



INFORMACIJSKI
POOBLAŠČENEC

Izkušnje Uredbe (EU) 2016/679 Evropskega
parlamenta in Sveta z dne 27.4.2016 o varstvu
posameznikov pri obdelavi osebnih podatkov in o
prostem pretoku takih podatkov ter o razveljavitvi
Direktive 95/46/ES
(GDPR) v praksi

**Mojca Prelesnik, univ. dipl. prav.
informacijska pooblaščenka
Portorož, 24.1.2020**



Večji poudarek odgovornosti zavezancev

- zakonitost, pravičnost in preglednost (*lawfulness, fairness and transparency*)
- omejitev namena (*purpose limitation*)
- najmanjši obseg podatkov (*data minimisation*)
- točnost (*accuracy*)
- omejitev shranjevanja (*storage limitation*)
- celovitost in zaupnost (*integrity and confidentiality*)
 - in razpoložljivost
- **odgovornost (*accountability*):**
odgovoren za skladnost s temeljnimi načeli in je to skladnost tudi
zmožen dokazati – **Proaktivnost! Dolžnost upravljavca!**



POGOSTA VPRAŠANJA IZ PRAKSE IP

- Kaj vse je OP?
- Je naše podjetje upravljavec, obdelovalec OP ali oboje?
- Kaj je (pogodbena) obdelava in kaj ni, kdo je obdelovalec in kdo ni, ali mora biti nujno sklenjena pogodba po 28. členu?
- Kateri upravljavci morajo imeti svoj akt o „zavarovanju“?
- Katere informacije o uporabniku OP mora upravljavec dati posamezniku (po 13., 14. in 15. členu) ?
- Kaj če ne obvestimo IP o kršitvi varstva OP?
- Kaj se skriva za kraticami: DPIA, DPO, DBN?



UPRAVLJAVEC - OBDELOVALEC - UPORABNIK

Upravljavec = fizična ali pravna oseba, javni organ ali agencija ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave.

(npr. podjetje, državni organ)

Obdelovalec = fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki obdeluje OP v imenu upravljavca.

(npr. računovodski servis, IT-podjetje)

Uporabnik = fizična ali pravna oseba, javni organ, agencija ali drugo telo, ki so mu bili OP razkriti.

(npr. sodni izvedenec, tolmač)



Sodni tolmači/izvedenci glede izvajanja tolmačenja /izdelave izvedenskih mnenj – upravljavci, obdelovalci, uporabniki OP?

Tolmačev/izvedencev praviloma ne štejemo za pogodbene obdelovalce. Njihov stik z OP pri upravljavcu namreč ni namen storitve, ki se najema. Zato so tolmači/izvedenci **uporabniki OP** za namene priprave prevoda ali mnenja. Ne glede na svoj status, pa morajo vsi vedno zagotoviti potrebne ukrepe varnosti OP, ki jih obdelujejo (= zavarovanje OP).

Pozor: za zbirke OP, ki jih vodijo na različnih pravnih podlagah (zakonih, privolitvah,) – npr. zaposlenih, strank, pa so **UPRAVLJAVCI**.



Revizorji in revizijske družbe – upravljavci, obdelovalci?

Bistveno ločiti, ali pravo omogoča upravljavcu, da določena dejanja, storitve, ki vključujejo obdelavo OP, lahko izvrši sam ali ne.

Če pravna oseba najame storitve revizijske družbe:

a.) za izvedbo notranje revizije, ki služi kot pomoč poslovodstvu podjetja, da bi to učinkovito vodilo podjetje, torej kot pomoč/svetovanje/priporočila = revizijska družba je **OBDELOVALEC**.

b.) za izvedbo zunanje revizije v smislu ZRev-2, ki jo lahko po 1. odst. 5. člena izvaja izključno revizijska družba in to ne glede na to, ali gre za zakonsko obveznost (prisilnost) ali za naročilo (prostovoljna odločitev) = revizijska družba je **UPRAVLJAVEC**, saj veljajo določbe ZRev: revizorji v svojem imenu in za svoj račun (npr. revidiranec ima dolžnost posredovanja OP revizorju, revizor ima izvorno pravico in dolžnost pridobivati in obdelovati OP, revizor „samostojno vodi postopek“; 1. odst. 37. člena ZRev-2).



Težave ob prehodu na GDPR

Nepoznavanje določb → pretiran strah in pretiravanja

- Slabo razlikovanje med 6 pravnimi podlagami: →
- Miti in legende o GDPR
- Fotografiranje otrok v šoli?
- Slabo informiranje posameznika
→ več prijav in pritožb
- ZVOP-2?

Pravne podlage za zasebni sektor, ko obdeluje običajne osebne podatke
člen 6 (1) Splošne uredbe

Primeri:

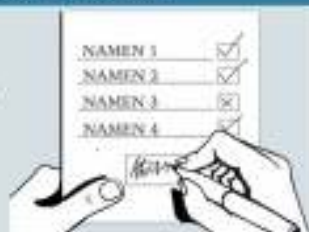
PRIVOLITEV točka (a)				
		Prijava na prejemanje e-novic.	Sodelovanje v nagradni igri.	Objava osebnih podatkov na spletu.
OBDELAVA JE POTREBNA ZA SKLENITEV ALI ZA IZVAJANJE POGODBE točka (b)				
		Posameznik izvede spletni nakup.	Nakup v veleblagovnici z bančno kartico.	Delo po pogodbi zunaj delovnega razmerja.
ZAKON ALI IZVAJANJE JAVNIH NALOG točki (c) ali (e)				
		Podatki zaposlenih na podlagi Zakona o delovnih razmerjih.	Podatki komitentov bank na podlagi Zakona o bančništvu.	Podatki zavarovancev na podlagi Zakona o zavarovalništvu.
ZAKONITI INTERESI, KI PREVLAJAJO NAD INTERESOM POSAMEZNIKA točka (f)				
		Pošiljanje obvestil za javnost na službene e-naslove novinarjev.	Varovanje omrežja.	Preprečevanje goljufij.



Pravne podlage za zasebni sektor, ko obdeluje običajne osebne podatke
člen 6 (1) Splošne uredbe

Primeri:

PRIVOLITEV
točka (a)



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)



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)



Podatki zaposlenih na podlagi
Zakona o delovnih razmerjih.



Podatki komitentov bank na
podlagi Zakona o bančništvu.



Podatki zavarovancev na podlagi
Zakona o zavarovalništvu.

**ZAKONITI
INTERESI,
KI PREVLAJAJO
NAD INTERESOM
POSAMEZNIKA**
točka (f)



Pošiljanje obvestil za javnost
na službene e-naslove
novinarjev.



Varovanje omrežja.



Preprečevanje goljufij.



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.



