzornem organu**: Pritožbo lahko podate Informacijskemu pooblaščencu (naslov: Dunajska 22, 1000 Ljubljana, e-naslov: gp.ip@ip-rs.si telefon: 01230 9730, spletna stran: www.ip-rs.si).
- **Informacije o tem:**
  - ali je zagotovitev osebnih podatkov **zakonska ali pogodbena obveznost:** *Da/ne.*
  - ali **mora posamezik zagotoviti osebne podatke** ter kakšne so morebitne **posledice, če jih ne zagotovi:** *Da/ne in pojasnilo.*
- **Informacije o obstoju avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov** ter vsaj v takih primerih smiselne informacije o **razlogih** zanj, kot tudi **pomen** in **predvidene posledice** take obdelave za posameznika, na katerega se nanašajo osebni podatki:
  _____
  Če posamezika profilirate ali z izvajate avtomatizirano odločanje na podlagi njihovih osebnih podatkov, potem jim kratko in razumljivo to pojasnite. Če npr. želite spremljati podatke o njihovih nakupih za namene prilagajanja oglaševanja in ponudbe, pojasnite vele razloge za to, kaj to pomeni za posameznika (npr. da boste zbirali podatke o ceni kupljenih artiklov, času in lokaciji nakupov (pd.) ter predvidene posledice za posameznika (npr. da bo prejemal oglase in ponudbo, ki bo temeljila na njegovih pretekih nakupih in preferencah).

Zahteva za seznanitev z lastnimi osebnimi podatki

Naziv in naslov upravljavca osebnih podatkov:

.....

Zahteva za seznanitev z lastnimi osebnimi podatki

(vabimo vas, da si pred izpolnjevanjem obrazca ogledate priloženo pojasnilo in navodilo)

Spodaj podpisani/-a *(ime in priimek)*: .....

(naslov prebivališča): .....

(drugi kontaktni podatki – po potrebi): .....

(rojstni datum ali drugi identifikacijski podatki, na podlagi katerih lahko upravljavec v svojih zbirkah najde vaše osebne podatke, ki jih zahtevate): .....

vlagam na podlagi člena 15 Splošne uredbe (EU) o varstvu podatkov zahtevo za seznanitev z osebnimi podatki, ki se nanašajo name (lastnimi osebnimi podatki). Zato vas prosim, da mi *(v nadaljevanju označite le tiste informacije, ki jih resnično želite)*:

- ☐ **potrdite, ali se osebni podatki v zvezi z menoj obdelujejo** ali ne *(prvi odstavek člena 15)*;
- ☐ omogočite **dostop do osebnih podatkov**, ki so vsebovani v zbirki osebnih podatkov in se nanašajo name *(prvi odstavek člena 15; OPOMBA: Mošen je vpogled ali pridobitev kopije, kar označite na koncu obrazca)*;
- ☐ posredujete **informacije o namenih obdelave osebnih podatkov** *(točka (a) prvega odstavka člena 15)*;
- ☐ posredujete **informacije o vrstah osebnih podatkov, ki se obdelujejo** *(točka (b) prvega odstavka člena 15; OPOZORILO: ta seznam ne bo vseboval konkretnih osebnih podatkov oziroma njihove vsebine)*;
- ☐ posredujete **informacije o uporabnikih ali kategorijah uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki** *(točka (c) prvega odstavka člena 15; OPOZORILO: uporabniki niso uslužbenci upravljavca, ki so pri upravljavcu obdelovali vaše osebne podatke)*;
- ☐ posredujete informacijo o **predvidenem obdobju hrambe osebnih podatkov**, če pa to ni mogoče, informacije o **merilih, ki se uporabljajo za določitev obdobja hrambe** *(točka (d) prvega odstavka člena 15)*;
- ☐ posredujete **informacije o obstoju pravice**, da se od upravljavca zahteva **popravek ali izbris** osebnih podatkov ali **omejitev** obdelave osebnih podatkov, ali obstoju pravice do **ugovora** taki obdelavi *(točka (e) prvega odstavka člena 15)*;
- ☐ posredujete **informacijo o pravici do vložitve pritožbe** pri nadzornem organu *(točka (f) prvega odstavka člena 15)*;
- ☐ posredujete **informacije v zvezi z virom** osebnih podatkov, če ti niso bili zbrani od mene *(točka (g) prvega odstavka člena 15)*;
- ☐ posredujete **informacije o obstoju avtomatiziranega sprejemanje odločitev, vključno z oblikovanjem profilov**, ter vsaj v takih primerih smiselne informacije o **razlogih** zanj, **pomenu in predvidenih posledicah** take obdelave za mene *(točka (h) prvega odstavka člena 15)*.

