

# Varstvo osebnih podatkov pri izvajanju kohezijske politike

Ministrstvo za kulturo, 17.4.2024

Anže Novak, univ. dipl. prav.

# Uvod

- Pomen varstva osebnih podatkov in digitalna revolucija
- Varstvo osebnih podatkov je **temeljna človekova pravica** (38. člen Ustave RS)
- Nova pravila, okrepljene pravice in nadzor nad osebnimi podatki – opolnomočenje posameznikov:
  - Splošna uredba (25.5.2018)
  - ZVOP-2 (26.1.2023)
  - Drugi področni predpisi
- Številne obveznosti upravljavcev za zakonito, transparentno, pošteno, varno in odgovorno obdelavo osebnih podatkov.
- Dvig zavedanja posameznikov → število prejetih pritožb/prijav IP
- Bogata praksa IP in judikatura Sodišča EU





## IDENTIFIKACIJSKI

IME IN PRIIMEK, EMŠO, DAVČNA ŠT.,  
GESLO, UPORABNIŠKO IME,  
IP-NASLOV,  
VIN ŠTEVILKA...



## KONTAKTNI

TELEFONSKA ŠTEVILKA,  
EMAIL, NASLOV...

## TRANSAKCIJSKI



NAKUPI, ZDRAVSTVENE  
STORITVE, UPORABA SPLETA,  
PREBRANE KNJIGE, LOKACIJSKI  
PODATKI...



## STATUSNI

ZDRAVJE, PREMOŽENJSKO  
STANJE, PREFERENCE, ŽELJE,  
POROČEN/SAMSKI, IZOBRAZBA,  
STAROST, SPOL, POKLIC...

Ali je posameznik  
**določljiv?**

**vir**

- ni pomemben  
SAM ZBRAL/ DELODAJALEC/  
PODJETJE

**oblika**

- ni pomembna  
ČRKE/ ŠTEVILKE/ VIDEO

**kontekst**

- je zelo pomemben  
KDO, ZAKAJ, KATERE, OD KOGA, KDAJ

Ključno  
vprašanje je,  
**ALI SE DA**  
**določiti**  
posameznika in  
**NE ali ga jaz/mi**  
**znamo**  
**določiti.**

psevdonimizirani  
podatki  
anonimizirani  
podatki

=

**osebni**  
**podatki**

≠



INFORMACIJSKI  
POOBlašČENEC

# Kaj so osebni podatki?

- **Definicija** (člen 4 Splošne uredbe): poenostavljeno → podatek, ki kaže na posameznika, ne glede na obliko, vir ali kontekst
- **Široka interpretacija**
  - Vse vrste informacij, objektivne in subjektivne (mnenja in presoje), če se „nanašajo“ na posameznika
  - Iz zasebnega, poklicnega in javnega življenja
  - Ne le podatki, kijih upravljavec zbere, tudi takšni, ki jih pridobi z dodatno obdelavo
- **Anonimizacija/psevdonimizacija**
  - Anonimizacija: podatki se ne nanašajo na določenega ali določljivega posameznika (NISO OSEBNI PODATKI)
  - Psevdonimizacija: ukrep, s katerim osebnih podatkov ni mogoče pripisati posamezniku brez dodatnih informacij, ki se hranijo ločeno (SO OSEBNI PODATKI)

# Primeri – kaj so/ niso osebni podatki

- **telefonska številka**
  - centrale?
  - mobilna tel. številka?
  - samo številka, brez imena/priimka...?
- **EMŠO, davčna, številka zdravstvenega zavarovanja**
- **IP naslov**
  - računalnika v spletni kavarni?
  - vaše tablice?
- **Psevdonimi**
- **podatki o nakupih, preferencah, statusih**
- **barva las?**
- **marjetica75@gmail.com**
- **prstni odtis**
  - matematična pretvorba vašega prstnega odtisa:  
8271sk3h123khf8 ?



"Your recent Amazon purchases, Tweet score and location history makes you 23.5% welcome here."

# Primeri – kaj so/ niso osebni podatki

- Elektronski naslov podjetja info@podjetje.si
- Elektronski naslov [ime.priimek@podjetje.si](mailto:ime.priimek@podjetje.si)
- Naslov direktorja (ime, priimek, naslov stalnega prebivališča), ki je dostopen v AJPES
- Podatek o lastništvu nepremičnine, ki je dostopen iz evidence
- Registrska oznaka vozila, VIN številka
- Ime in priimek javnega uslužbenca



# Kdaj se uporabljajo pravila varstva osebnih podatkov?



**obdelava osebnih podatkov  
IN  
v celoti ali delno z  
avtomatiziranimi sredstvi  
ALI  
del zbirke ali so namenjeni  
oblikovanju dela zbirke.**

**Če gre za popolnoma  
zasebno ali domačo  
dejavnost se pravila  
varstva osebnih  
podatkov ne uporabljajo.**



**posameznik**

**upravljavec**

**U**



zaupa  
svoje OP,  
uveljavlja  
pravice

zbira OP na eni  
od PRAVNIH  
PODLAG za  
NAMEN



Če gre za popolnoma  
zasebno ali domačo  
dejavnost se pravila  
varstva osebnih  
podatkov ne uporabljajo.

# Načela varstva osebnih podatkov



## Za kršitev katerega načela gre?

ZAKONITOST,  
POŠTENOST,  
PREGLEDNOST

OMEJITEV NAMENA

NAJMANJŠI OBSEG  
PODATKOV

TOČNOST

OMEJITEV  
SHRANJEVANJA

ZAUPNOST IN  
CELOVITOST

ODGOVORNOST

- Udeleženci usposabljanja niso bili seznanjeni s tem, da se dogodek snema
- Avtorska pogodba ni vsebovala določbe, da se delavec obvezuje varovati osebne podatke v skladu s pravili družbe
- Ministrstvo je objekt hekerskega napada, pri katerem pride do šifriranja celotne baze osebnih podatkov.

## Za kršitev katerega načela gre?

ZAKONITOST,  
POŠTENOST,  
PREGLEDNOST

OMEJITEV NAMENA

NAJMANJŠI OBSEG  
PODATKOV

TOČNOST

OMEJITEV  
SHRANJEVANJA

ZAUPNOST IN  
CELOVITOST

ODGOVORNOST

- Za namen preverjanja identitete upravljavec zbira in hrani kopije osebnih dokumentov.
- Delodajalec kopijo diplome, ki jo je pridobil od zaposlenega javno objavi
- Udeleženec usposabljanja brez vednosti organizatorja, fotografira listo prisotnosti z imeni, priimki in telefonskimi številkami prisotnih in kontaktne podatke uporabi za lastno poslovno dejavnost.



posameznik

upravljavec

U



zaupa  
svoje OP,  
uveljavlja  
pravice

zbira OP na eni  
od PRAVNIH  
PODLAG za  
NAMEN

U

Če gre za popolnoma  
zasebno ali domačo  
dejavnost se pravila  
varstva osebnih  
podatkov ne uporabljajo.

#### PRAVNE PODLAGE

- (a) privolitev
- (b) pogodba
- (c) zakonska obveznost
- (d) reševanje ljudi
- (e) oblastna naloga ali javni interes
- (f) zakoniti interes

#### POSEBNE VRSTE OP

(npr.: zdravstveni podatki, spolna usmerjenost, versko, politično, filozofsko prepričanje,...)

#### LEGENDA



posameznik



obdelovalec



člen Splošne uredbe  
(GDPR)



upravljavec



(pod)obdelovalec



osebni podatek

# NAČELO ZAKONITOSTI: Pravne podlage

## Po Splošni uredbi

### Člen 6 – „navadni OP“

a)privolitev

b)pogodba

c)zakonska obveznost

d)reševanje ljudi

e)oblastna naloga ali javni interes

f)zakoniti interes \*

\* ne velja za organe v javnem sektorju, pri izvajanju njihovih nalog

### Člen 9 - posebne vrste OP – dodatni pogoji

(Rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo)

## Po ZVOP-2

**Osebna privolitev** (javni sektor) če tako določa zakon (v okviru javnih pristojnosti), ko ne gre za izvajanje pristojnosti ni treba, da privolitev določi zakon.

**Zakonska obveznost in izvajanje javnih nalog** (točki c. in e., člena 6 Splošne uredbe primarno), zakon mora določiti: *obdelavo osebnih podatkov, vrste osebnih podatkov, kategorije posameznikov, namen obdelave in rok hrambe osebnih podatkov ali rok za redni pregled potrebe po hrambi (dodatno, če je mogoče) uporabniki osebnih podatkov, posamezna dejanja obdelave in postopki obdelave ter drugi ukrepi za zagotovitev zakonite, poštene in pregledne obdelave*

**Izjema za točko 6(1)e** lahko, tisti osebni podatki, ki so **nujno potrebni za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega sektorja, če se s to obdelavo ne poseže v upravičen interes posameznika**

# NAČELO ZAKONITOSTI: Primeri

## Katera pravna podlaga je ustrezna?

- PT za izvedbo projekta sklene avtorsko pogodbo s posameznikom.
- PT pridobi in shrani podatka od skrbnika pogodbe, ki je zaposleni pri izvajalcu
- PT od izvajalcev pridobiva podatke o etnični pripadnosti, invalidnosti, spolu in starosti udeležencev zaradi obveznosti poročanja Evropski komisiji na razpisu.

# NAČELO ZAKONITOSTI: Primeri

## Katera pravna podlaga je ustrezna?

- Delodajalec zbira podatke o nekaznovanosti od kandidata za zaposlitev in zaposlenega.
- Upravni organ vodi dokumentarno gradivo v zvezi z upravnim postopkom.
- Organizator dogodka javno objavi fotografijo iz dogodka, kjer so razpoznavni posamezniki na fotografiji.

# NAČELO ZAKONITOSTI: Primeri

## Katera pravna podlaga je ustrezna?

- Posredniško telo (PT) za izvajanje naloge na podlagi 2 tč., člena 69 UREDBA (EU) 2021/1060, ki določa, da mora država članica zagotoviti oz. zbirati informacije o dejanskih lastnikih prejemnikov sredstev Unije, zbira **podatke o imenu, priimku, datumu rojstva in davčni številki** o dejanskih lastnikih.

# NAČELO ZAKONITOSTI: Privolitve

- Prostovoljna
  - Informirana
  - Konkretna (specifična)
  - Nedvoumna izjava volje
  - Dokazljiva
- **Prostovoljnost** privolitve je vprašljiva v javnem sektorju (če gre za oblastno delovanje) in v delovnem razmerju (nesorazmerje moči)
  - [Več o privolitvi](#)

### Ali je privolitev ustrezna pravna podlaga?

- Delodajalec dovoli zaposlenim uporabo službenega avtomobila za zasebne namene, pod pogojem, da dovolijo sledenje z GPS napravo.
- Delodajalec na podlagi privolitve delavca pridobi njegovo zasebno telefonsko številko za namen lažjega in hitrejšega komuniciranja.

## NAČELO ZAKONITOSTI – primeri privolitev

### Ali je privolitev ustrezna pravna podlaga?

- Upravljavec za **analizo strukture udeležencev seminarja izvede anketo in pridobiva privolitve** anketirancev za obdelavo njihovih osebnih podatkov (starost, stopnja izobrazbe, kraj bivanja)
- Upravljavec želi **objaviti (neanonimne) komentarje udeležencev seminarja**, ki ga je organiziralo (npr. z navedbo konkretnega imena in naziva delodajalca), da bi tako k udeležbi prepričalo tudi bodoče udeležence.

## Posebna ureditev obdelave: Svoboda izražanja in obveščanja

- Splošna uredba: 85. člen – države članice z zakonom usklajujejo pravico do varstva osebnih podatkov na podlagi te uredbe s pravico do svobode izražanja in obveščanja.
- ZVOP-2: 73. člen, 19. člen
  - Določa pogoje za zakonitost obdelave osebnih podatkov za namen svobode izražanja in obveščanja:
    - **Nameni:** obveščanje javnosti s strani medijev, književnega, umetniškega ali raziskovalnega ustvarjanja, resne kritike, obrambe kakšne pravice ali varstva upravičene koristi in izobraževanja ali izobraževanja prek javno dostopnih objav in publikacij.
    - **Pogoji:** privolitev, uporaba podatkov, ki jih je posameznik sam objavil, podatki, ki so bili zakonito pridobljeni, drug zakon določa njihovo javnost...
  - Predpisuje sodno varstvo, ko gre za uveljavljanje pravic (razen za podatke iz zbirke – pristojen je IP).

## Primer - Svoboda izražanja in obveščanja

Medij objavi podatke o ministru in vključi tudi podrobne podatke o njegovi družini in družinskih članih. Ker minister meni, da gre za prekomerno objavo osebnih podatkov, ki presegajo njegovo javno funkcijo, zahteva od medija izbris članka in anonimizacijo osebnih podatkov.

- Ali je minister upravičen do izbrisa?
- Ali bo o izbrisu odločal Informacijski pooblaščenec (IP)?
- Kakšne pravne možnosti ima na voljo minister?

## Primer - Svoboda izražanja in obveščanja

Medij objavi osebne podatke, ki očitno izhajajo iz policijskega zapisnika o hišni preiskavi pri ministru, ki je bil vpleten v korupcijsko afero.

- Če minister zahteva izbris članka od medija – ali bo do izbrisa upravičen?
- Ali bo o pritožbi zoper odločitev medija odločal IP?
- Kako in zoper koga lahko ukrepa IP?

## **Posebna ureditev obdelave: Varstvo pravice do dostopa do informacij javnega značaja v razmerju do pravice do varstva osebnih podatkov**

- Splošna uredba: člen 86 - v skladu s pravom Unije ali pravom države članice, ki velja za javni organ ali telo
- ZVOP-2: 74. člen, 75. člen, 19. člen
  - zakonitost obdelave osebnih podatkov za namen posredovanja informacij javnega značaja se zagotavlja skladno z ZDIJZ.
  - Izključeno je obveščanje posameznika in vabljenje k stranski udeležbi, ko so podatki javni na podlagi zakona

## **Primer – Varstvo pravice do dostopa do informacij javnega značaja v razmerju do pravice do varstva osebnih podatkov**

Ministrstvo mora skladno s sklepom Vlade RS voditi poimenski seznam zaposlenih na področju izvajanja evropske kohezijske politike, in sicer: naziv JU, plačni razred, konkretne delovne naloge. Podatke zbira od ministrstev, zaradi poročanja MJU za analizo obremenjenosti kadrov in posameznih kvot po posameznih resorjih in zaradi poročanja Evropski komisiji v zvezi z izvajanjem te politike.