Miti in legende o direktnem marketingu

OBDELAVA OSEBNIH PODATKOV PRI NEPOSREDNEM TRŽENJU FIZIČNIM OSEBAM

Obdelava dopustna BREZ PRIVOLITVE

POT OBVEŠČANJA	PODATKI	POGOJI	PRAVNA PODLAGA	POSEBNI POGOJI
Navadna pošta 	Ima, primak, stalno in začasno prebivališče	<p>Če so podatki javno objavljeni (imenik, profilna spletna stran, itd.).</p> <p>Če so bili podatki pridobljeni v okviru zakonitega opravljanja dejavnosti (vizitka, dogodki, sejmi, nakup, itd.).</p>	<p>72/I ZVOP-1</p> <p>72/II ZVOP-1</p>	Jasna možnost, da lahko zahteva prenehanje pošiljanja obvestil (obvestilo o pravici do ugovora po 73. čl. ZVOP-1).
Elektronska pošta 	E-naslov	<p>Če podjetje od kupca svojih izdelkov/storitev pridobi njegov elektronski naslov, ga lahko uporablja tudi za trženje svojih podobnih izdelkov/storitev.</p> <p>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.</p>	<p>158/II ZEKom-1</p> <p>Pogodba med ponudnikom spletne storitve in posameznikom v povezavi s 6(1f) Splošne uredbe</p>	<p>Jasna možnost, da brezplačno in enostavno zahteva prenehanje uporabe naslova za ta namen (pravica po drugem odst. 158 ZEKom-1).</p> <p>Možnost, da lahko zahteva prenehanje pošiljanja obvestil (obvestilo o pravici do ugovora po čl. 21 Splošne uredbe).</p>
Telefon 	Tel. številka iz imenika	Za namen ponujanja izdelkov ali storitev po telefonu na številko 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 trži na kontakt zaposlenega, ki 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).

UPOŠTEVAJTE PREKLECE

V drugih primerih je obdelava dopustna le na podlagi PRIVOLITVE



INFORMACIJSKI
POOBlašČENEC





Najbolj iskana mnenja v 1 mesecu

	Naziv	št.
1	Podatki, ki jih lahko delodajalec pridobi za izračun nadomestila začasne odsotnosti iz dela	1050
2	Videonadzor na delovnem mestu	196
3	Fotografiranje naključnih oseb na javnih površinah pri nas	107
4	EMŠO-DŠ- osebni dokument	91
5	Objava fotografij otrok in drugih udeležencev prireditve	93
6	Snemanje oseb in vozil na ulici brez vednosti posameznika in objava posnetkov na internetu	89
7	Zvočno snemanje kot dokaz na sodišču	83
8	Dopustnost preverjanja prisotnosti drog ali alkohola v krvi zaposlenih v okviru rednega zdravstvenega pregleda	77
9	Pogoji za izvajanje videonadzora po GDPR	67
10	GDPR hramba podatkov	69



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.





Evidenca dejavnosti obdelave (pogosto nezavedno)



OP zaposlenih, ki se zberejo ob uporabi službenih sredstev – zbirke OP

- **e-pošta**
- **Internet**
- **videonadzorni posnetki**
- **biometrija**
- **telefoni**
- **mrežni tiskalniki**
- **čip kartice za odpiranje vrat**
- **GPS naprave...**

Pravne podlage, nameni, roki hrambe, dostopne pravice?



ZEPDSV (7. in 12. člen, 4 evidence in nabor OP)- **delodajalci vedno upravljavci**

- Evidenca o zaposlenih delavcih
- Evidenca o stroških dela
- Evidenca o izrabi delovnega časa
- Evidenca o oblikah razreševanja kolektivnih delovnih sporov pri delodajalcu

Nameni evidenc: *za uveljavljanje pravic iz sistema socialnega zavarovanja in socialnega varstva,
*statističnega spremljanja in *inšpekcijskega nadzora.



ZEPDSV

Za posameznega delavca od dneva sklenitve **pogodbe o zaposlitvi** do prenehanja pogodbe.

Evidenca o stroških dela = mesečno vpisovanje, listine trajne vrednosti (če delodajalec preneha, to prevzame pravni naslednik, če ga ni, pa Arhiv RS)

Evidenca o izrabi delovnega časa = dnevno vpisovanje, listine trajne vrednosti (če delodajalec preneha, prevzame p.naslednik, če ga ni pa Arhiv RS)



OBDELAVA OP V DELOVNEM RAZMERJU

48. člen ZDR-1

OP zaposlenega se v DR lahko obdelujejo le, če

določeno v zakonu
(ZDR ali drug, npr. ZJU)

potrebno zaradi uresničevanja pravic in
obveznosti iz DR ali v zvezi z DR



VIDEONADZOR V DELOVNIH PROSTORIH

- ste upravljavec (predlog ZVOP-2)

- Le če **nujno potrebno** za varnost ljudi ali premoženja ali za varovanje TP/PS, teh namenov pa ni možno doseči z milejšimi sredstvi + le glede tistih delov in prostorov v obsegu, kjer je treba varovati te interese.
- Vpogled/uporaba/posredovanje le za te namene, razen če zakon določa.
- Spremljanje neposrednega dogajanja pred kamerami le, če izvaja pooblaščen varnostno osebje ali drugo posebej pooblaščen in usposobljeno osebje upravljavca.
- **Zaposlene prej pisno obvestiti** + delodajalec se posvetuje z reprezentativnimi sindikati ter svetom delavcev/delavskim zaupnikom, če obstajajo. Posvetovanje **30 dneh** oz. v daljšem roku kot določi delodajalec. To NE velja na področju obrambe, OVS dejavnosti države in varovanja TP: T, ST.
- Poslovne stavbe: le če za **> 70% solastniških deležev** na skupnih delih.



Videonadzorni posnetek - odpoved pogodbe o zaposlitvi iz krivdnega razloga?

Je videonadzorni posnetek: zaposleni kradel (zbirni center komunalnega podjetja), veljaven dokaz o kršitvi pogodbe o zaposlitvi?

- Sodišče v pravnem postopku praviloma ne sme uporabiti dokazov, ki bi bili pridobljeni s kršitvijo ustavno zajamčenih človekovih pravic in temeljnih svoboščin.
- Videonadzor se lahko brez predhodne obveščенosti izvede le izjemoma, le če obstaja utemeljen sum storitve KD (seznanitev 77. čl. ZVOP-1).
- Sodba Vrhovnega sodišča (VII Ips 2/2018, 30.5.2018): V pravdnem postopku sodišče praviloma ne sme uporabiti dokazov, pridobljenih s kršitvijo ustavno zajamčenih pravic, a to ni absolutno. Izvedba dokaza, dobljenega s kršitvijo pravice do zasebnosti, je v pravnem postopku **LAHKO DOPUSTNA, ČE** za to obstajajo posebej utemeljene okoliščine + izvedba dokaza mora imeti prav poseben pomen **za izvrševanje neke druge ustavne pravice** – upoštevati načelo sorazmernosti in skrbno presoditi kateri pravici se da prednost. Detektiv v predal nastavljal napravo za male tatove (ponarejeni in označeni bankovci + avdio-video posnetek)



LAŽNE IN NEDELUJOČE VIDEO KAMERE?

ključno: nastanek
zbirke posnetkov (OP)



REPUBLIKA SLOVENIJA
UPRAVNA ENOTA LJUBLJANA

Tolstova ulica 5, 1000 Ljubljana

T: 01 206 30 00

F: 01 206 32 92

E: oe.ljubljana@gov.si

www.upravnienota.gov.si/ljubljana

OBVESTILO

Cenjene stranke obveščamo, da imamo v prostorih Sektorja za upravne notranje zadeve nameščene kamere, vendar niso vključene.