Zahteva za seznanitev z lastnimi osebnimi podatki

Podrobnejši opis zahtevanih osebnih podatkov oziroma dokumentov:

.....

.....

.....

.....

.....

.....

.....

.....

.....

Prosim vas, da mi zahtevane informacije zagotovite v naslednji obliki:

☐ vpogled pri upravljavcu	☐ fotokopija ali izpis v form. A4 oziroma v form. .....
☐ po e-pošti	☐ elektronski zapis na CD/DVD/drugem splošno uporabljivem prenosnem nosilcu podatkov

Opombe (npr. priloge): .....

Datum: ..... Podpis: .....

Člen 32 - Varnost obdelave

1. Ob **upoštevanju najnovejšega *tehnološkega razvoja** in **stroškov** izvajanja ter **narave, obsega, okoliščin in namenov *obdelave**, pa tudi ***tveganj** za **TČP,** ki se razlikujejo po **verjetnosti** in **resnosti**, **upravljavec/obdelovalec** z **ustreznimi tehničnimi** in **organizacijskimi** ukrepi zagotovita **ustrezno raven varnosti glede na tveganje**, vključno med drugim z ukrepi, kot je ustrezno:

(a) **psevdonimizacijo** in **šifriranjem** OP;
(b) zmožnostjo zagotoviti stalno **zaupnost, celovitost, dostopnost** in **odpornost sistemov** in storitev za obdelavo;
(c) zmožnostjo pravočasno **povrniti razpoložljivost** in dostop do OP v primeru fizičnega ali tehničnega incidenta;
(d) postopkom **rednega testiranja**, **ocenjevanja** in **vrednotenja učinkovitosti** tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave.

Razkrivanje varnostnih ranljivosti

AKTERJI: Novinarji, aktivisti, hekerji (beli/črni), notranji viri, prizadeti posamezniki, ….

POSLEDICE: Javno razkrivanje ranljivosti (mediji), blatenje ugleda upravljavca, inšpekcijski postopki in sankcije.

VPRAŠANJA: Koliko varnosti? Kdo je odgovoren? Kako ravnati?

Obvestilo o kršitvi VOP (33., 34. čl.)

a.) v primeru kršitev VOP (razen če ni verjetno, da bodo ogrožene TČP) mora **upravljavec v 72 urah obvestiti IP**

(kršitev; kategorije in pribl. število posameznikov; katere zbirke OP; DPO; predvidene posledice kršitve; že sprejeti ukrepi).

b.) (le) če je verjetno, da kršitev VOP povzroči veliko tveganje za TČP, upravljavec brez nepotrebnega odlašanja kršitev obvesti **posameznika** (DPO, opis posledic in sprejetih ukrepov) – razen če: *je upravljavec že izvedel ustrezne tehnične in organizacijske zaščitne ukrepe glede kršitve ali *je že sprejel ukrepe za zagotovitev, da se veliko tveganje za TČP verjetno ne bo več udejanjilo ali * bi to zahtevalo nesorazmeren napor – v tem zadnjem primeru objavi javno sporočilo ali podoben ukrep, s katerim so **posamezniki na katere se nanašajo OP**, enako učinkovito obveščeni .

12. odst. 4. člena: *„**Kršitev VOP**“ = kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do OP, ki so poslani, shranjeni ali kako drugače obdelani.*

Gre lahko za **več tipov kršitev**:

- Kršitev **zaupnosti** OP *(nepooblaščena seznanitev z OP)*
- Kršitev **celovitosti** OP *(nepooblaščeno spreminjanje)*
- Kršitev **dostopnosti** OP *(nezmožnost pooblaščenega dostopa do OP)*

Pot obveščanja:

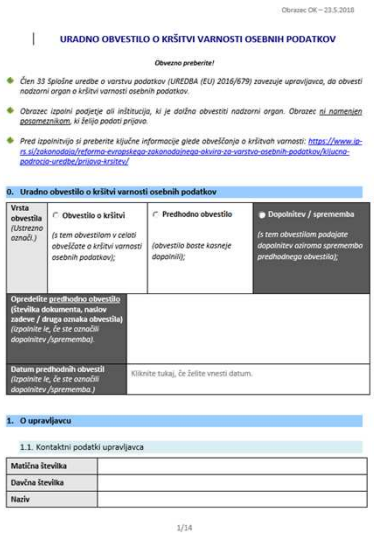
Incident pri obdelovalcu → obvestilo upravljavcu → obvesti IP

Incidenti pri upravljavcu → obvesti IP

Vsaka kršitev VOP je varnostni incident, a ni treba obveščati IP za vsak varnostni incident.