- Ali je sklep Vlade ustrezna pravna podlaga za obdelavo osebnih podatkov?
- Ali bi podatke pridobil prosilec za dostop do informacij javnega značaja?

## **Primer – Varstvo pravice do dostopa do informacij javnega značaja v razmerju do pravice do varstva osebnih podatkov**

Medij objavi osebne podatke, ki očitno izhajajo iz policijskega zapisnika o hišni preiskavi pri ministru, ki je bil vpleten v korupcijsko afero. Policijski zapisnik je v celoti, brez prikritih osebnih podatkov, mediju posredovala uradna oseba po ZDIJZ pri ministrstvu, ker je ocenila, da je za razkritje podan prevladujoč interes javnosti.

- Kakšna pravna sredstva ima na voljo minister in njegova družina?

## Posebna ureditev: obdelava kontaktnih podatkov

- ZVOP-2: 92
  - NAMEN: **objava kontaktnih podatkov vodilnih oseb in tistih katerih delo je potrebno zaradi poslovanja s strankami oziroma uporabniki storitev**
  - PODATKI: ime, naziv ali funkcijo, službeno telefonsko številko in naslov službene elektronske pošte



## Posebna ureditev: obdelava kontaktnih podatkov

- ZVOP-2: 93
  - NAMEN: **organiziranje uradnih srečanj, izobraževanj, ipd., dajanja izjav za javnost, razen izvajanja neposrednega trženja**
  - PODATKI (za javni sektor): osebno ime, telefonska številka, naslov elektronske pošte ali druga komunikacijska številka/oznaka, podatki o delodajalcu/organizaciji ter podatki o področju dela, položaju, funkciji, članstvu v klubu ali hobiju posameznika – naslov prebivališča le po privolitvi
  - POGOJ: pridobljeni iz javno dostopnih virov ali v okviru izvrševanja svojih javnih nalog, če so ji jih posamezniki prostovoljno razkrili ali dali privolitev.

## Posebna ureditev: obdelava kontaktnih podatkov

- ZVOP-2: 93
  - NAMEN: za **obveščanje javnosti** sme oseba javnega ali zasebnega sektorja obdelovati OP, vključno z objavo
  - PODATKI: **osebna imena, nazive, fotografije in videoposnetke posameznikov,**
  - POGOJ:
    - pridobljene na dogodkih, ki jih v okviru svojih nalog, pristojnosti ali dejavnosti organizira ta oseba,
    - če posameznik te obdelave ni prepovedal.

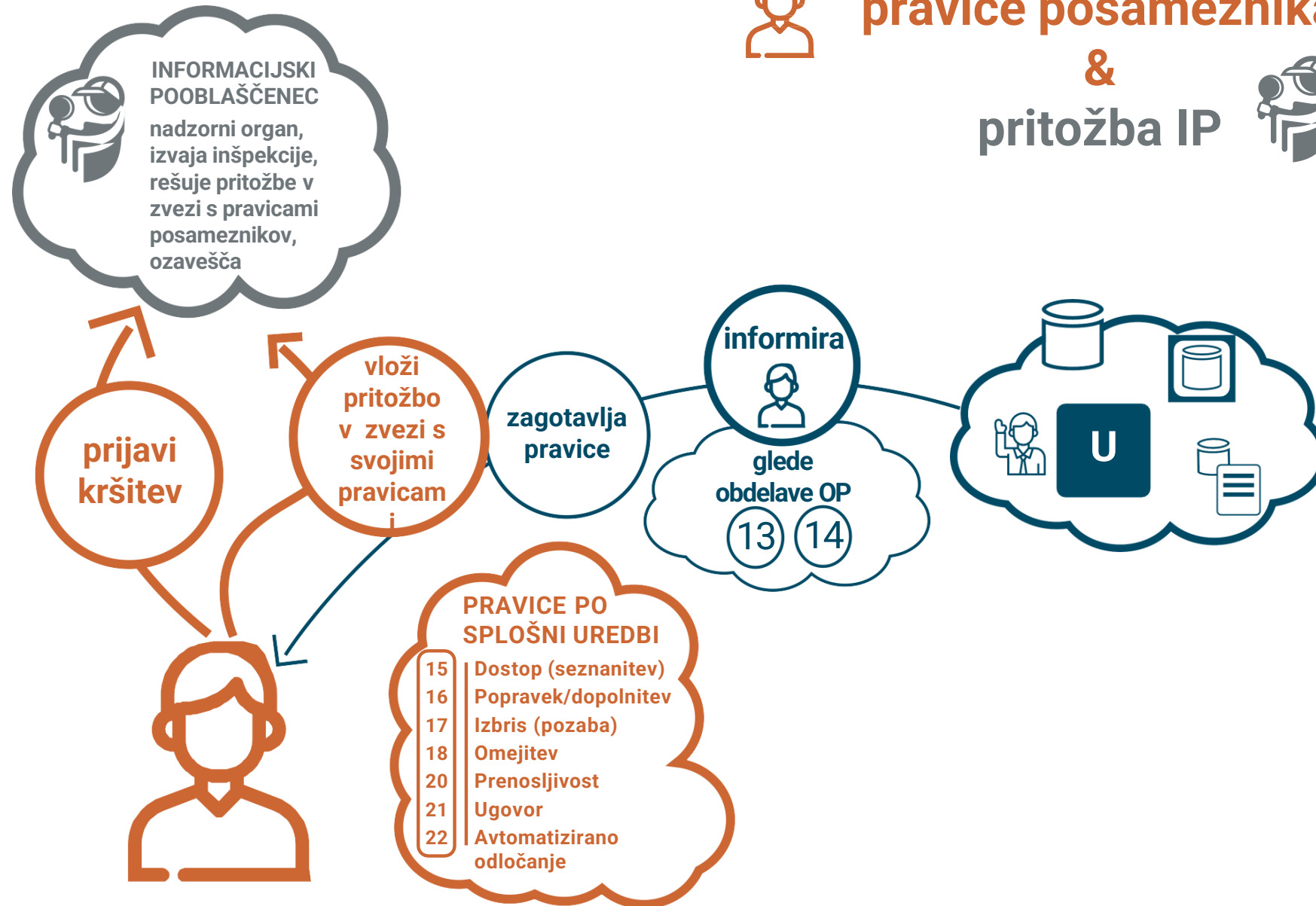
## Posebna ureditev: obdelava kontaktnih podatkov

- ZVOP-2: 94. člen obdelava osebnih podatkov iz uradnega identifikacijskega dokumenta
  - NAMEN: za namen **identifikacije posameznika ali** za namen **zagotavljanja točnosti in posodobljenosti** osebnih podatkov
    - Zasebni sektor: **vpogledati** v njegove uradne identifikacijske dokumente
    - Javni sektor: tudi **prepisati**, kopirati ali drugače obdelati podatke iz tudi prepisati, kopirati ali drugače obdelati podatke iz njegovih uradnih identifikacijskih dokumentov.
  - PODATKI/ZBIRKA: **Uradni identifikacijski dokument**: osebna izkaznica, potni list, obmejna prepustnica, vozniško dovoljenje, orožni list in uradni identifikacijski dokumenti drugih držav ali mednarodnih organizacij.

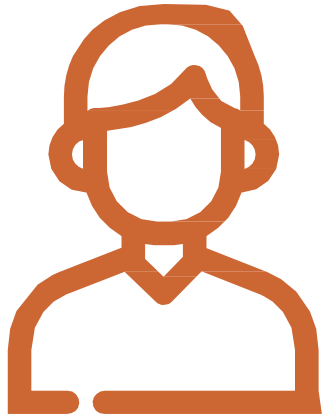


# pravice posameznika &

## pritožba IP



# Informiranje/obveščanje posameznikov



13

14

75

GDPR

ZVOP-2

## Načelo preglednosti:

- ✓ Obveznost upravljavca
- ✓ **Vsebina: bistvene vidike obdelave**
  - KDO zbira,
  - ZAKAJ in na KATERI PODLAGI,
  - za KOLIKO ČASA,
  - KOMU PODATKE POSREDUJE,
  - ali se prenašajo v tretje države...
- ✓ člen 13 Splošne uredbe, ko se podatke zbira od posameznika; člen 14 ko se podatke zbira od tretjih oseb (razlika zlasti **informacija o viru**)
- ✓ Izjeme od obveznosti obveščanja – določene z zakonom (75. člen ZVOP-2, podatki ki so javni po zakonu)
- ✓ Več o informiranju posameznikov: [Spletna stran IPRS](#)

# Informiranje/obveščanje posameznikov

13(1)

GDPR

## Katere informacije je obvezno zagotoviti?

- ✓ **identiteto in kontaktne** podatke upravljavca in njegovega predstavnika, kadar ta obstaja;
- ✓ kontaktne podatke **pooblaščene osebe** za varstvo podatkov, kadar ta obstaja;
- ✓ **namene**, za katere se osebni podatki obdelujejo, kakor tudi **pravno podlago** za njihovo obdelavo;
- ✓ kadar obdelava temelji na **točki (f) člena 6(1), zakonite interese**, za uveljavljanje katerih si prizadeva upravljavec ali tretja oseba;
- ✓ **uporabnike ali kategorije uporabnikov** osebnih podatkov, če obstajajo;
- ✓ 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.

# Informiranje/obveščanje posameznikov

13(2)

GDPR

**Katere informacije je tudi obvezno zagotoviti, če je ustrezno?**

- ✓ **obdobje hrambe** ALI merila, ki se uporabijo za določitev tega obdobja;
- ✓ **obstoj pravice** (dostop, popravek, izbris osebnih podatkov, omejitev obdelave, ugovor, prenosljivosti);
- ✓ da se lahko **privolitev** kadar koli **prekliče**;
- ✓ pravico do vložitve **pritožbe pri nadzornem organu**;
- ✓ ali je zagotovitev osebnih podatkov **obveznost** (zakonska / pogodbeno, ki je potrebna za sklenitev pogodbe) in **kakšne so posledice, če ne**
- ✓ obstoj **avtomatiziranega sprejemanja odločitev**, vključno z oblikovanjem profilov iz člena 22(1) in (4), 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.

# Razlogi ko informacij ni treba zagotoviti?

13(2)

GDPR

## ▪ INFORMACIJE SE ZBIRAJO OD POSAMEZNIKA



- Posameznik informacije že ima;

### IZJEME:

- **Ko zakon določa**, da obveščanje ni potrebno, npr. obveščanje o razkritju javnih podatkov po ZDIJZ (75 ZVOP-2)

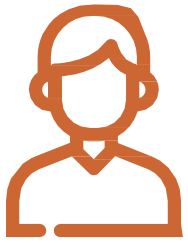
## ▪ INFORMACIJE SE NE ZBIRAJO OD POSAMEZNIKA

- Posameznik informacije že ima;
- Nemogoče ali bi vključevalo; nesorazmeren napor (arhiviranje, raziskovanje, statistika);
- Je pridobitev ali razkritje izrecno določeno s pravom Unije ali pravom države članice;
- poklicna skrivnost.

## Primer – Obveščanje posameznikov

PT v vlogah na javni razpis pridobi osebne podatke zaposlenih pri izvajalcu.

- Ali je PT dolžan obveščati posameznike o obdelavi?



## Pravice posameznika po Splošni uredbi

15

16

17

18

20

21

22

GDPR

### Pravice - vsebina:

- ✓ Dostop (seznanitev)
- ✓ Popravek/dopolnitev
- ✓ Izbris (pozaba)
- ✓ Omejitev
- ✓ Prenosljivost
- ✓ Ugovor
- ✓ Avtomatizirano odločanje

# Pravica dostopa ali seznanitve z lastnimi osebnimi podatki

15

GDPR

## Splošna uredba: člen 15

- Potrditev obdelave
- Dostop
- Informiranje

## Namen pravice do dostopa in informacij je, da se posameznik:

- **Seznani** z obdelavo
- **Razume**, kako se osebni podakti obdelujejo in kakšne so posledice takšne obdelave
- **Preveri** zakonitost, točnost, itd.
- **Uveljavlja** druge pravice (npr. do popravka, izbrisa, ugovora, odškodnine)

## Pravica ni odvisna od tega:

- Ali upravljavec obdeluje majhno ali veliko količino podatkov?
- Kakšna je narava podatkov?
- Zakaj posameznik uveljavlja pravico?

# Pravica dostopa ali seznanitve z lastnimi osebnimi podatki

## POTRDITEV OBDELAVE – DA/NE

### DOSTOP

- Vpogled/reprodukcija – določi prosilec (če reprodukcija ni mogoča, vpogled le s soglasjem prosilca)
- Če zahteva elektronsko, se mu pošlje splošno dostopnem odprtem format (ne v plačljivi programski opremi)
- Razlikovati:
  - Pravica do vpogleda v upravni spis (82. člen ZUP)
  - Pravica dostopa do informacij javnega značaja (ZDIJZ)
- Stroški
  - Prva kopija brezplačna
  - Za nadaljnje kopije lahko upravljavec zaračuna razumno pristojbino ob upoštevanju upravnih stroškov (=le materialni stroški, pravilnika še ni)

# Pravica dostopa ali seznanitve z lastnimi osebnimi podatki

## INFORMIRANJE

- Namen
- Vrste OP
- Uporabniki – notranji /zunanji (zadeva C-579/21)
- Obdobje hrambe
- Katere pravice ima v zvezi s to obdelavo
- Pravica do pritožbe pri IP
- Viri
- Avtomatizirane odločitve: ali se sprejemajo (npr. credit scoring), ali se posameznika profilira in kakšne so posledice



# Primeri – Pravica dostopa

## Pogosti primeri DOSTOPA

- Zahtevam vse podatke, ki jih hranite o meni (razčistiti obseg)
  - Dostop do kadrovskih evidenc
  - Dostop do zvočnih posnetkov sej / klicov na center nujne medicinske pomoči
  - Dostop do posnetkov videonadzornih kamer
- \* Seznanitev z zdravstveno dokumentacijo (Zakon o pacientovih pravicah)

## Pogosti primeri zahtev po INFORMACIJAH

- Katere podatke vodite o meni in v katerih evidencah?
- Kdo in kdaj je dostopal do mojih osebnih podatkov (sledljivost)
- Komu ste posredovali moje podatke in zakaj?
- Kakšno pravico imate da obdelujete moje podatke (pravna podlaga)

## Razlogi, ki opravičujejo izbris

- osebni podatki **niso več potrebni** za namen, za katere so bili zbrani
- posameznik, na katerega se nanašajo osebni podatki, **prekliče privolitev**
- Izbris po uspešnem **ugovoru**
- osebni podatki so bili **obdelani nezakonito** (npr. pomotoma zbrani, brez pravne podlage)
- Rok hrambe je potekel in **zakon določa obveznost izbrisa**.