Bečka Trnčar univ. d.o.o. prav.
VODJA SEKTORJA





Nedopustni napaki upravljavcev – delodajalecev:

Preusmerjanje ali prebiranje e-pošte (tudi bivših) zaposlenih

- če delodajalec po koncu DR preusmeri e-naslov na drug naslov v podjetju: krši 8. čl. ZVOP-1 (=ni podlage v zakonu); =vpogled v OP pošiljateljev in naslovnikov);
- vpogled/prebiranje vsebine e-pošte delavca brez vednosti in soglasja: **KD Kršitve tajnosti občil** (150. čl. KZ).

Kdaj delodajalec sploh lahko vpogleda v delavčevo pošto?

- Le izjemoma: če to nalaga zakon ali posebne okoliščine: npr. smrt delavca (a sorazmerno, če oceni, da res službena pošta).
- IP svetuje delodajalcem: pridobite sodno odredbo, sicer izjemoma delajte to sporazumno, če ne gre pa komisijsko – v komisiji naj sodeluje tudi predstavnik zaposlenih ali sindikata!

Dokumente neizbranih kandidatov iz postopkov za zaposlitev je dopustno hraniti zaradi:



ZAKONA/ DRUGEGA PREDPISA

Zaradi zahtev specialnih zakonov ali drugih predpisov
(npr. ZVDAGA, Uredba o upravnem poslovanju, zahteve računovodskih in davčnih predpisov).



POGODBE

V skladu z morebitnimi specifičnimi pogodbenimi obveznostmi
(npr. v zvezi s hrambo dokumentacije iz razpisov).



PRIČAKOVANJA PRAVNEGA SREDSTVA

Najmanj do roka, ko je mogoče pričakovati, da bo zoper odločitev
o izbiri vloženo pravno sredstvo
(npr. Obligacijski zakonik določa splošni zastaralni rok 5 let od
nastanka terjatve).



PRAVNEGA POSTOPKA V TEKU

Če je začel postopek pred pristojnim organom je dokumente
dopustno hraniti do njegovega pravnomočnega zaključka.

KONEC HRAMBE

**ORIGINALE
VRNE**



**KOPIJE
UNIČI**



ORIGINALE mora delodajalec vrniti kandidatu tudi pred potekom predvidenega roka hrambe, če kandidat to zahteva skladno s 30. členom ZDR-1. Delodajalec si lahko dokumentacijo skopira in kopije hrani do poteka roka hrambe. Po preteku roka hrambe lahko originale vrne in kopije uniči.

Ali lahko delodajalec hrani podatke neizbranih kandidatov za morebitne prihodnje razpise?

NE, razen če kandidat v to vnaprej privoli!



NAČELO OMEJITVE SHRANJEVANJA:

Osebni podatki se hranijo le toliko časa, kolikor je potrebno za namene, za katere se obdelujejo. Delodajalci sami presodijo koliko časa in katere dokumente je glede na zgornje kriterije treba hraniti in koliko časa.



INFORMACIJSKI
POOBlašČENEC



Vzorec evidence dejavnosti obdelav – ZA UPRAVLJAVCE

Obrazec ID-1 – 25.5.2018

VZOREC EVIDENCE DEJAVNOSTI OBDELAVE ZA UPRAVLJAVCE

Obravnavajte!

- Pred uporabo varnost se podrobno seznajite z dolžnostmi zaupancem glede evidentiranja dejavnosti obdelave. Vse potrebne informacije najdete na spletni strani:
= <https://www.ia-rs.si/slovenskajaznformacijevnosilnizakonodajneokolozavarstvozgodovinskihpodatkov/izvorna-podlaga-uredbe/evidenca-dejavnosti-obdelave/>
- Vzorec ni predpis in je zgolj v pomoč zaupancem. Podani primeri ne predstavljajo nujno dejanskega stanja in so zgolj informativne narave.
- Za vsota zbirka osebnih podatkov pripravite njen »opis«, t.j. evidenco dejavnosti obdelave, ki je lahko tudi v elektronski obliki.

1. Podatki o zaupancu

Naziv ali ime	npr. Informacijski posredovalec
Naslov	npr. Zbirka evra 59. 3000 Ljubljana
Elektronska pošta	npr. ipo.ia@ia-rs.si
Telefon	npr. 01 230 57 51

a. Podatki o posredniški osebi za varstvo osebnih podatkov, če je imenovana

Ime in priimek	Nasvet: Več informacij o dolžnostih imenovane posredniške osebi najdete na spletni strani Informacijskega posredovalca ¹
Delovna mesta	
Elektronski naslov	
Telefon	

b. Podatki o stvarnem upravljalcu, če obstaja

Naziv ali ime	Nasvet: Pred vnositvijo podatkov preverite določbe uredbe glede stvarnih upravljalcev (26. člen).
Naslov	
Elektronska pošta	
Telefon	

c. Podatki o predstavitelju upravljalca, če obstaja

Naziv ali ime	Nasvet: Pred vnositvijo podatkov preverite določbe uredbe glede predstavnikov (27. člen). Predstavniki so pod pogoji iz tega člena dolžni imenovati upravljalci ali upravljalci, ki nimajo sedeža v EU.
Naslov	
Elektronska pošta	
Telefon	

¹ <https://www.ia-rs.si/slovenskajaznformacijevnosilnizakonodajneokolozavarstvozgodovinskihpodatkov/izvorna-podlaga-uredbe/evidenca-dejavnosti-obdelave/>



Vzorec evidence dejavnosti obdelav – ZA OBDELOVALCE

Oblika: ED-G – 25.3.2018

VZOREC EVIDENCE DEJAVNOSTI OBDELAVE ZA OBDELOVALCE

Oblastno prebrskite!