Presoja se „od primera do primera“.

URADNO OBVESTILO O KRŠITVI VARNOSTI OSEBNIH PODATKOV



Obrazec OK – 23.5.2018

URADNO OBVESTILO O KRŠITVI VARNOSTI OSEBNIH PODATKOV

Obvezno preberite!

- *Člen 33 Splošne uredbe o varstvu podatkov (UREDBA (EU) 2016/679) zavezuje upravljavca, da obvesti nadzorni organ o kršitvi varnosti osebnih podatkov.*
- *Obrazec izpolni podjetje ali inštitucija, ki je dolžna obvestiti nadzorni organ. Obrazec ni namenjen posameznikom, ki želijo podati prijavo.*
- *Pred izpolnitvijo si preberite ključne informacije glede obveščanja o kršitvah varnosti: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/prijava-krsitev/*

0. Uradno obvestilo o kršitvi varnosti osebnih podatkov

Vrsta obvestila *(Ustrezno označi.)*	○ **Obvestilo o kršitvi** *(s tem obvestilom v celoti obveščate o kršitvi varnosti osebnih podatkov);*	○ **Predhodno obvestilo** *(obvestilo boste kasneje dopolnili);*	● **Dopolnitev / sprememba** *(s tem obvestilom podajate dopolnitev oziroma spremembo predhodnega obvestila);*
Opredelite predhodno obvestilo (številka dokumenta, naslov zadeve / druga oznaka obvestila) *(izpolnite le, če ste označili dopolnitev /sprememba).*			
Datum predhodnih obvestil *(izpolnite le, če ste označili dopolnitev /sprememba.)*	Kliknite tukaj, če želite vnesti datum.		

1. O upravljavcu

1.1. Kontaktni podatki upravljavca

Matična številka	
Davčna številka	
Naziv	

1/14

GDPR koraki

1.) Preveritev veljavnosti obstoječih privolitev (jasna, razumljiva izjava, dana z nedvoumnim pritrdilnim dejanjem in dokazljiva; 6. in 7. čl + r: 32,42,43,171) in pridobivanje novih privolitev (ustrezno obveščen posameznik komu daje svoje OP, katere in zakaj ter kakšne pravice ima; čl. 12-14)

2.) Prilagoditev pogodb z (pogodbenimi) obdelovalci
(nekatere klavzule v pogodbah z računovodskimi servisi, IT-ponudniki…. bodo obvezne; čl. 28)

3.) Preveritev in prilagoditev popisa zbirk OP – „evidence dejavnosti obdelave“ (čl. 30) ----------→>

4.) Preglejte postopke zagotavljanja pravic posameznika
(seznanitev/omejitev/izbris/popravek/prenos/ugovor; 12-22.)

5.) Pripravite se na načelo odgovornosti. Če so OP osnova vašega poslovanja, pravočasno preverite:

a.) ali boste morali izvajati ocene učinka na VOP (DPIA, čl. 35)

b.) ali boste morali imenovati DPO (čl. 37)

c.) vaše postopke za minimizacijo (= načela vgrajenega in privzetega VOP) →> minimizirajte torej: količino OP, obseg njihove obdelave, rok hrambe, kdo jih obdeluje (čl. 25)
----------→>

6.) preglejte in prilagodite varnostne politike in njihovo izvajanje (več o varnosti na varninainternetu.si, čl. 24)

7.) Kdo bo poročal v primeru varnostnega incidenta

(če OP izgubite/pridejo v nepooblaščene roke, o tem poročate IP v 72 urah, v določenih primerih pa tudi posameznikom, čl. 33)

8.) Ne zmorete sami? Lahko poiščete zunanje strokovnjake,

a ne nasedajte vsaki ponudbi in strašenjem z visokimi kaznimi.