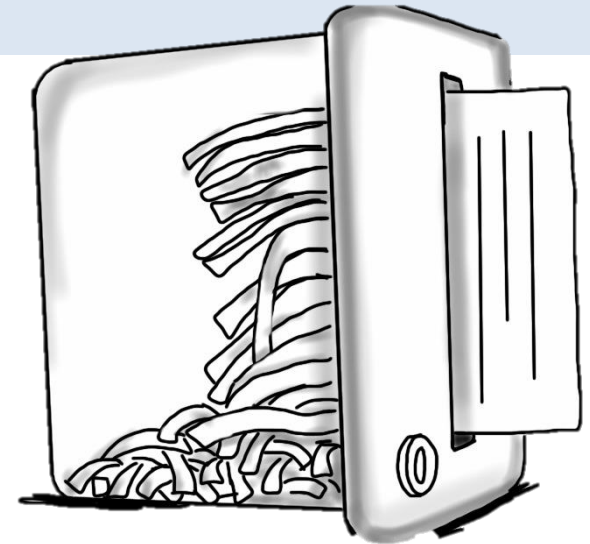
## Kdaj pravica do izbrisa ne bo uspešna?

- Uresničevanje svobode izražanja in obveščanja
- Obdelavo obvezno določa zakon (npr. matične knjige)
- Določeni nameni javnega interesa (javno zdravje, arhiviranje, statistika)
- Uveljavljanje, izvajanje ali obramba pravnih zahtevkov

# Primeri – Pravica do izbrisa

## Pogosti primeri IZBRISA

- Izbrišite me iz baze prejemnikov e-obvestil
- Zahtevam izbris iz seznama prejemnikov subvencij Eko sklada
- Zahtevam izbris podatka, da sem bil hospitaliziran v psihiatrični bolnišnici
- Odslužil sem zaporno kazen, želim da me izbrišete iz medijskih člankov



## Pravica do popravka

16

GDPR

- Popravek netočnih
- Dopolnitev nepopolnih
- Netočnost in potrebo po dopolnitvi je treba dokazati

### Primeri

- Sprememba podatkov v zbirkah fakultete: v evidencah praviloma DA, na diplomi NE
- Izjava zaposlene A, da je B lažnivka – dokazuje se kaj je A rekla, ne pa kaj je res.
- Zdravstvo: po ZPacP se ne spreminja zdravstvene dokumentacije, lahko pa se doda pripombe

# Pravice – postopek za državne organe

12

13

15

16

18

19

20

21

12

GDPR

ZVOP-2

- ✓ **Postopkovna pravila:** subsidiarno ZUP,
- ✓ **Rok:** najkrajši možni čas, najkasneje 1 mesec (izjemoma možnost podaljšanja za dva dodatna meseca)
- ✓ **Posebnost odločbe:** obvezna opredelitev omejitve pregleda spisa v izreku (če je z zakonom določena omejitev pravic)
- ✓ **Izvršba:** Informacijski pooblaščenec
- ✓ **Stroški:** za posameznika praviloma brezplačno, izjema: očitno neutemeljene ali pretirane zahteve – v tem primeru samo materialne stroške posredovanja
- ✓ **Obvezno zavarovanje dokumentacije v času teka postopka**

# Posredovanje osebnih podatkov – javni sektor



1. pravna podlaga za posredovanje v skladu s 6. členom ZVOP-2, ter na podlagi zahteve iz prvega odstavka 41. člena tega zakona
2. Zahteva iz 41. čl. ZVOP-2: pravna podlaga za pridobitev

## POSTOPEK:

1. Prejem zahteve
2. Rok za odločitev o zahtevi: 15 dni
3. Pravno sredstvo:
  - posredovanje osebnih podatkov iz uradnih evidenc ali javnih knjig → Informacijski pooblaščenec odloči o pritožbi
  - posredovanje iz drugih zbirk → nepravdno sodišče

**OBVEZNA HRAMBA SLEDI POSREDOVANJA ŠE 2 LETI:** kateri osebni podatki so bili posredovani, komu, kdaj in na kateri pravni podlagi, za kateri namen oziroma iz katerih razlogov oziroma za potrebe katerega postopka





posameznik

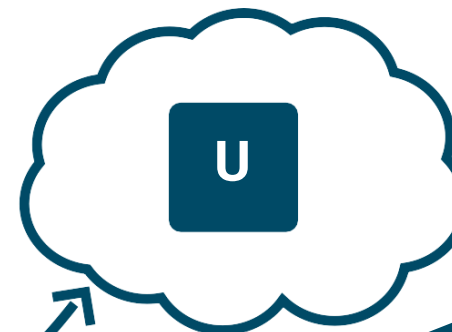
upravljavec

U



zaupa  
svoje OP,  
uveljavlja  
pravice

zbira OP na eni  
od PRAVNIH  
PODLAG za  
NAMEN



Če gre za popolnoma  
zasebno ali domačo  
dejavnost se pravila  
varstva osebnih  
podatkov ne uporabljajo.

#### PRAVNE PODLAGE

- (a) privolitev
- (b) pogodba
- (c) zakonska obveznost
- (d) reševanje ljudi
- (e) oblastna naloga ali javni interes
- (f) zakoniti interes

#### POSEBNE VRSTE OP

(npr.: zdravstveni podatki,  
spolna usmerjenost, versko,  
politično, filozofsko  
prepričanje,...)

#### LEGENDA



posameznik



obdelovalec



člen Splošne uredbe  
(GDPR)



upravljavec

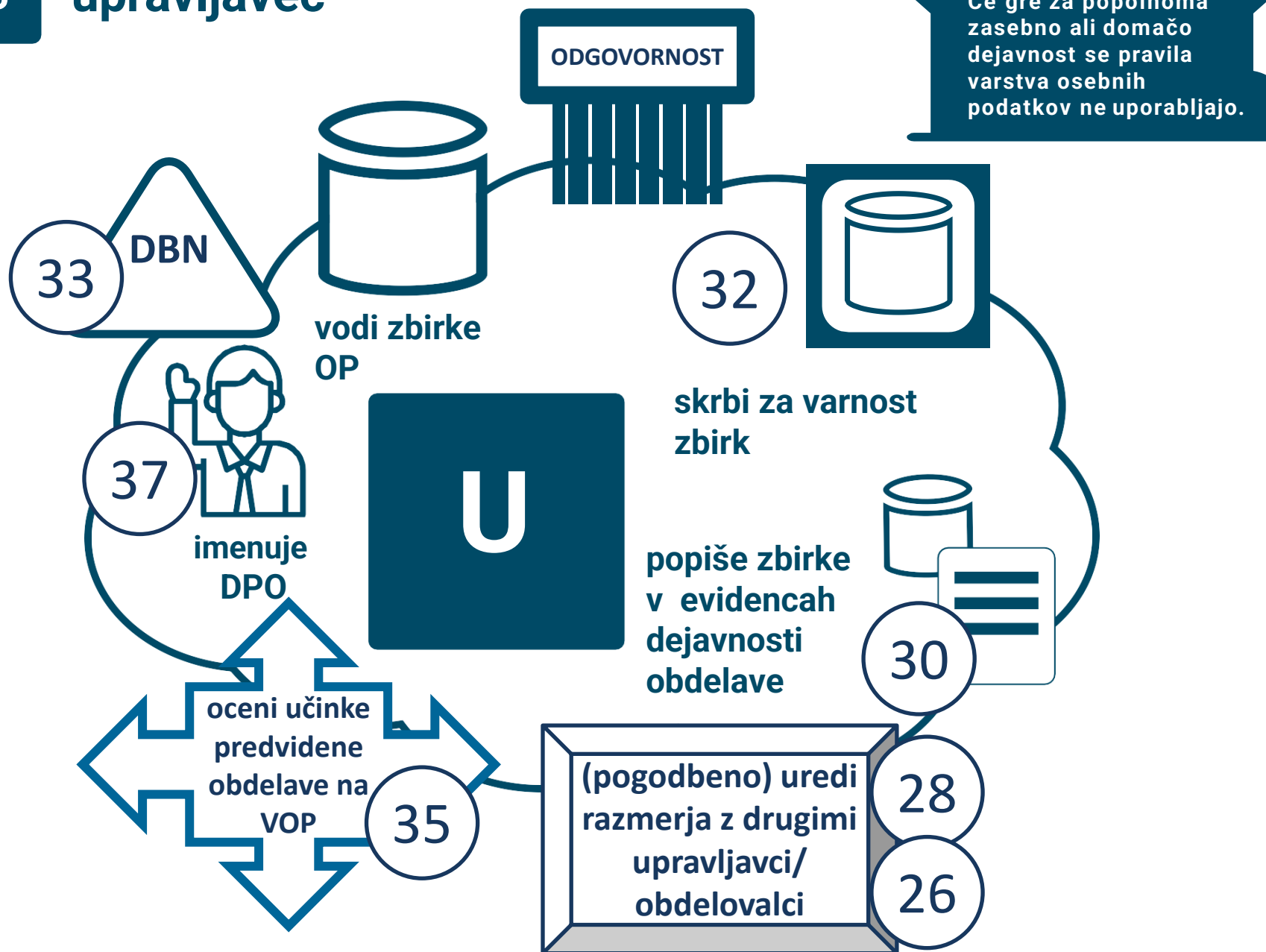


(pod)obdelovalec



osebni podatek

# U upravljavec



# Odgovornost upravljavca, vgrajeno in privzeto varstvo osebnih podatkov



5(2)

24

25

GDPR

## Zagotavlja in izkazuje skladnost:

- ✓ **Pripravi** interne pravilnike, pravila, politike VOP
- ✓ **skrbi za izvajanje** sprejetih pravil
- ✓ periodično **preverja ustreznost** sprejetih pravil, protokolov (glede na tehnični napredek in pravni razvoj)
- ✓ **obvezno dokumentira vse pomembnejše dogodke** (uveljavljanje pravic, ocena učinkov, varnostni incident...)

# Varnost



32

22

23

GDPR

ZVOP-2

## Upravljavec zagotavlja varno obdelavo:

- ✓ Sprejme ustrezne tehnične in organizacijske ukrepe glede na tveganje, da zagotovi: **celovitost, zaupnost in razpoložljivost podatkov.**
- ✓ Kjer je potrebno zagotavlja sledljivost vpogledov/posredovanj (**dnevnik obdelav, posredovanje osebnih podaktov**)
- ✓ varnost na **področju posebnih obdelav**



## Dnevnik obdelav

### Kdaj je obvezen?

- Ko se v avtomatiziranih sistemih obdelave osebnih podatkov izvajajo obsežne obdelave posebnih vrst osebnih podatkov, ali
- kadar gre za redno in sistematično spremljanje posameznikov, ali
- kadar je z oceno učinka ugotovljeno tveganje, ki ga je mogoče učinkovito upravljati z vodenjem dnevnika obdelave, ali
- če tako določa zakon.

### Kaj mora beležiti?

Zbiranje, spreminjanje, vpogled, razkritje, vključno s prenosi, izbris, druga dejanja obdelave, ki jih določa zakon.

### Katere podatke mora vsebovati posamezni zapis?

Vrsto dejanja obdelave (narava); datum in čas obdelave; identifikacijo osebe, ki je izvedla dejanje obdelave; identifikacijo uporabnikov; dodatne vsebine (določi upravljavec) ob upoštevanju ocene učinka.



## Dnevnik obdelav

### **Zakaj se ga sme uporabljati (nameni)?**

Za izkazovanje zakonitosti obdelave, izvajanje notranjega nadzora, izvajanje nadzorov ali drugih zakonsko določenih preverjanj s strani nadzornega organa ali drugih pristojnih organov, zagotavljanje celovitosti in varnosti osebnih podatkov ter za odpravljanje napak v delovanju informacijskega sistema ali obdelavi podatkov

### **Koliko časa se mora podatke v dnevniku hraniti?**

- dve leti od zaključka koledarskega leta in
- največ 5 let (kadar je z oceno učinka ali analizo upoštevni tveganj ugotovljeno tveganje, ki ga je mogoče učinkovito upravljati s podaljšanjem roka)

**Rok za uskladitev:** 2 leti od pričetka veljavnosti ZVOP-2 (**do 26.1.2025**)

**Predvidena globa:** 4.000 - 12.000 / 8.000 – 36.000; 400 – 4.000 za odgovorno osebo državnega organa



## Varnost na področju posebnih obdelav

23

ZVOP-2

### V informacijskih sistemih:

- Na področjih upravnih notranjih zadev, finančne uprave, državljanstva, SOVA, zdravstvenega varstva, obveznega zdravstvenega zavarovanja, uveljavljanja pravic iz javnih sredstev ter kazenskih in prekrškovnih evidenc;
- se obdeluje več kot 100.000 posameznikov na podlagi zakona, razen videonadzora;
- upravljavec ali obdelovalec kot temeljno dejavnost izvajata obsežno obdelavo posebnih vrst osebnih podatkov;
- posebne vrste osebnih podatkov več kot 10.000 posameznikov.