- Obdelovalec pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebnostne podatke v imenu upravitelja. Upravitelj torej kot naročnik storitve najame 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.ipe-rs.si/priponodeja/informacije-izvajalca-priponodeja-obdelava-iz-vestne-osebne-podatke/kisvna-postroca-uradno/pogodbeno-obdelavo/>
- Pri uporabi vprašalnika se podrobno seznanite z dolžnostmi zavezanca glede evidentiranja dejavnosti obdelave. Vse potrebne informacije najdete na spletni strani:
 - <https://www.ipe-rs.si/priponodeja/informacije-izvajalca-priponodeja-obdelava-iz-vestne-osebne-podatke/kisvna-postroca-uradno/priponodeja-obdelavo-iz-vestne-osebne-podatke/>
- Vzorec ni predpisni in je zgolj v pomoč zavezanecem. 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.

I. Podatki o zavezanecem

Naziv ali ime	npr. Poslovni sistem d.o.o.
Naslov	npr. Zvezna cesta 58, 2000 Ljubljana
Elektronska pošta	npr. naz.ime@podjetje.si
Telefon	npr. 01 230 97 80

Podatki o poslovalni osebi za vestno osebnih podatkov, če je imenovana

Ime in priimek	Ime in priimek osebe, ki je imenovana za vestno osebnih podatkov, če je imenovana
Delo mesto	
Elektronski naslov	
Telefon	

¹ <https://www.ipe-rs.si/priponodeja/informacije-izvajalca-priponodeja-obdelava-iz-vestne-osebne-podatke/kisvna-postroca-uradno/priponodeja-obdelavo-iz-vestne-osebne-podatke/>



„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))



POSAMEZNIK

INFOGRAFIKA:
Pravne podlage za
obdelavo osebnih
podatkov



Zbiranje
osebnih
podatkov

UPRAVLJAVEC lahko
pridobiva osebne podatke
od posameznika na
ustrezni pravni podlagi.

Kdaj GRE za pogodbeno obdelavo?

Računovodski servis za obračun plač
zaposlenih,
ponudniki storitev arhiviranja in
hrambe osebnih podatkov...

Kdaj NE GRE za pogodbeno obdelavo?

Pravno zastopanje po odvetniku,
operaterji, pošta in banke pri izvajanju
reguliranih storitev,
ponudniki taksi prevozov...

Pogodbena
obdelava
osebnih
podatkov



POGODBA med
upravljavcem in obdelovalcem
mora vsebovati vse sestavine
po členu 28 Splošne uredbe.
Enako pa tudi pogodba med
obdelovalcem in
podobdelovalcem.

VZOREC
pogodbe o
obdelavi
osebnih
podatkov

UPRAVLJAVEC lahko pooblasti obdelovalca za
izvajanje določenih dejanj obdelave, na podlagi pisne
pogodbe ali drugega ustreznega akta.

OBDELOVALEC lahko pooblasti podobdelovalca le ob predhodnem
pisnem dovoljenju upravljavca. Pisno dovoljenje je lahko splošno (za vse
podobdelovalce) ali specifično (za točno določene podobdelovalce).

PODOBDELAVA se lahko veriži naprej, pri čemer morajo biti izpolnjeni vsi pogoji,
ki veljajo za obdelovalca (pisna pogodba ali drug ustrezen akt). Poleg tega mora obstajati
še posebno pisno dovoljenje upravljavca.

POGOSTA VPRAŠANJA:



- Ali gre za pogodbeno obdelavo (računovodske storitve, oblaka hramba, pošta,...)?
- Kaj vse mora vsebovati pogodba o obdelavi osebnih podatkov?
- Na kaj je treba paziti pri sklepanju pogodbe o obdelavi, da bo v skladu z zakonodajo?



Smernice IP o pogodbeni obdelavi
(www.ip-rs.si)

Spletna stran za pomoč podjetjem
(www.upravljavec.si)



INFORMACIJSKI
POOBLAŠČENEC



(POGODBENA) OBDELAVA V PRAKSI

Hramba podatkov: virtualna (ponudniki gostovanja) ali fizična (ponudniki sefov), DA, če je obdelovalec seznanjen, da hrani OP za upravljavca, sicer NE.

Operater elektronskih komunikacij, Pošta Slovenije: NE

Storitve čiščenja: NE

Storitve prevozov, taxi: NE



(POGODBENA) OBDELAVA V PRAKSI

Če upravljavec najame prostor/strežniško infrastrukturo:

- in upravljavec sam dostopa do prostorov + sam odloča in skrbi za varovanje in dostop do teh prostorov, je to klasičen najem in NE pogodbeni obdelava
- če pa za varnost lokacije skrbi „najemodajalec“ + dostopajo osebe zaposlene pri tem „najemodajalcu“, potem ta je JE pogodbeni obdelovalec

Izvajalec medicine dela: NE (svoji predpisi, svoja dejavnost, je upravljavec)

Upravljavec mora poveriti OP v obdelavo (obdelovalec obdeluje namesto njega), obdelava je bistvo storitve.



(POGODBENA) OBDELAVA V PRAKSI

Kaj je to „drug pravni akt“ po 28. členu - podlaga za izvajanje obdelave?

Medsebojne P/D se določijo s podpisano pogodbo/dogovorom, lahko tudi z internim aktom upravljavca (pravilnik/navodilo....), ki se ga obdelovalec izrecno in PISNO zaveže spoštovati.

Bistvo: da so v pogodbi/internem aktu vse sestavine iz 28. čl.



Interni akt – pravilnik o zavarovanju OP - DA ali NE?

Kateri upravljavci morajo imeti pravilnik – interni akt o „postopkih in ukrepih za varstvo OP“?

- Vsi za katere ta obveznost še velja po ZVOP-1 (čl. 7 in 2. odst. 25. ZVOP-1: javni sektor);
- Vedno, kadar ocenjena stopnja tveganja za posege v pravice in svoboščine posameznikov glede na vrste OP in obdelave, ki jih izvaja upravljavec, terja sprejetje internega akta (32. člen GDPR).

Nasvet IP prav vsakemu upravljavcu zbirk OP: Imejte interni akt!!



Informacije, ki jih upravljavec zagotovi posamezniku, če OP pridobi od njega (13. čl.) - takrat, ko pridobi OP:

*upravljavec, kontaktni podatki DPO, namene (op. IP: to vključuje konkreten nabor OP) in pravno podlago obdelave, kadar obdelava temelji na 6 (1)/f zakonite interese za katere si prizadeva upravljavec ali 3. oseba, uporabnike ali kategorije uporabnikov OP, namera prenosa v 3. državo, če mogoče rok hrambe (sicer merila za določitev), obstoj pravic: dostop, popravek, izbris, omejitev obdelave, pravica do ugovora, pravica do prenosljivosti, do preklica privolitve, do vložitve pritožbe na IP, obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov!, namen nadaljne obdelave

Obveščanje pa ni potrebno (op.: le), če posameznik vse te informacije že ima! (razlika →)



Informacije, ki jih upravljavec zagotovi posamezniku, če OP NE pridobi od njega (14. člen):

*upravljavec, kontaktni podatki DPO, namene (razlika s 13. čl, kjer op. IP, da to vključuje konkreten nabor OP) in pravno podlago obdelave, vrste OP, uporabnike OP, namera prenosa v 3. državo, rok hrambe če mogoče (sicer merila za določitev), kadar obdelava temelji na 6 (1)/f zakonite interese za katere si prizadeva upravljavec ali 3. oseba obstoj pravic (dostop, popravek, izbris, omejitev obdelave, pravica do ugovora, pravica do prenosljivosti, do preklica privolitve, do vložitve pritožbe na IP, izvor OP, obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov, uporaba za drug namen)

*zagotovi najpozneje v 1 mesecu po prejemu OP, a se upoštevajo posebne okoliščine: najpozneje ob prvem komuniciranju s posameznikom ali ob prvem razkritju drugemu uporabniku ali pred predvideno nadaljnjo uporabo za drug namen.