Princip: „zdrava pamet ☺“

ŠE NEKAJ MITOV IN NERESNIC O GDPR

1. mit: "NA ZAHTEVO POSAMEZNIKA BOMO SEDAJ MORALI IZBRISATI VSE NJEGOVE OP"

Člen 17

- Ni pravica do izbrisa zgodovine, do cenzure!
- **Umik podatkov oz. povezav do nepotrebnih, zastarelih, izrazito škodljivih podatkov o posamezniku**
  - npr. nepremišljene izjave/objave v mladosti
  - javne osebe
- **Tehtanje pravic**!
- **Druge pravne podlage!**
- **Številne izjeme**: svoboda izražanja in obveščanja, pravna obveznost, javni interes, arhiviranje v javnem interesu, za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene…

2. mit: „VEDNO BOM LAHKO DOBIL E-VERZIJO SVOJIH OP"

Člen 20

Posameznik ima pravico, da prejme OP, ki jih je posredoval upravljavcu, **v strukturirani, splošno uporabljani in strojno berljivi obliki**, in **pravico, da te OP posreduje drugemu upravljavcu**, **ko:**

a) obdelava temelji na privolitvi (ali pogodbi),
b) se obdelava izvaja z avtomatiziranimi sredstvi.

Bomo tako (počasi) spoznali pravo vrednost naših OP?

- Posameznik ima **pravico, da se OP neposredno prenesejo od enega upravljavca k drugemu, *kadar je to tehnično izvedljivo*.**
- Uresničevanje pravice ne posega v druge pravice – dobiš **kopijo lastnih OP** in ne **podatkov drugih (npr. intelektualno lastnino).**
- Ta pravica se **NE** uporablja za obdelavo, potrebno za opravljanje **naloge v javnem interesu** ali izvajanju **javne oblasti upravljavca.**

3. mit: „PROFILIRANJE NE BO DOVOLJENO“

Člen 22

Posameznik ima pravico, da zanj **ne velja odločitev, ki temelji zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov**, ki ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva.

Avtomatizirano odločanje in profiliranje **bo dopustno, če** je odločitev:

a) **nujna za sklenitev/izvajanje pogodbe** med posameznikom in upravljavcem;
b) **dovoljena v pravu EU ali DČ + zaščitni ukrepi**, ali
c) **utemeljena z izrecno privolitvijo posameznika**.

Pravica do :
- **osebnega posredovanja upravljavca**,
- do **izražanja lastnega stališča in**
- **izpodbijanja odločitve**.

Avtomatiziranih odločitev načeloma NI na *posebnih vrstah OP* (so možne izjeme)
- npr. da **računalnik samostojno odloča o vaši diagnozi in zdravljenju.**
(uspešna umetna inteligenca: AI-zdravniki, odvetniki)

4. mit: „VSI UPRAVLJAVCI BODO MORALI IMETI DPO“

Upravljavec in **obdelovalec** imenujeta DPO, kadar:

a) **javni organ ali telo, razen sodišč**, kadar delujejo kot sodni organ;
b) temeljne dejavnosti zajemajo dejanja **obdelave**, pri katerih je treba **zaradi njihove narave, obsega in/ali namenov posameznike redno in sistematično obsežno spremljati,** ali
c) temeljne dejavnosti upravljavca ali obdelovalca zajemajo **obsežno obdelavo *posebnih* vrst podatkov** in OP v zvezi s KD in prekrški.

5. mit: „ZA VSE KRŠITVE BOMO DOBILI 20 MILIONSKO KAZEN“

Sankcije bodo **učinkovite**, **sorazmerne** in **odvračilne**.

Upravne globe **do 10 mio EUR** ali **2 % skupnega svetovnega letnega prometa oz. do 20 mio EUR** ali **4% skupnega svetovnega letnega prometa** - kateri znesek je višji.

Upoštevalo se bo **11 kriterijev**:

a) **narava, teža in trajanje kršitve**, **število posameznikov**, **raven škode**, ki so jo utrpeli;
b) ali je kršitev **namerna** ali posledica **malomarnosti**;
c) vsi **ukrepi, ki jih je sprejel upravljavec ali obdelovalec**, da bi ublažil škodo, ki so jo utrpeli posamezniki;
d) **stopnja odgovornosti upravljavca/obdelovalca**, pri čemer se upoštevajo tehnični in organizacijski ukrepi;
e) vse zadevne **predhodne kršitve** upravljavca ali obdelovalca;
f) **stopnja sodelovanja z IP** pri odpravljanju kršitve in blažitvi škodljivih učinkov kršitve;
g) **vrste OP**, ki jih zadeva kršitev,
h) **kako je IP izvedel za kršitev**, ali je bil uradno obveščen o kršitvi;
i) če so bili ukrepi že prej odrejeni zoper upravljavca/obdelovalca z enako vsebino, skladnost s temi ukrepi;
j) **upoštevanje odobrenih kodeksov ravnanja** ali **odobrenih mehanizmov potrjevanja**, in
k) morebitni **drugi oteževalni ali olajševalni dejavniki** (npr. pridobljene finančne koristi).