## Varnost na področju posebnih obdelav

23

ZVOP-2

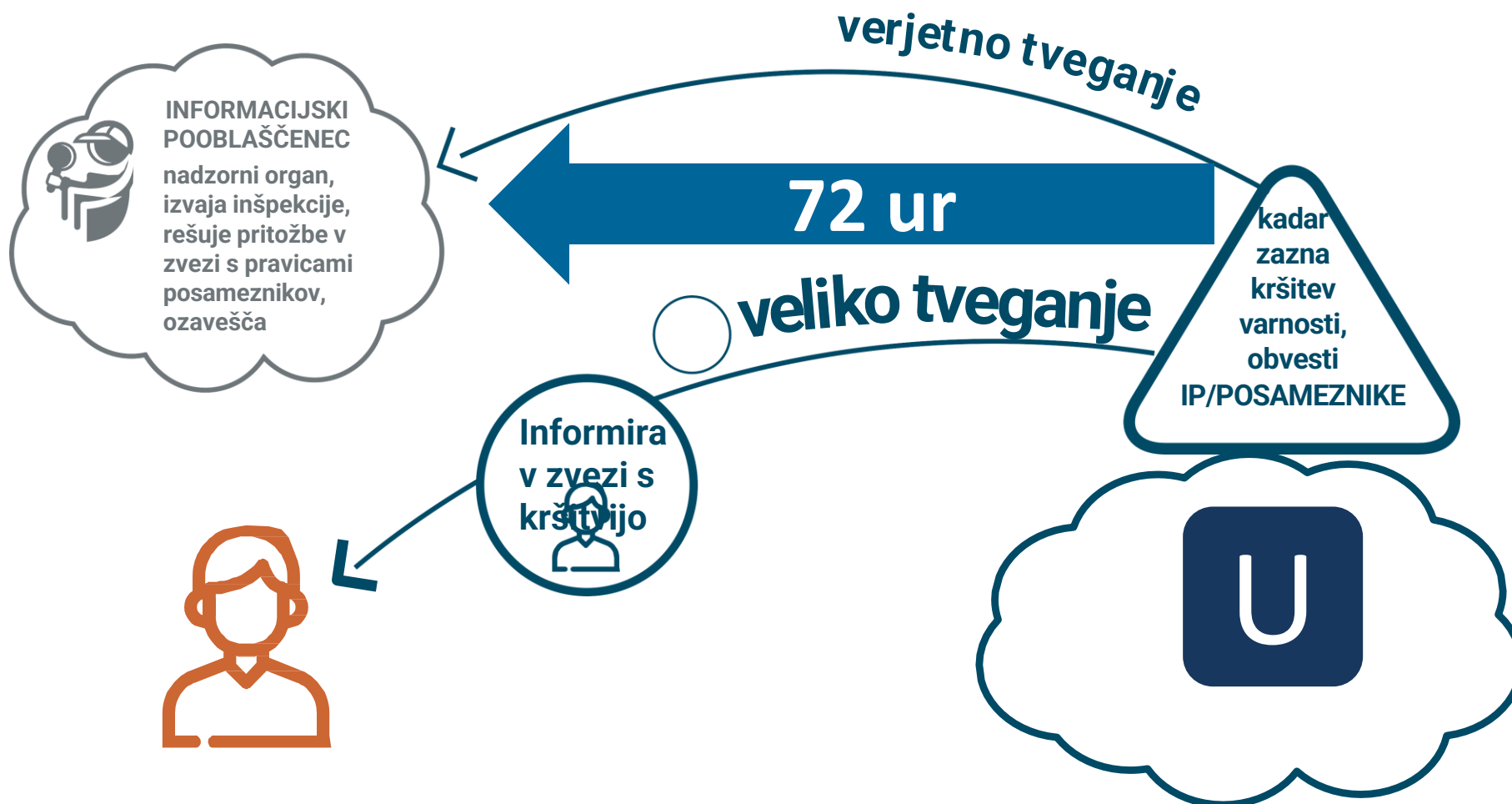
### Kakšne so obveznosti?

- Smiselna uporaba Zakona o informacijski varnosti (ZInfV) glede varnostnih zahtev in priglasitve incidentov
- ko upravljavci v javnem sektorju izvajajo posebne obdelave, pri čemer obdelujejo **biometrične podatke, zdravstvene podatke ali podatke iz prekrškovnih evidenc** je prepovedana hramba, če fizična lokacija hrambe ni znana v vseh fazah postopka.
- **Obvezna ocena učinkov**, pri kateri je treba upoštevati tudi škodljive posledice za varnost države; obveznost izvedbe DPIA tudi ob spremenjeni pravni podlagi
- IP mora v letnem načrtu opredeliti te nadzore
- **Obvezno imeti pooblaščen osebno (DPO)**

**Rok za uskladitev:** 3 leta od veljavnosti ZVOP-2 (do 26. 1. 2026)



## prijava kršitev varnosti (Data Breach Notification)



# PRIJAVA KRŠITEV VARNOSTI ("data breach notification")

## 1 U ZAZNA KRŠITEV

### KRŠITEV VARNOSTI

povzroči nenamerno /nezakonito:

razkritje ali dostop do osebnih podatkov nepooblaščenim (ZAUPNOST)



spremembo (CELOVITOST)



izgubo dostopa ali uničenje (RAZPOLOŽLJIVOST)



### POT OBVEŠČANJA:



obvesti



obvesti



IN/ALI

### PRIPOROČILA

1. POGODBA O OBDELAVI  
NAJ UREJA  
OBVEZNOST  
POROČANJA



(pogodba mora vsebovati podrobna določila, kdaj in kdo pri obdelovalcu obvesti upravitelja)

2. INTERNO UREJEN  
POSTOPEK  
(VSAK v



organizaciji mora vedeti **KOMU** in **KAJ** sporočiti, ko naleti na kršitev varnosti, **KDO** evidentira kršitev in **KOMU** poroča)

## 2 U OCENI TVEGANJE



verjetnost



resnost

### KRITERIJI:

Vrsta kršitve

Narava, občutljivost in količina osebnih podatkov

Enostavnost identifikacije posameznikov (posredno, neposredno, šifrirani...)

Resnost posledic za posameznike

Posebne značilnosti posameznika

Posebne značilnosti U (npr. bolnišnica ali oglaševalec)

Število prizadetih posameznikov

Izdelava OCENE TVEGANJA za VSAKO kršitev je ključna za pravočasno in ustrezno ukrepanje!!!

**U** MORA interno dokumentirati VSAKO kršitev varnosti NE GLEDE NA UGOTOVLJENO TVEGANJE

### legenda



UPRAVLJAVEC



INFORMACIJSKI POOBlašČENEC



OBDELOVALEC



POSAMEZNIK

## 3 U UKREPA

### NIZKO TVEGANJE



INTERNO (lastna evidenca)

#### PRIMERI:

Izguba USB ključka z osebnimi podatki, ki so šifrirani in upravitelj ima kopijo.  
Nekaj minutni izpad elektrike v klicnem centru onemogoči strankam, da pridobijo telefonsko zvezo z upraviteljem, da lahko dostopajo do svojih zbirk.

### VERJETNO TVEGANJE

verjetno, da so ogrožene pravice in svoboščine



obvesti



#### PRIMERI:

Izguba USB ključka, podatki niso bili varno šifrirani.  
Izguba šifriranih kopij, U nima varnostnih kopij.  
Izsiljevalski napad povzroči šifriranje vseh podatkov in U nima varnostnih kopij (lahko da je treba obvestiti tudi posameznike)

### VELIKO TVEGANJE

za pravice in svoboščine



obvesti



#### PRIMERI:

V kibernetnem napadu ukradejo številke kreditnih kartic gostov hotela.  
Bančni komitent je prejel izpisek drugega komitenta (včasih - odvisno od občutljivosti podatkov).  
Na spletu se objavijo uporabniška imena, gesla in zgodovina nakupov strank spletne trgovine.



**www.ip-rs.si:**  
Prijava kršitev varnosti

**obrazec:**  
Uradno obvestilo o kršitvi varnosti osebnih podatkov



INFORMACIJSKI POOBlašČENEC

## Primeri – Kršitev varnosti (1)

Informacijski sistemi v organa javne uprave so bili izpostavljeni kibernetickemu napadu. Podatki v sistemih so bili šifrirani z najsodobnejšim šifrirnim algoritmom. Dešifrirni ključ ni bil ogrožen. Napadalec je imel dostop le do šifriranih osebnih podatkov. Kršitev ni vplivala na sistem elektronske pošte niti na sisteme strank, ki so bili uporabljeni za dostop do njega. Preiskava incidenta je pokazala, da so na voljo dnevniki, ki sledijo vsem podatkovnim tokovom, ki zapustijo organ (vključno z odhodno epšto). Analiza dnevnikov in podatkov je potrdila, da je storilec podatke samo šifriral, ne da bi jih eksfiltriral (iz dnevnikov ni razviden noben izhodni podatkovni tok v časovnem okviru napada). Varnostna kopija je bila takoj na voljo in podatki so bili obnovljeni nekaj ur po napadu. Kršitev ni imela nobenih posledic za vsakodnevno delovanje upravljavca. Pri rednem poslovanju organa ni prišlo do zamud.

## Primeri – Kršitev varnosti (1)

- Kako je želel napadalec onemogočiti delovanje organa? Za kakšno vrsto kršitve gre (zaupnost, celovitost, razpoložljivost)?
- Katere varnostne ukrepe je organ sprejel PRED KRŠITVIJO?
- Katere ukrepe je sprejel PO KRŠITVI?
- Ali je organ dolžan o tej kršitvi obvestiti Informacijskega pooblaščenca?
- Ali je organ dolžan to kršitev dokumentirati?
  
- Če organ iz prejšnjega primera ne bi uporabljal najsodobnejšega šifrirnega orodja ali pa bi bil šifrirni ključ ogrožen – katera vrsta kršitve bi nastopila?
- Kaj pa, če varnostne kopije v elektronski obliki ne bi bilo – katera vrsta kršitve bi nastopila?
- Ali se v teh primerih tveganje poveča in ali bi bilo treba v teh primerih obvestiti IP?

## Primeri – Kršitev varnosti (2)

Informacijski sistem bolnišnice je bil izpostavljen kibernetickemu napadu, napadalec pa je šifriral velik del njenih podatkov. V preiskavi incidenta je bolnišnica potrdila, da je storilec podatke samo šifriral, ne da bi jih eksfiltriral. Osebni podatki, na katere je kršitev vplivala, se nanašajo na zaposlene in paciente, kar je skupaj več tisoč posameznikov. Na voljo so bile varnostne kopije v elektronski obliki. Večina podatkov je bila obnovljena, vendar je ta postopek trajal dva delovna dneva in je povzročil precejšnje zamude pri zdravljenju pacientov, saj so bile operacije odpovedane oziroma odložene, raven storitev pa se je zaradi nerazpoložljivosti sistemov znižala.

- Ali je kršitev povzročilo večje tveganje za pravice in svoboščine posameznikov?
- Ali je treba o kršitvi obvestiti IP?
- Ali je treba o kršitvi obvestiti posameznike?

## Primeri – Kršitev varnosti (3)

Zavod za zaposlovanje je bil žrtev kibernetkega napada, s katerim je bila na njegovo spletno mesto nameščena zlonamerna koda. Zaradi te zlonamerne kode so bili osebni podatki, ki so bili poslani prek spletnih obrazcev za prijavo za delovno mesto in shranjeni na spletnem strežniku, dostopni nepooblaščenim osebam. Kršitev bi lahko vplivala na 213 takih obrazcev, vendar je bilo po analizi podatkov, ki so bili predmet kršitve, ugotovljeno, da kršitev ni vplivala na nobeno posebno vrsto podatkov. Poseben nameščen paket zlonamerne programske opreme je vključeval funkcije, ki so napadalcu omogočale, da je odstranil vso zgodovino eksfiltracije podatkov, ter spremljanje obdelave v strežniku in zajemanje osebnih podatkov. Paket je bil odkrit šele mesec po njegovi namestitvi.

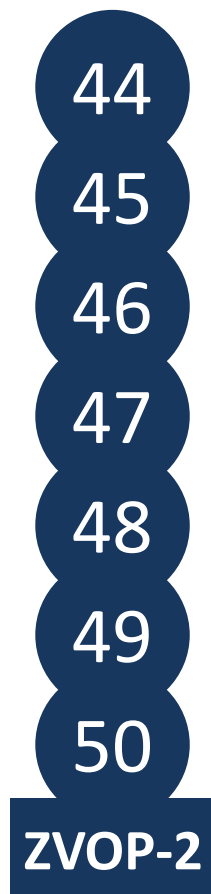
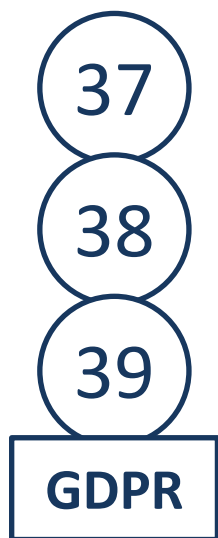
- Kako bi moral zavod odreagirati na kršitev?
- Ali je dolžan o tem obvestiti posameznike?

## Primeri – Kršitev varnosti (4)

Zaposleni v državnemu organu med odpovednim rokom kopira podatke iz podatkovne zbirke organa. Pooblaščen je za dostop do podatkov samo za opravljanje svojih delovnih nalog. Več mesecev pozneje, po prenehanju delovnega razmerja, tako pridobljene podatke (osnovne kontaktne podatke) uporabi za obdelavo novih podatkov, ki jih upravlja, da bi navezal stik s strankami in jih privabil k svojemu novemu poslu.

- Kako bi moral organ odreagirati na kršitev?
- Ali je dolžan o tem obvestiti posameznike?

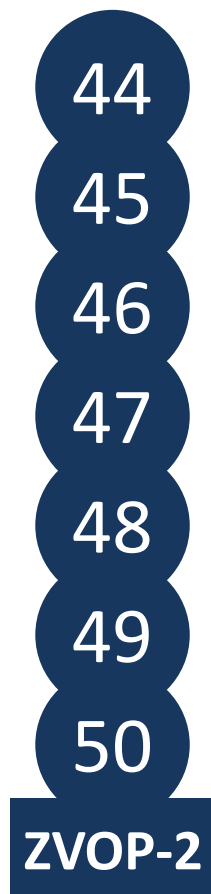
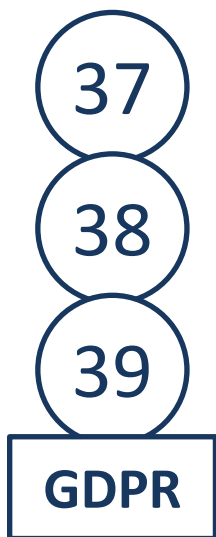
# Pooblaščenca oseba za varstvo osebnih podatkov (DPO)



## DPO

- ✓ izvaja svetovalne in nadzorne naloge
- ✓ notranja / zunanja / skupna
- ✓ državni organi: obvezno notranji, lahko skupna
- ✓ minimalne zahteve glede kdo je lahko DPO
- ✓ nasprotja interesov (absolutno **NE**: upravljavec IS, skrbnik IS, ali vodja informacijske varnosti, predstojnik, sistemsko odloča o obdelavi OP...)