Obveščanje NI potrebno: ----- >>



- a.) če posameznik te informacije že ima,
- b.) če bilo to obveščanje nemogoče ali nesorazmeren napor (npr. zlasti pri arhiviranju v javnem interesu, znanstveno – ali zgodovinsko-raziskovalne ali statistične namene) ali če bi to onemogočilo ali resno oviralo uresničevanje namenov te obdelave. V teh primerih upravljavec sprejme ustrezne ukrepe za zaščito TČP ter zakonitih interesov posameznika, tudi tako a informacije objavi. - Kako vse to v praksi?
- c.) je pridobitev ali razkritje **izrecno določeno s pravom EU ali DČ**,
- d.) morajo OP ostati zaupni po pravu EU ali DČ - tudi poslovna skrivnost.



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

Obvestilo OIV – 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)

Opisite in pojasnite:

- Informacija, ki tega obvestila ni treba vsebovati, kadar in kdaj posamezniki, na katerega se nanašajo osebni podatki, že imajo te informacije (dokazni izvešje je na upravljalca).
- Na kakšen je informacijski sistem in ni predpisanih.
- Informacije, ki jih posamezniki, na katere se nanašajo osebni podatki, imajo na voljo iz 13. člena Splošne uredbe, npr.:
 - Obdelava ali uporaba podatkov, ki so bili ustvarjeni iz informacij, ki jih posamezniki imajo na voljo, da bi se izognili kakršnim koli dodatnim (ali dodatnim) obdelavam. Obdelava vključuje samo obdelavo, ki jo ustvarijo ali drugemu posamezniku omogoča dostopnost in izvešje.
 - Obdelava ali uporaba podatkov, npr. za analizo, poročanje informacij, ki jih posamezniki imajo na voljo, da bi se izognili kakršnim koli dodatnim (ali dodatnim) obdelavam. Obdelava vključuje samo obdelavo, ki jo ustvarijo ali drugemu posamezniku omogoča dostopnost in izvešje.
 - Obdelava ali uporaba podatkov, ki jih posamezniki imajo na voljo, da bi se izognili kakršnim koli dodatnim (ali dodatnim) obdelavam. Obdelava vključuje samo obdelavo, ki jo ustvarijo ali drugemu posamezniku omogoča dostopnost in izvešje.

- **Upravitelj zbirke osebnih podatkov:** _____
naziv, naslov, telefon, elektronska pošta
- **Kontakti pooblaščen osebe za varstvo osebnih podatkov (ang. DPO), če je imenovana:** _____
Telefon, e-pošta.
- **Namen obdelave osebnih podatkov:** _____
Opisite namene obdelave, kot jih določa zakonodaja ali kot ste jih sami opredelili. Da 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...).
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 omrežja). Če je pravna podlaga druga (npr. privolitev, zakon...), potem pustite prazno.
- **Uporabniki ali kategorije uporabnikov¹ osebnih podatkov, če obstajajo:** _____
Navedite, katerim tretjim osebam se posredujejo osebni podatki (npr. konkretnemu organu, zavodu, podjetju, pogodbenemu obdelovalcu ali dovolj jasno in ozko opredeljen kategorije uporabnikov...). Zaposleni pri upravljavcu se ne štejejo za uporabnike.

¹ Točka (f) člena 6(1) Splošne uredbe.

² Točka (9) člena 4 Splošne uredbe.



VZOREC OBVESTILA POSAMEZNIKOM¹ GLEDE OBDELAVE OSEBNIH PODATKOV

navedite zbirko osebnih podatkov

(npr. V EVIDENCI VSTOPOV IN IZSTOPOV IZ URADNIH PROSTOROV ORGANA)

- **Upravljalavec zbirke osebnih podatkov:** *Naziv, naslov, telefon, elektronska pošta.*
- **Kontakti pooblaščenih oseb za varstvo osebnih podatkov (DPO):** *Telefon, e-pošta.*
- **Namen obdelave osebnih podatkov:** *Opišite namene obdelave, kot jih določa zakonodaja ali kot ste jih sami opredelili.*
- **Pravna podlaga za obdelavo osebnih podatkov:** *Navedite pravno podlago za obdelavo osebnih podatkov (npr. privolitev posameznika po določbi 6.a Splošne uredbe o varstvu osebnih podatkov, 48. člen Zakona o delovnih razmerjih...).*
- **Obrazložitev zakonitih interesov²:** *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 omrežja). Če je pravna podlaga druga (npr. privolitev, zakon...), potem pustite prazno.*
- **Uporabniki ali kategorije uporabnikov osebnih podatkov, če obstajajo:** *Navedite, katerim tretjim osebam se posredujejo osebni podatki (npr. konkretnemu organu, zavodu, podjetju, pogodbenemu obdelovalcu....). Zaposleni pri upravljavcu se ne štejejo za uporabnike.*
- **Informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo:** *Če se podatki prenašajo v tretje države ali mednarodne organizacije, navedite, katere so in podajte ustrezne informacije³.*

Opombe:

1. Informacije posredujete posameznikom, od katerih neposredno zbirate osebne podatke, kot to zahteva 13. člena Splošne uredbe, na različne načine, kot je ustrezno, npr.:
 - Zaposlenim ob zaposlitvi podate takšen ustrezno izpolnjen obrazec z informacijami, katere njihove osebne podatke boste obdelovali kot delodajalec za namene delovnega

¹ Obvestilo je izdano na podlagi določb 1. odstavka 13. člena Splošne uredbe (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 Točka (f) člena 6(1) Splošne uredbe

³ Kadar je ustrezno, dejstvo, da upravljavec namerava prenesti osebne podatke v tretjo državo ali mednarodno organizacijo, ter obstoj ali neobstoj sklepa Komisije o ustreznosti ali v primeru prenosov iz člena 46 ali 47 ali drugega pododstavka člena 49(1) sklic na ustrezne ali primerne zaščitne ukrepe in sredstva za pridobitev njihove kopije ali kje so na voljo.

Obrazec OBV – 22. 6. 2018

razmerja. Obrazec lahko nato objavite tudi na intranetu ali drugemu zaposlenim enostavno dostopnemu mestu.