Kakšen ZVOP-2 in kdaj bo sprejet v DZ?

25. 5. 2018

Vsekakor: GDPR = neposredno uporabljiv pravni vir.

Področne ureditve ZVOP-2: VOP umrlih, DPO posebne določbe, postopek za potrjevanje kodeksov ravnanja/certificiranje, pristojnosti IP, razmerje do ZDIJZ (psevdonimi), neposredno trženje, videonadzor, biometrija, evidentiranje vstopov in izstopov, povezovanje zbirk OP, strokovni nadzor, prekrški, prehodne določbe

POSLEDICE KRŠITEV DOLOČB ZVOP-1 – dosedanje globe

INŠPEKCIJSKI POSTOPEK
PREKRŠKOVNI POSTOPEK (**sankcija:** opomin, globa)

- Pravna oseba in s.p.: **4.170 do 12.510 EUR**
- Odgovorna oseba pravne osebe: **830 do 2.080 EUR**
- Odgovorna oseba državnega organa: **830 do 2.080 EUR**
- Posameznik: **200 do 830 EUR**

Za kršitve: *neposredno trženje, *videonadzor večstanovanj. objektov, *evidenci vstopov in izstopov **so globe 1/2**

Plačilo ½ globe v roku

83. člen GDPR: Splošni pogoji za naložitev upravnih glob

Upravne globe v znesku **do 10 000 000 EUR** ali v primeru družbe v znesku **do 2% skupnega svetovnega letnega prometa** v preteklem proračunskem letu, odvisno od tega, kateri znesek je višji:

a) obveznosti upravljavca in obdelovalca v skladu s čl. 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 in 43;
b) obveznosti organa za potrjevanje v skladu s čl. 42 in 43;
c) obveznosti organa za spremljanje v skladu s čl. 41(4).

Upravne globe v znesku **do 20 000 000 EUR** ali v primeru družbe v znesku **do 4% skupnega svetovnega letnega prometa** v preteklem proračunskem letu, odvisno od tega, kateri znesek je višji:

a) osnovna načela obdelave, vključno s pogoji za privolitev, v skladu s čl. 5, 6, 7 in 9;
b) pravice posameznika, na katerega se nanašajo podatki, v skladu s čl. 12 do 22;
c) prenosi osebnih podatkov prejemniku v tretji državi ali mednarodni organizaciji, v skladu s čl. 44 do 49;

KOMBINACIJA GDPR
IN DO NOVEGA ZVOP-2
ŠE VEDNO VELJAVNIH DOLOČB ZVOP-1

Kakšen bo ZVOP-2 in kdaj bo sprejet v DZ?

ZVOP-1 velja deloma (če ni urejeno v GDPR + ni z njo v koliziji z GDPR), v celoti pa za tiste organe, ki obdelujejo OP za namene preprečevanja, preiskovanja, odkrivanja ali pregona KD ali izvrševanja kazenskih sankcij (še ne prelita Direktiva EU 2016/680) – policija, DT, UIKS

GDPR = od 25. 5. 2018 neposredno uporabljiv pravni vir.

Področne ureditve predvidoma v ZVOP-2: VOP umrlih, DPO posebne določbe, postopek za potrjevanje kodeksov ravnanja/certificiranje, pristojnosti IP, razmerje do ZDIJZ (psevdonimi), neposredno trženje, videonadzor, biometrija, evidentiranje vstopov in izstopov, povezovanje zbirk OP, strokovni nadzor, prekrški, prehodne določbe

Najpogosteje zastavljeno vprašanje – „arhivske matične knjige“:
Ali GDPR res ne dopušča, da se raziskovalni namen pridobi vpogled v „arhivske matične knjige“, ki se hranijo v župniji? Kaj pa oklicne knjige, poročni spisi, oporoke, računi?

Ker glede seznanitve z OP umrlih, **ne glede na GDPR, še vedno velja 23. člen ZVOP-1**, je seznanitev s starim gradivom dopustna, če:

- je gotovo, da so posamezniki umrli
- oseba ki prosi za OP, ustrezno izkaže „znanstveno-raziskovalni, statistični ali zgodovinski“ namen seznanitve in
- posamezniki pred smrtjo niso pisno prepovedali seznanitve oz. njegovi dediči 1. ali 2. dednega reda, če zakon ne določa drugače.