# Pooblaščenca oseba za varstvo osebnih podatkov (DPO)



## DPO

- ✓ nasprotja interesov (relativno: koliščine, ki predstavljajo ali bi lahko predstavljale nasprotje interesov – o tem takoj pisno obvesti U ali O)
- ✓ Naloge: svetovalne in nadzorne
- ✓ Obveznost varovanja tajnosti in omejitev uporabe osebnih podatkov izključno za namene izvajanja nalog DPO
- ✓ **Več info:** [Pooblaščenca oseba za varstvo podatkov](#) (spletna stran IPRS)

# Evidenca dejavnosti obdelave



30

GDPR

## Popis zbirke

- ✓ Opredeli namen, vrste OP, uporabnike in druge elemente po členu 30 Splošne uredbe
- ✓ Informacijski pooblaščenec priporoča, da se v evidenco dejavnosti obdelave doda tudi naziv zbirke in pravna podlaga
- ✓ **Vzorec:** [Vzorec evidence dejavnosti obdelave za UPRAVLJAVCE \(člen 30 Splošne uredbe\)](#) (spletna stran IPRS)
- ✓ **Več info:** [Evidenca dejavnosti obdelave](#) (spletna stran IPRS)

| Evidenca udeležencev strokovnega posveta 26.1.2023, odgovorna oseba: Štefan Štefanič |                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Naziv in kontaktni podatki upravljavca                                               | Firma d.o.o., Cesta 3, 1000 Ljubljana, telefon:01/1234567, info@firma.si                                                                                                                                                                           |
| Pooblaščen oseba za varstvo osebnih podatkov                                         | Miha Mihovec, Berlinska cesta 55, 1000 Ljubljana; elektronski naslov: dpo@firma.si, telefonska številka: 01 55 55 777.                                                                                                                             |
| Namen obdelave                                                                       | Izvedba strokovnega posveta, posredovanje s tem povezanih gradiv, posredovanje potrdil o udeležbi na posvetu, obveščanje o podobnih dogodkih v organizaciji Firma d.o.o.                                                                           |
| Opis kategorij posameznikov, na katere se nanašajo osebni podatki                    | Osebe, ki so se prijavile na strokovni posvet.                                                                                                                                                                                                     |
| Opis vrst osebnih podatkov v evidenci                                                | Ime, priimek, naziv delodajalca, delovno mesto, elektronski naslov.                                                                                                                                                                                |
| Kategorije uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki          | Pogodbeni obdelovalec (Prireditve d.o.o., Berlinska cesta 250, 1000 Ljubljana), ki pripravlja in omogoča spletno prijavo na dogodke v organizaciji Firma d.o.o.; Pogodbeni obdelovalec, ki vzdržuje spletno stran organizatorja dogodka.           |
| Informacija o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo  | Takšni prenosi se ne izvajajo, vsi podatki se hranijo znotraj EU.                                                                                                                                                                                  |
| Predvideni roki za izbris podatkov                                                   | Podatki se hranijo eno leto po izvedenem posvetu.                                                                                                                                                                                                  |
| Splošni opis tehničnih in organizacijskih varnostnih ukrepov                         | Ukrepi so določeni v Pravilniku o zavarovanju osebnih podatkov v podjetju Firma d.o.o., ki je dostopen na spletni strani podjetja: <a href="https://www.firma/akti/pravilnik-o-zavarovanju/">https://www.firma/akti/pravilnik-o-zavarovanju/</a> . |

## Evidenca dejavnosti obdelave - primer

# Ocena učinkov (DPIA)

## Kaj ?

**orodje** za identifikacijo, analizo in zmanjševanje tveganj glede nezakonitih ravnanj z osebnimi podatki, do katerih lahko pride pri določenem projektu, sistemu ali uporabi tehnologije

## Zakaj ?

**Pravočasno preprečevanje kršitev** varstva osebnih podatkov **ohranitev ugleda in zaupanja** s strani posameznikov, deležnikov in javnosti v našo organizacijo.

Izogib **negativnemu medijskemu poročanju**

Izogib **inšpekcijskim postopkom in visokim globam**

## Primeri iz prakse

**Sistem za elektronske vozovnice** v javnem potniškem prometu je nepotrebno beležil osebne podatke o času in kraju vstopa potnikov z mesečnimi vozovnicami, s čimer je prišlo do nesorazmerne obdelave osebnih podatkov – predhodna DPIA ni bila izvedena in potrebni so bili dragi ter zamudni popravki informacijskega sistema.

## Kdo mora izvesti DPIA?

DPIA je **obveznost upravljavca**, ki tudi odgovarja za njeno ustreznost

- 35 (1) GDPR: „...**upravljavec** pred obdelavo opravi oceno učinka predvidenih dejanj obdelave na varstvo osebnih podatkov.“

Kaj pa **obdelovalec**?

- 28 (3f) GDPR: „upravljavcu pomaga pri izpolnjevanju obveznosti iz členov 32 do 36 ob upoštevanju narave obdelave in informacij, ki so dostopne obdelovalcu;

Vloga **DPO**

- Upravljavec mora za mnenje zaprositi DPO (35(2))
- Podaja mnenja na DPIA je obveznost DPO (39 (1c))
- DPO ni odgovoren za izvedbo ali ustreznost DPIA, to je lastnik/skrbnik procesa obdelave (npr. vodja trženja pri klubu zvestobe, vodja IT pri prenovi IT,...)

## Kdaj je DPIA obvezna?

### **Temeljno pravilo:**

- veliko tveganje za pravice in svoboščine posameznikov

Tveganje:

**VERJETNOST**

**RESNOST  
POSLEDIC**

## Kdaj je DPIA obvezna?

### Dodatna merila (35(3) GDPR):

- **sistematično in obsežno vrednotenje osebnih vidikov v zvezi s posamezniki, ki temelji na avtomatizirani obdelavi**, vključno z oblikovanjem profilov, in je osnova za odločitve, ki imajo pravne učinke v zvezi s posameznikom ali nanj na podoben način znatno vplivajo;
- obsežne **obdelave posebnih vrst podatkov** iz člena 9(1) ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški iz člena 10, ali
- obsežno **sistematično spremljanje javno dostopnega območja**.

# Kdaj je DPIA obvezna? - seznam

Seznam dejanj obdelave osebnih podatkov, za katere velja obveznost izvedbe ocene učinka (**priloga smernic [Informacijskega pooblaščenca o ocenah učinkov](#)**):

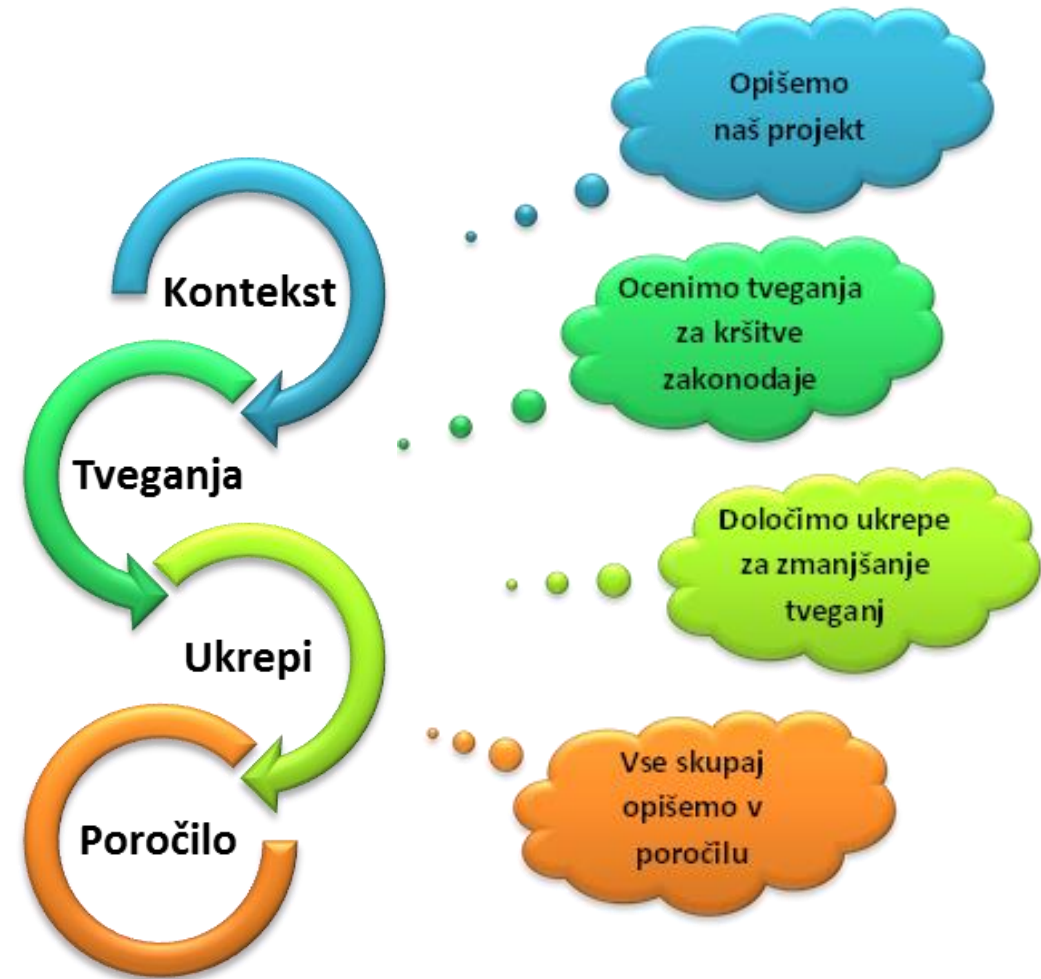
| Kriterij                                                                                        | Primeri                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>OBSEŽNO VREDNOTENJE IN PROFILIRANJE POSAMEZNIKOV</b>                                         | <ul style="list-style-type: none"><li>- Pridobitev kredita na podlagi podatkov v SISBONU in drugih podatkov</li><li>- genetsko testiranje in ugotavljanje verjetnosti za nastanek določene bolezni</li><li>- beleženje podatkov o vožnjah in ustvarjanje profilov voznikov za popust pri zavarovanju</li></ul>                                                                                                                                                                                                                                                                                           |
| <b>AVTOMATIZIRANO ODLOČANJE S PRAVNIM ALI PODOBNIM UČINKOM</b>                                  | <ul style="list-style-type: none"><li>- avtomatizirano odločanje o pridobitvi/zavrnitvi: stanovanjskega ali drugega kredita, denarne socialne omoči, štipendije, usposobljenosti za delo, zdravstvenega zavarovanja ...</li></ul>                                                                                                                                                                                                                                                                                                                                                                        |
| <b>SISTEMATIČEN NADZOR NAD POSAMEZNIKOM, KI SE GA POSAMEZNIK NE ZAVEDA OZ. NANJ NIMA VPLIVA</b> | <ul style="list-style-type: none"><li>- sistemi avtomatske prepoznavne registrskih tablic,</li><li>- sistemi javnega prevoza in elektronskega cestninjenja,</li><li>- projekti e-uprave, o predhodno preverjanje podatkov letalskih potnikov,</li><li>- preverjanje uporabnikov bencinskega servisa s seznamom ubežnikov brez plačila,</li><li>- videonadzor prireditve na javnem prostoru iz brezpilotnika,</li><li>- videonadzor javnih površin,</li><li>- množične ali sistematične obdelave osebnih podatkov, ki jih izvajajo organi pregona v zvezi s kaznivimi dejanji ali prekrški itd.</li></ul> |

| Kriterij                                                                                                                                                                                                                                                                      | Primeri                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>OBDELAVA POSEBNIH VRST OSEBNIH PODATKOV IN PODATKI O KAZNIVIH DEJANJIH IN PREKRŠKIH</b>                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>- Zdravstveni podatki o pacientih v bolnišnici</li> <li>- Kazenske in prekrškovne evidence</li> <li>- Podatki o lokaciji, elektronski komunikaciji posameznika, spletne varnostne kopije podatkov posameznika, pametne naprave, ki beležijo aktivnosti posameznika</li> <li>- Podatki o varovankah v varnih hišah, o pripadnikih določene vere, članih drugih društev, ki zbirajo posebne vrste podatkov</li> </ul> |
| <b>MNOŽIČNOST OBDELAVE OSEBNIH PODATKOV</b><br>Množičnost obdelave osebnih podatkov, pri čemer se upošteva število (ali delež) zadevnih posameznikov, obseg podatkov, trajanje ali stalnost obdelave in geografski obseg obdelave, kot na primer:                             | <ul style="list-style-type: none"> <li>- Klubi zvestobe pri trgovcih</li> <li>- Podatki o uporabi elektronskih komunikacij pri operaterjih</li> <li>- Podatki o zavarovancih in škodnih primerih pri zavarovalnicah</li> <li>- Registri na državni ravni</li> <li>- Podatki o komitentih in njihovi uporabi bančnih storitev v bankah in hranilnicah</li> </ul>                                                                                            |
| <b>PRIMERJANJE IN KOMBINIRANJE RAZLIČNIH ZBIRK PODATKOV IN ANALITIKA NA OSNOVI MASOVNIH PODATKOV</b><br>Primerjanje in kombiniranje različnih zbirk podatkov (npr. pridobljenih skozi različne aktivnosti upravljavca) in analize na osnovi masovnih podatkov, kot na primer: | <ul style="list-style-type: none"> <li>- Primerjanje podatkov o zavarovancih in podatkov o škodnih primerih pri zavarovalnici z namenom ugotavljanje deležev, trendov, vzročno-posledičnih povezav ipd.</li> <li>- Primerjanje podatkov o absentizmu in podatkov o spolu, starosti in izobrazbi zaposlenih</li> <li>- Primerjanje nakupovalnih navad in podatkov o gibanju kupcev</li> </ul>                                                               |
| <b>NESORAZMERJE MOČI IN OBDELAVA PODATKOV RANLJIVIH SKUPIN</b>                                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>- Obdelava osebnih podatkov zaposlenih, otrok, psihičnih bolnikov, prosilcev za azil, migrantov, starejših, pacientov</li> <li>...</li> </ul>                                                                                                                                                                                                                                                                       |

| Kriterij                                                                                      | Primeri                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>INOVATIVNA UPORABA OBSTOJEČIH IN NOVIH TEHNOLOGIJ</b>                                      | <ul style="list-style-type: none"> <li>- Biometrijska prepoznavna prstnih odtisov, obraza</li> <li>- Testiranje in analiza genetskih vzorcev</li> <li>- Sistemi inteligentne videoanalitike</li> </ul> |
| <b>OBDELAVA, KI OMEJUJE PRAVICE ALI PREPREČUJE POSAMEZNIKU DOSTOP DO STORITEV ALI POGODBE</b> | <ul style="list-style-type: none"> <li>- Obdelava podatkov o uporabi avtocestnega omrežja z elektronskim cestninjenjem</li> <li>- Predhodno preverjanje kreditne sposobnosti komitenta</li> </ul>      |
| <b>NEPOSREDNO TVEGANJE ZA ZDRAVJE IN VARNOST POSAMEZNIKOV</b>                                 | <ul style="list-style-type: none"> <li>- uporaba zdravstvenih elektronskih naprav, delovanje katerih lahko vpliva na zdravje posameznika</li> </ul>                                                    |