- **Strankam** na podoben 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 nudenja storitve ali na drug ustrezen način).
 - **Prijavljenim na e-novice in obvestila** lahko te informacije podate na spletni strani ob poljih, v katere vnesejo svoje podatke ali z enostavno dostopno povezavo na takšno besedilo.
2. Upravljalavec bi moral posamezniku, na katerega se nanašajo osebni podatki, zagotoviti vse dodatne informacije, potrebne za zagotavljanje poštene in pregledne obdelave ob upoštevanju specifičnih okoliščin in okvira obdelave osebnih podatkov. V določenih primerih, ko npr. izvajate avtomatizirano odločanje ali profiliranje, je tako treba posameznikom ponuditi tudi dodatne informacije (npr. razloge, pomen in predvidene posledice za posameznika, če ga profilirate) – glejte 2. odstavek 13. člena Splošne uredbe.



Pravica dostopa (15. čl.) – seznanitev z lastnimi OP

1.) Posameznik **ima pravico** od upravljavca dobiti potrditev, ali se njegovi OP obdelujejo, omogočiti vpogled ali posredovati reprodukcijo teh OP (=dostop do OP) + naslednje informacije:

*namene obdelave, vrste OP, **uporabnike ali kategorije uporabnikov** (ki so jim bili ali jim bodo razkriti OP; stališče IP: tu izbira posameznik), če mogoče rok hrambe (sicer merila za določitev tega obdobja), obstoj pravice o možnosti zahtevati popravek/izbris/omejitev obdelave OP/ugovora obdelavi, pravico do vložitve prijave k IP, informacije o viru OP, obstoj avtomatizirane obdelave/profiliranja s posledicami obdelave, seznanitev s prenosom v 3. državo in zaščitni ukrepi.

2.) Upravljavec zagotovi 1 kopijo obdelovanih OP, za dodatne kopije na zahtevo posameznika pa lahko zaračuna razumno (? Pravilnik) pristojbino. Če zahteva po e-poti, se info zagotovijo v splošno uporabljani e-obliki, razen če zahteva drugače. (=problem ugotavljanja identifikacije)



Zahteva za seznanitev z lastnimi osebnimi podatki

Naziv in naziv upravljavca osebnih podatkov:

Zahteva za seznanitev z lastnimi osebnimi podatki

(Vključna vas, da o pred upravljanjem obrazca opredelite priložna [pogoje in razpoložljive](#))

Spodaj podpisani/a (ime in priimek):

(naslov prebivališča):

(drugi kontaktni podatki – po potrebi):

(najstni 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](#) zahteva za seznanitev z osebnimi podatki, ki se nanašajo name (lastnimi osebnimi podatki). Zato vas prosim, da mi (v nadaljevanju [pohvalite](#) je [sve informacije](#) ki jih namrečno želite):

- ☐ potrđite, 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; OPOZORILO: Mašen je vpogled ali pridobitev kopije, kar določite na koncu obrazca);
- ☐ posredujete informacije o namenu 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).



SEZNANITEV Z INFORMACIJAMI O UPORABNIKIH ALI (LE) KATEGORIJAH UPORABNIKOV (čl. 13., 14., 15.)?

Ko upravljavec obvešča posameznika o uporabnikih, ki jim je ali jim bo posredoval njegove OP: razlika 13. - 14. - 15. člen.

Ali mora biti uporabnik konkretno naveden (navedba firme) ali mora biti le opisno opredeljen po področju/nalogi v okviru katere uporabnik obdeluje OP (npr. obdelovalec pooblaščen za IT-podporo; obdelovalec pooblaščen za sklepanje zavarovanj ipd.)?

Priporočena dobra praksa = KONKRETNO NAVEDEN, a razlika:

- 13., 14. čl. = upravljavec odloči, kako bo opredelil uporabnika
- 15. člen: posameznik se odloči, katere informacije o uporabnikih želi (ali konkretni uporabniki ali kategorije uporabnikov)



Varnost obdelave (32. člen)

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) možnostjo zagotoviti stalno **zaupnost, celovitost, dostopnost** in **odpornost sistemov** in storitev za obdelavo;
- (c) možnostjo 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.



Zavarovanje občutljivih OP (14. čl.)

Zahteve ZVOP-1: kriptografske metode, e - podpis

(plačne liste?, občutljivi OP v dokumentih)

Priporočila:

- pošiljanje po e- pošti **z medsebojnim šifriranjem** (varni kanali)
- uporaba kvalificiranih digitalnih potrdil (na obeh straneh komunikacijske poti), uporaba https protokola ter dodatna zaščita z uporabniškim imenom in geslom
- nezavarovan prenos ni dovolj!
- sledljivost!

Oddaljen dostop do zbirk z občutljivimi OP:

- e-podpis (če tudi pisanje, brisanje, popravljanje)



Zavarovanje OP v praksi

Osnovna varnost je lahko / mora biti preprosta.

Strojna oprema – izhodne naprave? Skladno z naravo dela in nalogami: omejitve glede USB ključev, prenosnih medijev, CD/DVD

Samodejno zaklepanje zaslona (ctrl+alt+delete in enter)

Vklop sledenja spremembam (revizijske sledi, dnevniške datoteke).

Gesla (trdnost gesel, dolžina, alfanumerični znaki, hramba gesel 😊)

Nevarnost socialnega inženiringa:

- klici po telefonu – lahko preverimo identito?



Zakaj se to dogaja?

- ☞ radovednost
- ☞ zaslužek s prodajo podatkov
- ☞ nepoznavanje pravil

Kateri podatki so najbolj "zanimivi"?

- ☞ bančni podatki
- ☞ podatki pri operaterjih
- ☞ iz državnih registrov in evidenc
- ☞ zdravstveni podatki

NEUPRAVIČENI VPOGLEDI V OSEBNE PODATKE



Kako jih preprečimo?

1 OMEJITE DOSTOPE NA NUJNE

2 ZAGOTOVITE SLEDLJIVOST DOSTOPOV

TO NI STVAR IT-ja!
IT ne more preprečiti neupravičenih vpogledov.



DOSTOP
do baze

≠

PRAVICA do
vpogleda!