Če gre za arhivsko gradivo po ZVDAGA: Tolmači Arhiv RS (IP ne sme).

Še veljavni členi ZVOP-1 (razlaga Ministrstva za pravosodje)

I. DEL – SPLOŠNE DOLOČBE – velja le še:

* 4. in 5. člen (prepoved diskriminacije, ozemeljska veljavnost ZVOP-1)
* le delno 6. člen - le definiciji javnega/zasebnega sektorja

II. DEL – OBDELAVA OP veljajo le še določbe, ki jih GDPR nima:

* 8. člen (pogoji za zakonsko določanje obdelav OP)
* 9. člen (dodatne omejitve za določitev pravne podlage v javnem sektorju, ne pa 3. odst. (=sklenitev pogodbe)
* 17. člen (znanstveno zavarovanje)
* 2. odst. 18. člena (vpogled v osebni dokument)
* 20. člen (uporaba istega povezovalnega znaka)
* 22. člen (posredovanje OP, zlasti brezplačno posredovanje OP med upravljavci v javnem sektorju)
* 23. člen (VOP umrlih)
* 24. člen (zavarovanje OP – kot dodatni ukrepi za varnost OP)
* 2. odst. 25. člena (interni akti za zavarovanje OP – le za javni sektor)

III. DEL – PRAVICE POSAMEZNIKA – velja le še:

***** 34. – 36. člen, ki urejajo sodno varstvo pravic posameznika

IV. DEL – INSTITUCIONALNO VARSTVO OP – velja skupaj z ZInfP (=pristojnosti IP), če niso v nasprotju z GDPR (npr. sklic na 7. točko 1. odst. 49. člena ZVOP-1 glede izdaje mnenj, zdaj: 58. čl. GDPR)

V. DEL – IZNOS OP – preneha veljati, veljajo pa še odločbe IP o iznosu OP, če niso nadomeščene z odločbami Evropske komisije

VI. DEL – PODROČNE UREDITVE – veljajo še naprej: Neposredno trženje, videonadzor, biometrija, evidentiranje vstopov in izstopov, povezovanje zbirk, strokovni nadzor, v kolikor niso v neskladju z GDPR (npr. definicija privolitve)

VII. DEL – KAZENSKE DOLOČBE – veljajo le še tiste določbe, ki se nanašajo na zgoraj navedene „preživele“ člene

IP je po 2. členu ZInfP pristojen za inšpekcijski nadzor nad izvajanjem **„vseh predpisov, ki urejajo varstvo ali obdelavo OP oziroma iznos OP** iz Republike Slovenije“ – pojem „predpis“ vključuje tudi GDPR.

IP mora v inšpekcijskem postopku svoje preiskovalne in popravljalne pristojnosti iz GDPR, izvajati **v skladu z domačo postopkovno zakonodajo**: ZInfP, ZIN, ZUP.

IP ostaja pristojen za obravnavo kršitev še veljavnih členov ZVOP-1, zaradi ozke definicije 2. člena ZInfP pa **IP ni pristojen tudi za obravnavo kršitev GDPR glede izrekanja sankcij za kršitve – dokler ne bo sprejet ZVOP-2, ki bo izrecno določil IP tudi kot prekrškovni organ za kršitve GDPR.** Lahko pa IP izvaja vse inšpekcijske nadzore in izreka vse inšpekcijske ukrepe.

Kaj pa pristojnost IP za pritožbe posameznikov glede izvajanja njihovih pravic po 15. – 22. in 34. čl. GDPR: seznanitev z lastnimi OP (15.), popravek in izbris (16.), RTBF (17.), pravica do omejitve obdelave (18.), obveznost obveščanja v zvezi s popravkom ali izbrisom ali omejitvijo obdelave (19.) Data portability (20.), Pravica do ugovora za obdelave iz točke (e) in (f) 6. člena GDPR (javni interes in zakoniti interes, 21.), Pravice glede avtomatizirane obdelave – profiliranja (22.) Sporočilo posamezniku o Data breachu (34.)?

Ministrstvo za pravosodje meni, da IP ni pristojen za obravnavo pravic iz 16. – 22. člena, zato posameznikom (za sedaj) ostaja le sodno varstvo.

Hvala za pozornost!

gp.ip@ip-rs.si