# Kako izvesti DPIA?

- **METODOLOGIJA** ni predpisana – koristno je opredeliti **tveganja po načelih varstva OP**
- **Uporabno:** standardi za upravljanje s tveganji (ISO/IEC 31000 – risk management, ISO/IEC 27001 – ožji, kot zahteva DPIA).
- **Bistveno:** DPIA ni promocijski material projekta (obdelave) temveč **analiza učinkov na pravice posameznikov in ukrepi za zmanjšanje negativnih učinkov**



# Zakonodajna ocena učinka

24

ZVOP-2

## PRIMERI

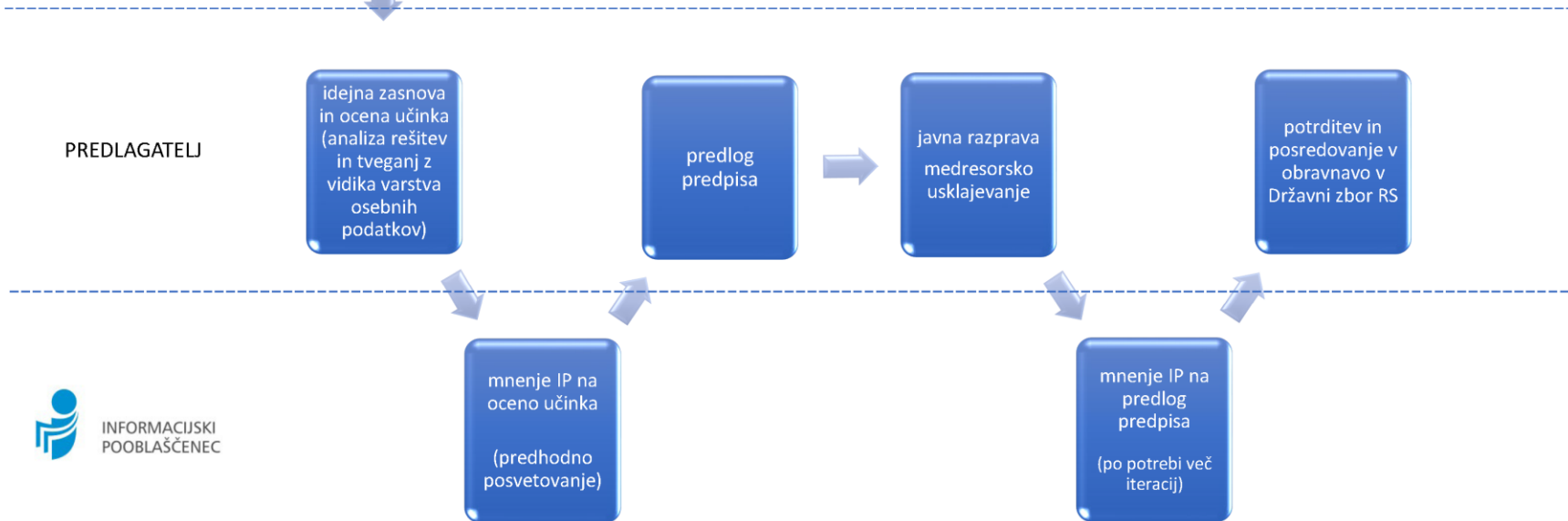
- digitalizacija zdravstva
- povezovanje zbirk
- uvajanje novih informacijskih sistemov
- avtomatizirano odločanje
- obdelava posebnih vrst osebnih podatkov

problematika,  
ki terja  
zakonsko  
urejanje

## Ocene učinkov na varstvo osebnih podatkov pri pripravi predpisov (zakonodajne ocene učinka)

Ocena učinkov je orodje za pravočasno **identifikacijo, analizo in zmanjševanje tveganj** glede nezakonitih ravnanj z osebnimi podatki. 24. člen **ZVOP-2** določa zahtevo po ocenah učinka pri pripravi zakonov: kadar se z zakonom določa obdelava osebnih podatkov, za katero je treba izdelati oceno učinka, predlagatelj predlogu zakona priloži oceno učinka v skladu s 35. členom Splošne uredbe (»zakonodajne ocene učinka«). Prav tako ZVOPOKD v 49. členu za določene primere zahteva izvedbo takšne zakonodajne ocene učinkov.

Namen **zakonodajnih ocen učinka** je, da se še pred oblikovanjem dokončnega besedila členov opravi **pravočasne razmisleke** o tem, kako **ustrezno upoštevati temeljna načela varstva osebnih podatkov pri določanju besedila zakona**. Te razmisleke (npr. ali je za dosego ciljev zakona resnično treba obdelovati osebne podatke, kakšne namene zasledujemo, kateri nabor osebnih podatkov je potreben, katere ukrepe je treba vključiti za zagotovitev zakonite in poštene obdelave, kakšne varovalke moramo vključiti v zakon, ali bo šlo za povezovanje zbirk podatkov, določitev rokov hrambe ipd.) se **opiše v oceni učinkov**, jo pošlje IP v mnenje (v t.i. **predhodno posvetovanje**) in na podlagi mnenja IP oblikuje (bolj) dokončno besedilo členov, ki gre lahko nato v medresorsko usklajevanje.



### Več informacij o ocenah učinka:

<https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/ključna-področja-uredbe/ocena-účinka-v-zvezi-z-varstvom-podatkov/>

### IP je pripravil osnutek metodologije za pripravo zakonodajnih ocen učinka:

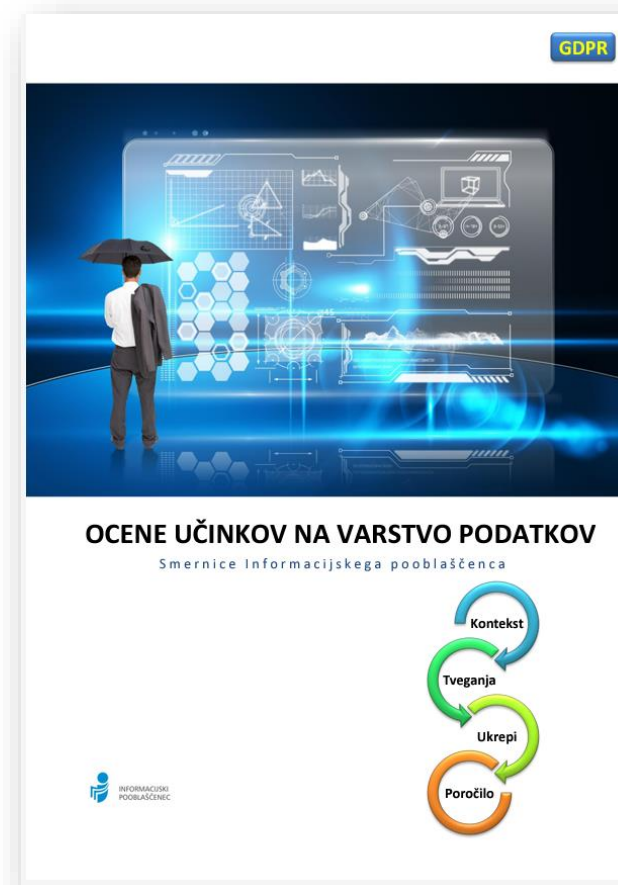
[https://www.ip-rs.si/fileadmin/user\\_upload/Pdf/priporombe/2022/MJU\\_metodologija\\_ocene\\_účinkov\\_jul2022.docx](https://www.ip-rs.si/fileadmin/user_upload/Pdf/priporombe/2022/MJU_metodologija_ocene_účinkov_jul2022.docx)

# Več o ocenah učinkov

## Smernice IP:

- Seznam obdelav, za katere je ocena učinkov obvezna
- EU seznam čezmejnih obdelav osebnih podatkov, za katere je ocena učinkov obvezna
- Kako izvesti DPIA – priporočila glede izbire metodologije...
- Primeri obstoječih ocen

## Pojasnila IP



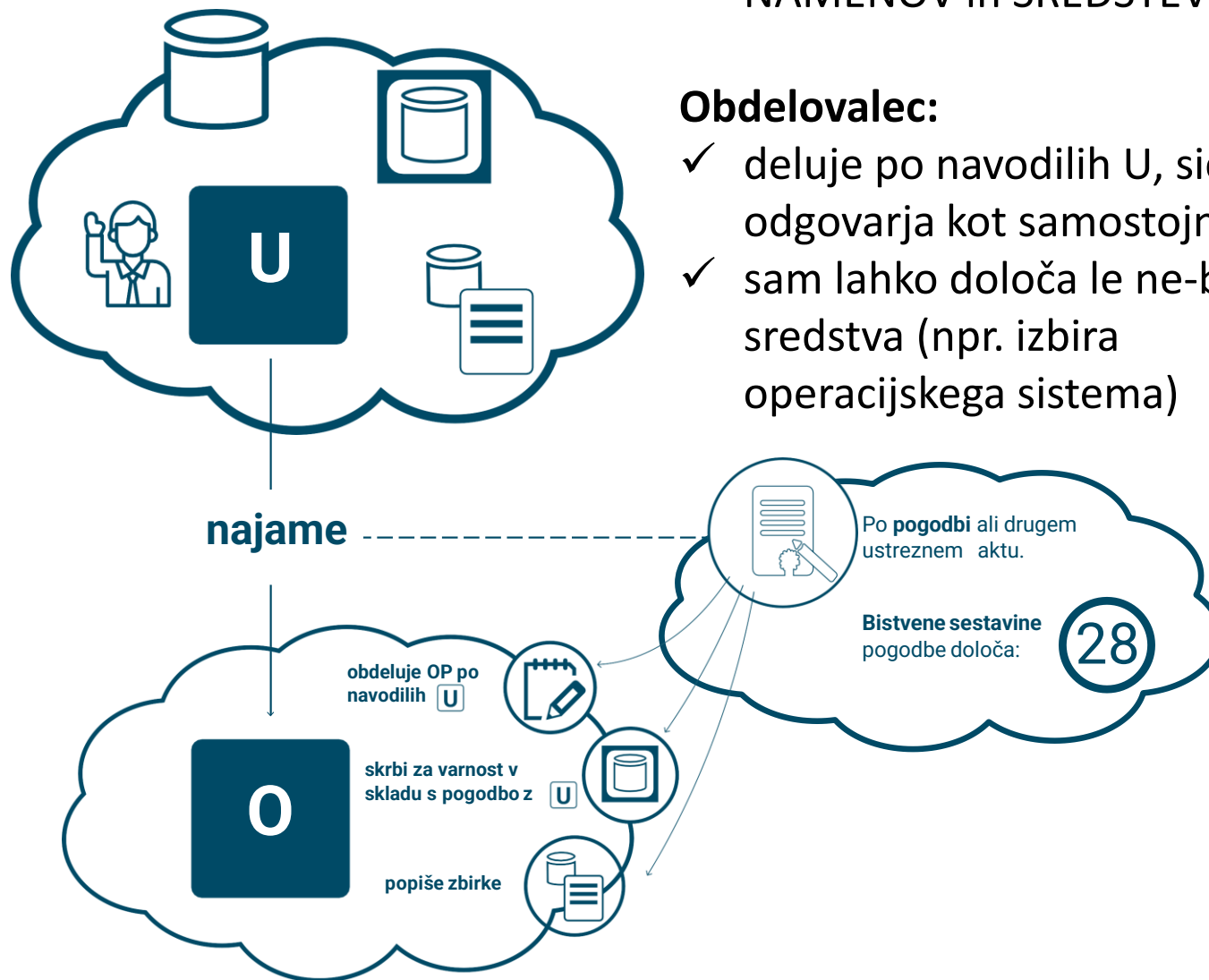
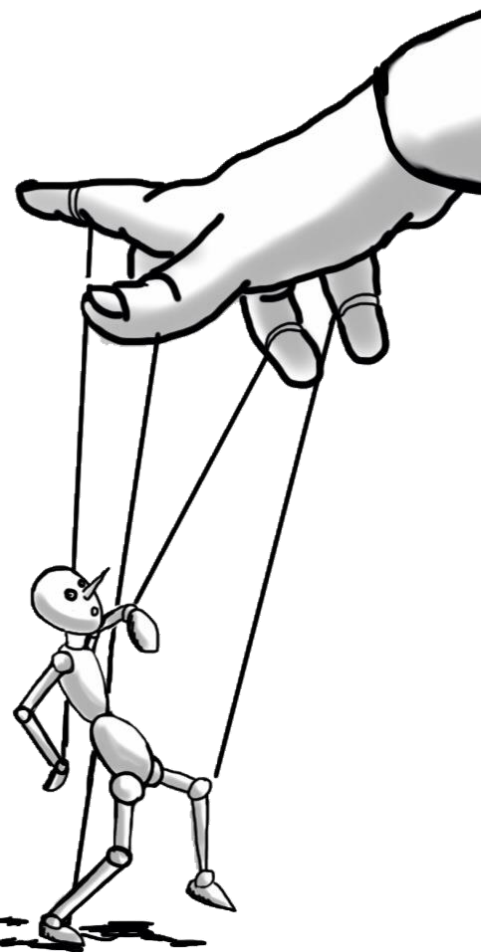
## 0 obdelovalec

### Upravljavec:

- ✓ ima resničen vpliv na določanje NAMENOV in SREDSTEV

### Obdelovalec:

- ✓ deluje po navodilih U, sicer odgovarja kot samostojni U
- ✓ sam lahko določa le ne-bistvena sredstva (npr. izbira operacijskega sistema)