3 OZAVESTITE UPORABNIKE

- ☞ da je neupravičen vpogled kazniv
- ☞ da se njihovi dostopi beležijo
- ☞ da bodo ujeti in kaznovani



4 IZVAJAJTE NOTRANJJI NADZOR

- ☞ o njem obvestite zaposlene
- ☞ lahko je naključen ali na podlagi suma (npr. zaradi odstopajočih statistik)

5 DOKUMENTIRAJTE STANJE

- ☞ sprejmite interna pravila v pisni obliki glede omejitve dostopov in zagotavljanja sledljivosti
- ☞ dokumentirajte aktivnosti ozaveščanja
- ☞ dokumentirajte notranje nadzore



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

a.) v primeru kršitev VOP (razen če ni verjetno, da bodo ogrožene TČP) mora **upraviteljec 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, upraviteljec brez nepotrebnega odlašanja kršitev obvesti **posameznika** (DPO, opis posledic in sprejetih ukrepov) – razen če: *je upraviteljec 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, nepooblaščno 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*)



URADNO OBVESTILO O KRŠITVI VARNOSTI OSEBNIH PODATKOV

- Člen 33 Splošne uredbe o varstvu podatkov (UREDBA (EU) 2016/679) zahteva upravitelja, da obvesti nadzorni organ o kršitvi varnosti osebnih podatkov.
- Obrazec izpolni podjetje ali institucija, 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.ica.si/rokovodilna/informacijska-sistemata-rokovodilnisa-ekipa-za-varnost-osebni-podatki/kli-vanje-podrocje-uredbe/porocila-kratki/>

Vrsta obvestila (Vzorno označi.)	<input type="checkbox"/> Obvestilo o kritiki: (s tem obvestilom o celoti obveščate o kritiki vamost/osebni podatki);	<input type="checkbox"/> Predhodno obvestilo: (obvestilo boste kasneje dopolnili);	<input checked="" type="checkbox"/> Dopolnilni / spremembi: (s tem obvestilom podajate dopolnilni oziroma spremembo predhodnega obvestila);
Opredelite predhodno obvestilo (številka dokumenta, naslov zadeve / druge oznake obvestila) (dopolnite le, če ste označili dopolnilni / spremembi);			
Datum predhodnih obvestil (dopolnite le, če ste označili dopolnilni / spremembi);		Kdaj ste prejeli, če želite vnesti datum;	

1.1 Kontaktni podatki upravitelca

2718



Postopki IP v praksi:

- prijav zoper davčne svetovalce, revizorje/revizorske hiše, računovodje/računovodske servise IP doslej (še) ni prejel;
- prijave zoper nekaj podjetij, ki so zunanjim revizorjem posredovale OP (ni bilo ugotovljenih kršitev);
- jeseni leta 2019 IP prejme DBN računovodskega servisa zaradi kibernetkega vdora v njihov računalniški sistem in izgube dostopa do OP strank.



- **Pripravljen neobvezen obrazec s strani EDPB:**
 - [https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/OBRAZEC -
_Obvestilo o krsitvi 01.docx](https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/OBRAZEC_-_Obvestilo_o_krsitvi_01.docx)
- **Smernice EDPB:**
 - [Smernice v zvezi z uradnim obvestilom o kršitvi varstva VOP](#)
- **Statistika po državah zelo raznolika (od 25.5.2018)**
 - VB: 4000+, Pl: 1700: FR: 600, DA: 1200, GR: 26
 - 80% kršitev ni povezanih z večjimi tveganji
 - Ključna ni statistika, pač pa: *učenje iz DBN-jev, *izogibanje napakam v prihodnosti , *večjo odgovornost zavezancev.

Zavezancem priporočamo sprejem in izvajanje **Politike upravljanja varnostnih incidentov**



Najpogostejše kršitve pri zavarovanju OP

- Poudarek na tehničnih ukrepih, premalo pa organizacijskih
- Interni akti ne ustrezajo (več) dejanskemu stanju
- Ni rednega izobraževanja
- Neurejene dostopne pravice
- Ni sledljivosti obdelave OP
- Neupoštevanje politike čiste mize in zaslona
- Pomanjkljiv nadzor + nejasne pogodbe pri pogodbeni obdelavi
- Premalo pozornosti informacijski varnosti pri razvoju novih rešitev



Dobre prakse

Ne pozabite na organizacijske ukrepe:

- izjave o seznanjenosti z GDPR, ZVOP,
 - obveščenost o beleženju dostopov do OP,
 - izobraževanje,
 - interni nadzor.
-
- določitev odgovorne osebo za (DPO)
 - program ukrepov za izboljšanje varstva OP
 - izobraževanje o socialnem inženiringu.





Kaj so ocene učinkov z zvezi z VOP (DPIA) - kdaj in zakaj?

Orodje za identifikacijo, analizo in zmanjševanje **tveganj** glede nezakonitih ravnanj z OP, do katerih lahko pride pri nekem projektu, sistemu ali uporabi tehnologije

Zakaj so koristne?

- **pravočasno preprečevanje kršitev VOP**
- **ohranitev ugleda in zaupanja** v organizacijo
- izogib **negativnemu medijskemu poročanju**
- izogib **inšpekcijskim postopkom in visokim globam**



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. --→>**



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)



Kaj naslavlja DPIA?

Primeri

- uvedba **videonadzora v stavbi**, kjer je **več organizacij**,
- **sistem za nakup vozovnic**, ki bo v uporabi **na več prodajnih mestih** (en upravljavec),
- Projekti e-uprave, e-pravosodja, e-zdravja...
- **obsežna nagradna igra**, kjer bo podatke sodelujočih dobilo več podjetij (skupni upravljavci).

Koristna tudi za **proizvajalce/ponudnike** tehnoloških rešitev, npr.:

- programska oprema za podporo vodenju šole,
- mobilna aplikacija za rezervacijo in najem vozil,
- razvoj informacijskega sistema za bolnišnice,
- pametni števcji za električno energijo,
- rešitev za hrambo podatkov v oblaku. ----- >>>>



KAKO izvesti DPIA?





KAKO izvesti DPIA?

METODOLOGIJA ni predpisana

- Uporabno:
 - standardi za upravljanje s tveganji ki sledijo ugotovitvi konteksta, oceni tveganj in obvladovanjem tveganj
 - ISO/IEC 31000 – risk management,
 - ISO/IEC 27001 – ožji, kot zahteva DPIA, nanaša se na informacijsko varnost; DPIA na zagotovitev pravic posameznikov; pokrivata se v zvezi z varnostjo OP .
 - Izbira metodologije je prosta – bistveno: **DPIA ni promocijski material** projekta (obdelave) temveč **analiza učinkov na pravice posameznikov in ukrepi za zmanjšanje negativnih učinkov**
 - Primeri metodologij
 - Slo – eUprava, nova policijska pooblastila, brezpilotni letalniki,
 - Tuje smernice/metodologije/vzorci.
 - **Samooceniitveni kriteriji za ustreznost DPIA** po WP 29



Predhodno posvetovanje z IP (36. čl.)

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

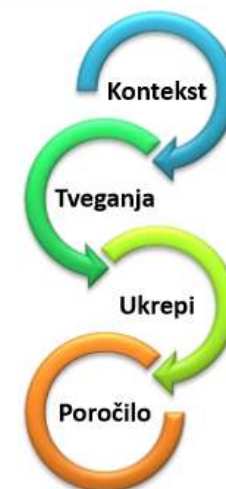
Pri posvetovanju mora upravljavec IP **predložiti**:

- 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.



OCENE UČINKOV NA VARSTVO PODATKOV

Smernice Informacijskega pooblaščenca





Še neizkoriščen potencial - certificiranje in kodeksi ravnanja (prostovoljno)

Kodeksi ravnanja (se pošljejo v potrditev IP)

Združenja, zbornice, zveze idr., ki predstavljajo vrste upravljavcev/obdelovalcev, če želijo večjo skladnost in enotnost izvajanja GDPR

- **Primeri:**

- Enoten obrazec za informiranje posameznika, psevdonimizacije
- Enotna politika obravnave varnostnih incidentov
- Poenotne druge varnostne politike
- Enoten obrazec za evidentiranje dejavnosti obdelave...



Certificiranje

- Potrebno še razviti **akreditacijske** in **certifikacijske sheme**
- Po preglednem postopku, oceniti stroške-koristi
- Certifikate bo podeljeval **akreditiran certifikacijski organ**
- IP predpiše dodatna merila
- Veljavnost **3 leta**, možnost podaljšanja
- **Primeri:** kadrovska funkcija, klub zvestobe, nova mobilna aplikacija, e-banka...





Vgrajeno in privzeto varstvo OP (25. člen) – na dobri poti do uspeha

Kot upravljavci ne zahtevajmo OP na zalogo, za vsak slučaj, „bo že kdaj prav prišlo“, od vseh vnaprej... ampak:



- Le takrat, ko jih potrebujemo,
- Le od oseb, od katerih jih potrebujemo,
- Le OP, ki jih potrebujemo,
- Le za čas, ko jih potrebujemo ali ga točno določa zakon, pogodba, dovoli posameznik.

Vgrajeno in privzeto varstvo OP = ves čas pazite, da se **obdelajo le tisti OP, ki so potrebni za vsak poseben namen obdelave - > MINIMIZACIJA.**

Zlasti pomembno pri razvoju, oblikovanju, izboru in uporabi aplikacij, storitev in produktov, ki temeljijo na obdelavi OP (npr. aplikacije za pametne telefone, zdravstvene spletne strani, klubi zvestobe ipd.).

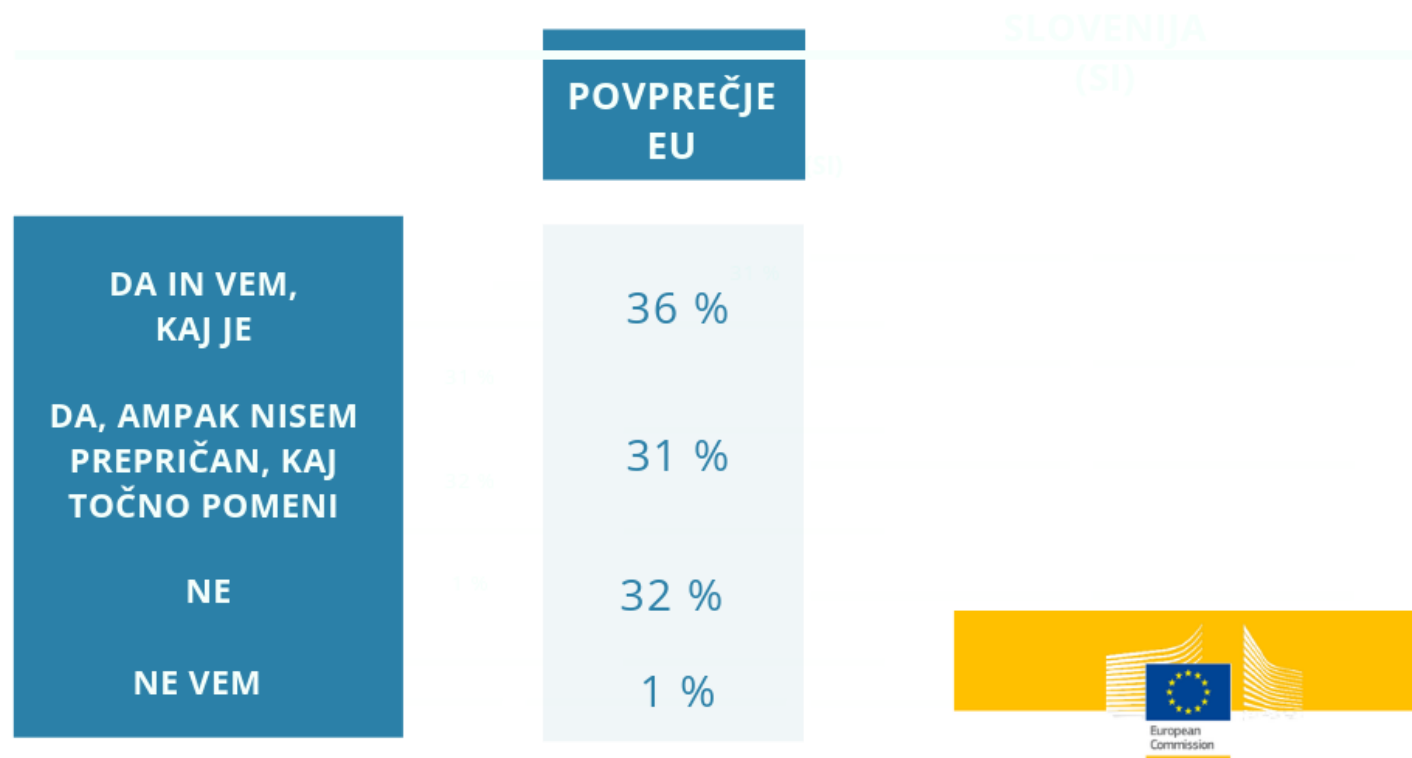


- V pogodbah z zunanjimi izvajalci **imejte klavzulo**, da vas morajo obvestiti, če bi prišlo zaradi njihovega ravnanja ali v njihovih storitvah do kršitve varnosti. Določite **koga** morajo obvestiti, v kakšnem **roku** in na kakšen **način**.
- Priporočljiva je uvedba **obveznega kriptiranja** vseh prenosnih **nosilcev podatkov** (npr. prenosni računalniki, tablice, prenosni zunanji diski, USB ključi ipd.).



Prepoznavnost povsod po EU

Ali ste že slišali za Splošno uredbo o varstvu podatkov (GDPR), ki je stopila v veljavo 2018?





Ali veste, da v vaši državi članici EU obstaja nadzorni organ, ki je pristojen za varstvo pravic s področja osebnih podatkov?

	POVPREČJE EU
DA IN VEM, KATERI ORGAN JE TO	20 %
DA, AMPAK NE VEM, KATERI ORGAN JE TO	37 %
SKUPAJ "DA"	57 % (EB 2015 +20 OT)
NE	41 % (EB 2015 -20 OT)
NE VEM	2 %



Special Eurobarometer 487a



Hvala za pozornost!

gp.ip@ip-rs.si