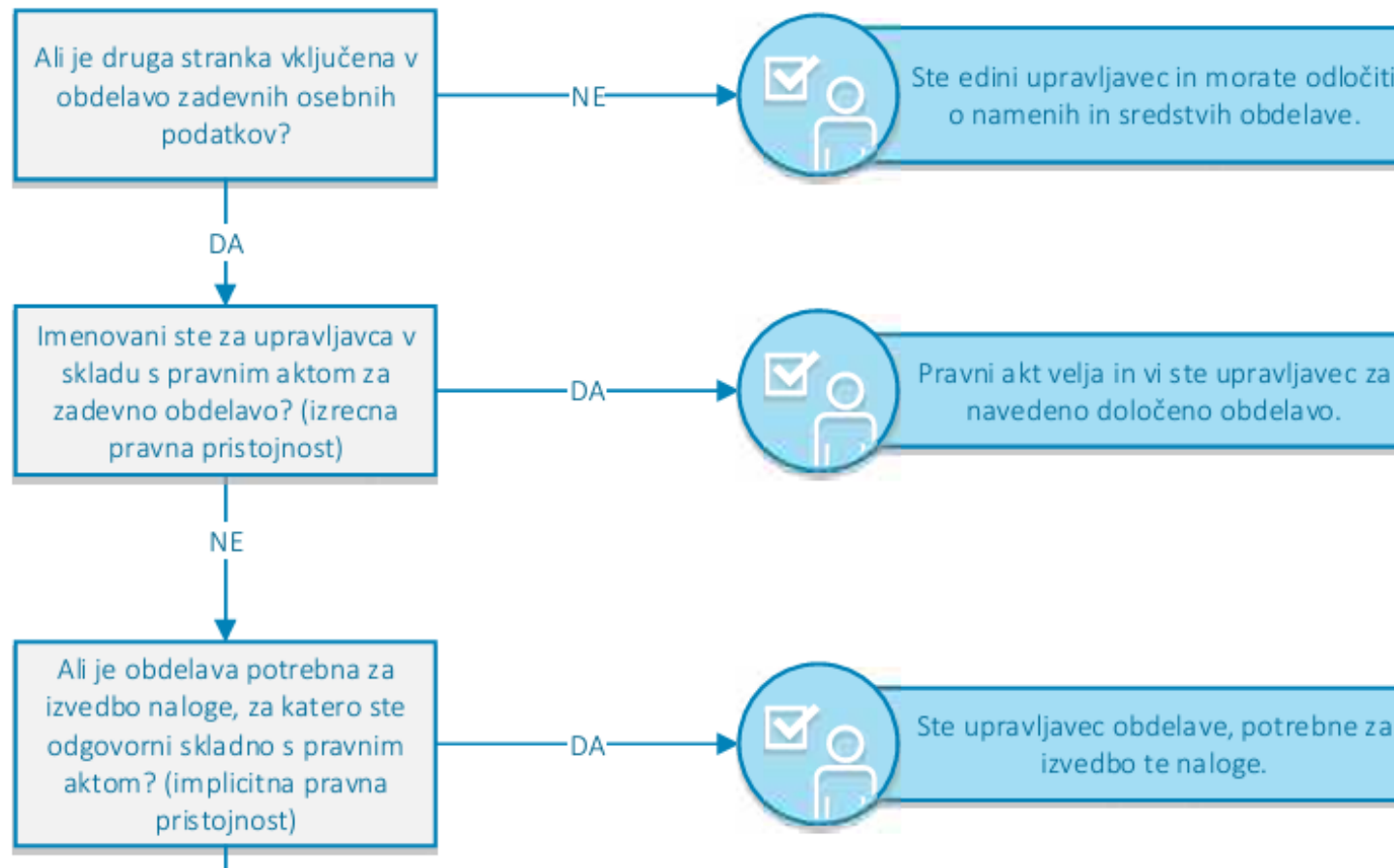
## PO

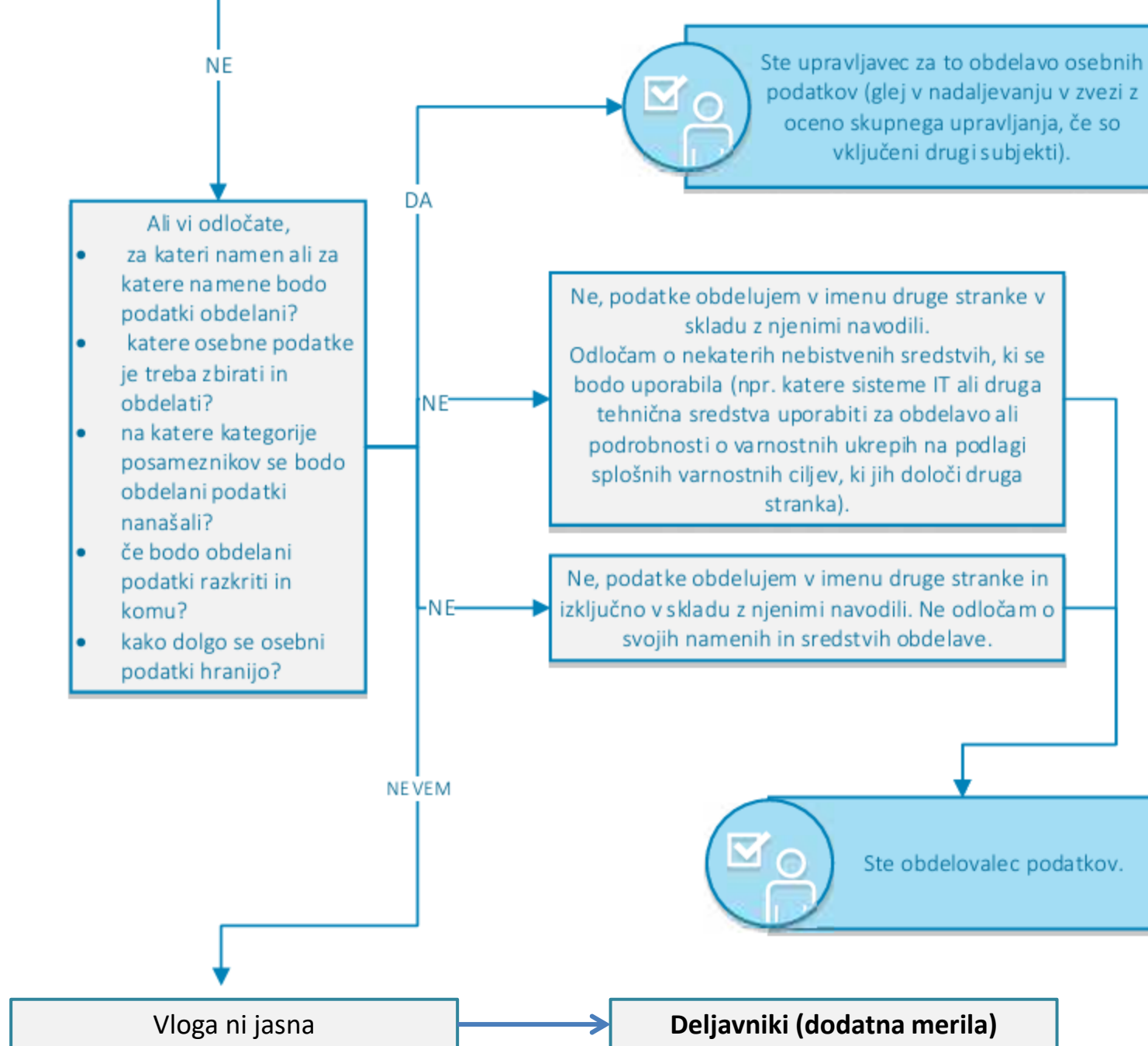


# Upravljavec ali obdelovalec?

Smernice 07/2020 o pojmi upravljavec in obdelovalec iz Splošne uredbe o varstvu podatkov

**Pred oceno je treba opredeliti obdelavo osebnih podatkov in natančno določiti namen**





# Dejavniki, ki kažejo na vlogo

## UPRAVLJAVEC

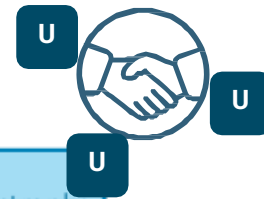
- Imate korist od obdelave ali se zanjo zanimате (ne zgolj za plačilo za storitve, prejeto od drugega upravljavca).
- Sprejemate odločitve o zadevnih posameznikih v okviru ali zaradi obdelave (npr. posamezniki, na katere se nanašajo osebni podatki, so vaši zaposleni).
- Dejavnosti obdelave se lahko štejejo za neločljivo povezane z vlogo ali dejavnostmi vašega subjekta (npr. zaradi klasičnih vlog ali strokovnega znanja), kar vključuje odgovornosti z vidika varstva podatkov.
- Obdelava zadeva vaš odnos s posamezniki, na katere se nanašajo osebni podatki, kot so zaposleni, stranke, člani itd.
- Ste popolnoma samostojni pri odločanju o načinu obdelave osebnih podatkov.
- Obdelavo osebnih podatkov ste zaupali zunanji organizaciji, da osebne podatke obdela v vašem imenu.

## OBDELOVALEC

- Osebne podatke obdelujete za namene druge stranke in v skladu z njenimi dokumentiranimi navodili – za obdelavo nimate svojega namena.
- Druga stranka spremlja vaše dejavnosti obdelave in preverja, ali spoštujete navodila in pogodbeni določila.
- Pri obdelavi nimate drugega namena razen lastnega poslovnega interesa za opravljanje storitev.
- Za izvajanje posebnih dejavnosti obdelave vas je zaposlil nekdo, ki je bil najet za obdelavo podatkov v imenu druge stranke in v skladu z njenimi dokumentiranimi navodili (ste podobdelovalec).



## Skupni upravljavci ?



Ali vi in druga(-e) vključena(-e) stranka(-e) skupaj določata(-e) namene in sredstva obdelave?  
Ali več kot ena stranka odločilno vpliva na to, ali in kako poteka obdelava – bodisi s *skupno odločitvijo* bodisi s *konvergentnimi odločitvami*, ki druga drugo dopolnjujejo in so potrebne za obdelavo, ker konkretno vplivajo na določitev namenov in sredstev?

To pomeni, da obdelava ne bi bila mogoča brez sodelovanja obeh strank – obdelava, ki jo izvede vsaka stranka, je neločljiva, tj. neločljivo povezana.

NE



Ste edini upravljevec – druge stranke so lahko ločeni neodvisni upravljavci za svoj namen ali obdelovalci v skladu z zgornjim shematskim prikazom.

DA

Ali se skupne ali konvergentne odločitve o namenih in sredstvih nanašajo na celotno zadevno obdelavo?

DA



Ste skupni upravljavci za celotno obdelavo.

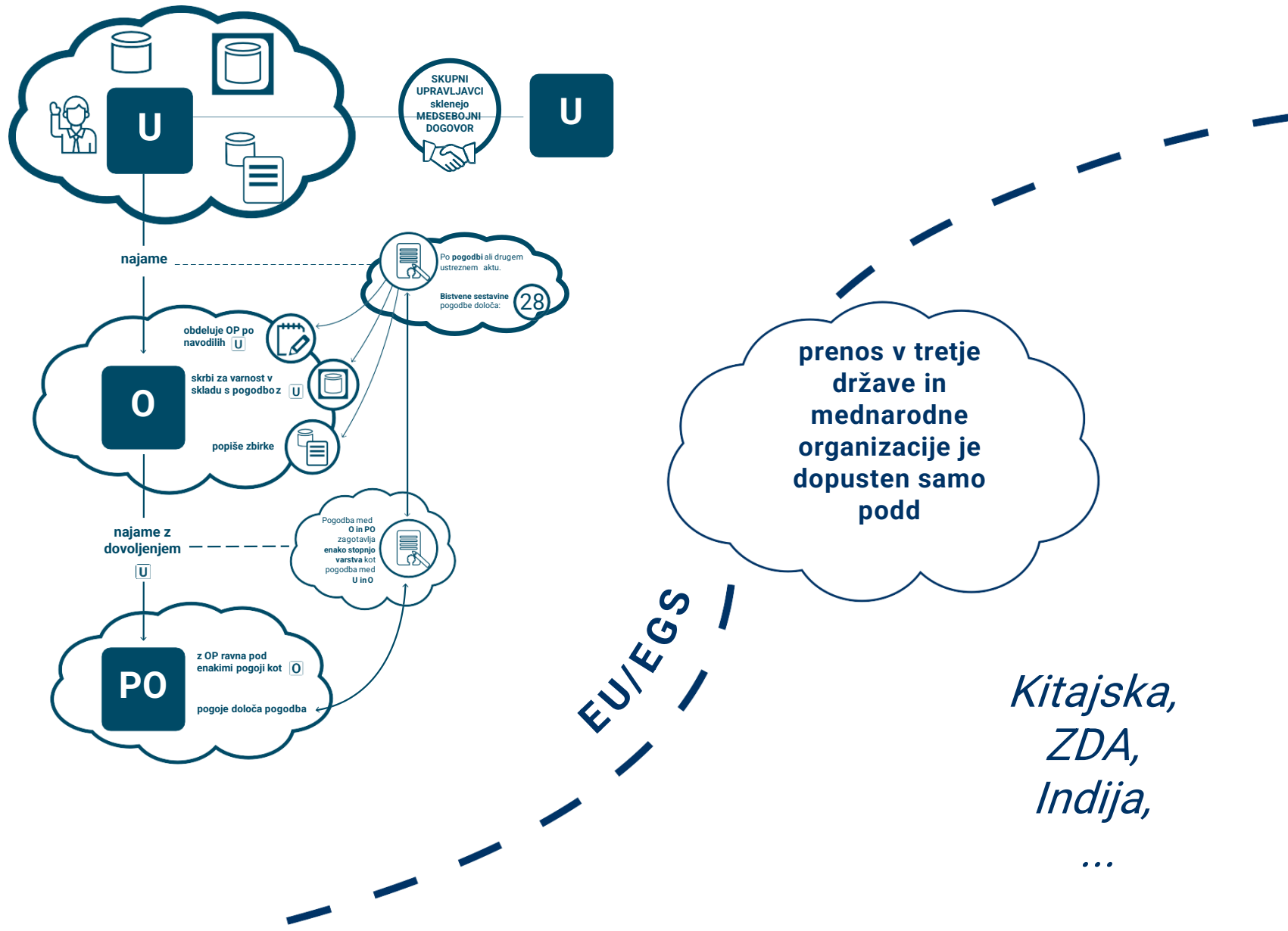
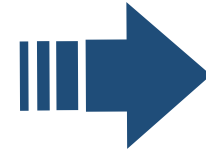
NE

Ne, skupne ali konvergentne odločitve se nanašajo le na določene dele obdelave.



Ste skupni upravljavci za dele obdelave, za katere skupaj določite namene in sredstva, ter ločeni upravljavci za dele obdelave, pri katerih ločeno določite namene in sredstva.

# prenos v tretje države in mednarodne organizacije





## I. KORAK: OSNOVNA PRAVNA PODLAGA

V prvem koraku zagotovite ustrezno pravno podlago za obdelavo osebnih podatkov (čl.6/9/28 Splošne uredbe\*).

\*Uredba (EU) 2016/679 (Splošna uredba o varstvu podatkov)

**ČLEN 6:**  
PRAVNE PODLAGE ZA  
OBDELAVO  
OBČAJNIH OP

**ČLEN 9:**  
PRAVNE PODLAGE  
ZA OBDELAVO  
POSEBNIH VRST OP

**ČLEN 28:**  
PODLAGA, KI IZVIRA IZ  
POGODBE O OBDELAVI  
OSEBNIH PODATKOV  
• [smernice IP o \(pogodbeni obdelavi OP\)](#)

Če je zagotovljena osnovna pravna podlaga, potem je za zakonit prenos treba zagotoviti še **podlago za prenose osebnih podatkov (II. korak)**.

## II. KORAK: PRAVNA PODLAGA ZA PRENOSE

Prenos je dopusten, če je na enega od naslednjih načinov zagotovljena ustrezna raven varstva osebnih podatkov po prenosu:

### 1 DRŽAVA ZAGOTAVLJA USTREZNO RAVEN VARSTVA OP

Evropska komisija in IP sta za nekatere države ugotovila, da zagotavljajo ustrezno raven varstva osebnih podatkov, to pomeni, da izvoznik lahko prenese podatke brez posebnega dovoljenja IP ali izpolnjevanja dodatnih pogojev (ustrezni zaščitni ukrepi, odstopanja v posebnih primerih).

Za katere države to trenutno velja?

- Andora,
- Argentina,
- Kanada,
- Ferski otoki,
- Guernsey,
- Izrael,
- Isle of Man,
- Jersey,
- Makedonija,
- Nova Zelandija,
- Švica,
- Urugvaj,
- Japonska.



Če je ta pogoj izpolnjen je prenos dopusten brez dodatnih omejitev



Če ta pogoj ni izpolnjen je treba preveriti, ali je mogoče prenos zagotoviti na podlagi **USTREZNIH ZAŠČITNIH UKREPOV**

### 2 USTREZNI ZAŠČITNI UKREPI

Ustrezni zaščitni ukrepi zagotavljajo, da upravljavec ali obdelovalec v tretji državi (uvoznik) zagotavlja ustrezno raven varstva osebnih podatkov. Delijo se glede na to, ali je potrebno predhodno dovoljenje IP.

Posebno dovoljenje IP ni pogoj za prenose na podlagi:

- zavezujočih poslovnih pravil (BCR),\*
- tipskih pogodbe Evropske Unije,
- odobrenih kodeksov ravnanja,
- odobrenih mehanizmov potrjevanja,
- pravno zavezujočih in izvršljivih instrumentov (javni sektor).

\*BCR pred prenosom potrdi vodilni nadzorni organ

Predhodno dovoljenje IP je pogoj za prenos na podlagi:

- pogodb, ki jih uvoznik in izvoznik določita sama
- določb, ki se vstavijo v upravne dogovore med javnimi organi (velja za javni sektor)



#### DODATNI ZAŠČITNI UKREPI PRED PRENOSOM!

Izvoznik preveri, če je raven varstva OP v tretji državi "v bistvu enakovredna ravni v EU."

Če oceni da ni

izvoznik sprejme

**DOPOLNILNE UKREPE**  
Priporočila EDPB o dopolnilnih ukrepih  
Priporočila EDPB o evropskih temeljnih jamstvih



Če so zagotovljeni ustrezni zaščitni ukrepi je prenos dopusten brez dodatnih omejitev.



Če ustreznih zaščitnih ukrepov ni mogoče zagotoviti je prenos izjemoma lahko dopusten na podlagi **ODSTOPANJ V POSEBNIH PRIMERIH**.

### 3 ODSTOPANJA V POSEBNIH PRIMERIH

Ko pravne podlage za prenose iz (1) in (2) niso možne, je prenos dopusten, če je izpolnjen eden od spodnjih pogojev. Prenos na tej podlagi je dopusten le izjemoma, zato ni ustrezen za izvajanje rednega oz. stalnega prenosa podatkov.

Prenos se lahko izjemoma izvede, če je podan vsaj eden od naslednjih pogojev:

- izrecna privolitev posameznika,
- izvajanje pogodbe s posameznikom ali predpogodbenih ukrepov,
- prenos je potreben za sklenitev ali izvajanje pogodbe, ki je v interesu posameznika,
- obstajajo pomembni razlogi javnega interesa,
- uveljavljanje, izvajanje ali obramba pravnih zahtevkov
- zaščita življenjskih interesov, ko posameznik ni sposoben dati privolitve,
- prenos iz registra, ki je po pravu EU ali države članice namenjen zagotavljanju informacij javnosti.

### 4 ODSTOPANJA OD ODSTOPANJ

Če prenos tudi na podlagi odstopanj v posebnih primerih (3) ni možen, je pa nujen, se prenos lahko izvede, če so izpolnjeni vsi naslednji pogoji:

- prenos ni ponovljiv,
- zadeva omejeno število posameznikov,
- je potreben zaradi nujnih zakonitih interesov, za katere si prizadeva upravljavec, nad katerimi ne prevladajo interesi ali pravice in svoboščine posameznikov, ter
- upravljavec je predhodno ocenil vse okoliščine v zvezi s prenosom in predvidel ustrezne zaščitne ukrepe v zvezi z varstvom osebnih podatkov in informacije posamezniku o prenosu (po 13. in 14. členu Splošne uredbe).

Upravljavec mora o tem prenosu obvestiti IP.



INFORMACIJSKI  
POOBLAŠČENEC



**Več o prenosih:**  
[Smernice IP](#)

# Videonadzor

## **ZVOP-2**

- 76. člen - splošne določbe o videonadzoru in varstvu osebnih podatkov;
- 77. člen - videonadzor dostopa v uradne službene oziroma poslovne prostore;
- 78. člen - videonadzor znotraj delovnih prostorov;
- 79. člen - videonadzor v prevoznih sredstvih, namenjenih javnemu potniškemu prometu;
- 80. člen - videonadzor na javnih površinah.

# Videonadzor – splošne obveznosti

**ODLOČITEV O UVEDBI** - sprejme predstojnik, direktor ali drug pooblaščen posameznik osebe javnega sektorja ali osebe zasebnega sektorja kot upravljavca

## OBVESTILO MORA VSEBOVATI

- pisno ali nedvoumno grafično opisano dejstvo, da se izvaja videonadzor;
- namene obdelave, navedbo upravljavca videonadzornega sistema, telefonsko številko ali naslov elektronske pošte ali spletni naslov za potrebe uveljavljanja pravic posameznika s področja varstva osebnih podatkov;
- informacije o posebnih vplivih obdelave, zlasti nadaljnje obdelave;
- kontaktne podatke pooblaščen osebe (telefonska številka ali naslov e-pošte);
- neobičajne nadaljnje obdelave, kot so prenosi subjektom v tretje države, spremljanje dogajanja v živo, možnost zvočne intervencije v primeru spremljanja dogajanja v živo.
- + informacije po prvem odstavku člena 13 Splošne uredbe

**Alternativno se lahko vse navedene informacije objavi na spletni strani, na fizičnem obvestilu navede spletni naslov, kjer se informacije objavijo.**

**PODATKI:** posnetek posameznika (slika), podatek o lokaciji, datum in čas posnetka, izjemoma, če je to posebej nujno potrebno, pa tudi zvok.

**!!!POZOR!!!**

**UPRAVLJALEC:**

**KONTAKT ZA UVELJAVLJANJE PRAVIC POSAMEZNIKA:**

☐ **VIDEONADZOR VHODOV V STAVBO**  
NAMEN IZVAJANJA VIDEONADZORA

☐ Varovanje ljudi  
☐ Varovanje prevoznih sredstev  
☐ Preprečevanje ogrožanja zaposlenih  
☐ Zagotavljanje nadzora vidnega v in izstopa iz poslovnih prostorov

☐ **VIDEONADZOR DELOVNIH PROSTOROV**  
NAMEN IZVAJANJA VIDEONADZORA

☐ Zagotavljanje varnosti ljudi  
☐ Zagotavljanje varnosti prevoznih sredstev  
☐ Preprečevanje in odkrivanje kršitev na področju igre na srečo  
☐ Varovanje tajnih podatkov  
☐ Varovanje poslovnih skrivnosti

☐ Upravitelj ne spremlja žive slike  
☐ Upravitelj spremlja živo sliko in ima možnost zvočne intervencije

☐ Upravitelj spremlja živo sliko in ima možnost zvočne intervencije

Pravna podlaga: Videonadzor se izvaja na podlagi zakonitega interesa in v skladu z določili 77. in 78. člena ZVOP-2. Posnetki se lahko posredujejo pogodbenim osebam, ki jih uporabljajo za druge uporabnike z ustreznimi pooblastili, npr. policiji. Posnetki se ne smejo razkriti tretjim osebam, razen če to zahteva zakon. Posnetki se ne smejo razkriti tretjim osebam, razen če to zahteva zakon. Posnetki se ne smejo razkriti tretjim osebam, razen če to zahteva zakon. Posnetki se ne smejo razkriti tretjim osebam, razen če to zahteva zakon.

PRAVICA DO PRITOŽBE: Posameznik ima pravico, da se pritoži informacijskemu pooblaščenca, naslov: Dolenjska 22, 1000 Ljubljana, e-mail: [info@info.si](mailto:info@info.si), tel. 01 2309 170, spletna stran: [www.ig-rs.si](http://www.ig-rs.si).

**IZVAJA SE VIDEONADZOR**

# Videonadzor – splošne obveznosti

**ROK HRAMBE:** Ob upoštevanju načel največ eno leto od posnetka.

**PREPOVEDANO SNEMATI:** V dvigalih, sanitarijah, prostorih za preoblačenje, hotelskih sobah in drugih podobnih prostorih, v katerih posameznik utemeljeno pričakuje višjo stopnjo zasebnosti.

**OMEJITEV NAMENA NADALNJE UPORABE POSNETKOV:** Vpogled, uporaba ali posredovanje posnetkov videonadzornega sistema so dopustni samo za namene, ki so zakonito obstajali ali bili navedeni na obvestilu v času zajema posnetka.

**OBVEZNA SLEDLJIVOST VPOGLEDOV:** Upravljalavec videonadzornega sistema za vsak vpogled ali uporabo posnetkov zagotovi možnost naknadnega ugotavljanja, kateri posnetki so bili obdelani, kdaj in kako so bili uporabljeni ali komu so bili posredovani, kdo je izvedel ta dejanja obdelave, kdaj in s kakšnim namenom ali na kateri pravni podlagi.

**ROK HRAMBE SLEDLJIVOSTI:** Te podatke hrani v dnevniku obdelave iz 22. člena tega zakona dve leti po koncu leta, ko so nastali.

# Videonadzor po ZVOP-2

**Dostop v uradne službene oziroma poslovne prostore** (podobno kot po ZVOP-1)

**NAMEN:** če je to potrebno za varnost ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa v te prostore ali izstopa iz njih ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih.

**PREPOVEDANO JE SNEMATI:** brez snemanja delov stanovanjskih stavb, ki niso službeni prostori in snemanja vhodov v stanovanja.

## **POSEBNI POGOJI:**

- Videonadzor je dovoljen, če s tem soglašajo lastniki, ki imajo v lasti več kot 70-odstotni delež skupnih delov.

**OBVEZNO OBVEŠČANJE ZAPOSLENIH:** O izvajanju videonadzora in o vsebinah iz obvestila so pisno obveščeni vsi zaposleni, ki opravljajo delo v nadzorovanem prostoru.

## **PODATKI:**

- posnetek posameznika (slika), podatek o lokaciji, datum in čas posnetka, izjemoma, če je to posebej nujno potrebno, pa tudi zvok
- datum in čas vstopa v uradni službeni prostor in izstopa iz njega, osebno ime posnetega posameznika, naslov njegovega stalnega ali začasnega prebivališča, zaposlitev, številko in podatke o vrsti njegovega osebnega dokumenta ter razlog vstopa, če se navedeni osebni podatki zbirajo skupaj s posnetkom videonadzornega sistema

# Videonadzor po ZVOP-2

## Videonadzor znotraj delovnih prostorov (podobno kot po ZVOP-1)

**NAMEN:** le, kadar je to nujno potrebno za varnost ljudi ali premoženja ali preprečevanje ali odkrivanje kršitev na področju iger na srečo ali za varovanje tajnih podatkov ali poslovnih skrivnosti, teh namenov pa ni mogoče doseči z milejšimi sredstvi.

**SME SE SNEMATI** v tistih delih in v obsegu, kjer je treba varovati interese iz namena.

**PREPOVEDANO JE SNEMATI** delovna mesta, kjer delavec po navadi dela, razen če je to nujno.

### POSEBNI POGOJI:

- neposredno spremljanje dogajanja pred kamerami (podaljšano oko) je dovoljeno le, če ga izvaja izrecno pooblaščen osebje upravljavca
- obvezno predhodno posvetovanje z reprezentativnimi sindikati pri delodajalcu in svetom delavcev oziroma delavskim zaupnikom (razen na določenih področjih)
- videonadzor skupnih prostorov v poslovnih zgradbah je dovoljen, če s tem soglašajo lastniki, ki imajo v lasti več kot 70-odstotni delež skupnih delov.

**OBVEZNO OBVEŠČANJE ZAPOSLENIH:** Obvezno pisno obveščanje zaposlenih.

# Videonadzor po ZVOP-2

## Videonadzor v prevoznih sredstvih, namenjenih javnemu potniškemu prometu (NOVO)

**NAMEN:** Varnost potnikov in premoženja, če tega ni mogoče doseči z drugimi ukrepi.

**KJE SE SME SNEMATI:** V prevoznih sredstvih, namenjenih javnemu potniškemu prometu, le v delih prevoznega sredstva, namenjenih potnikom.

**ROK HRAMBE POSNETKOV:** Najpozneje v sedmih dneh po njihovem nastanku.

**OMEJITEV NAMENOV UPORABE:** Posnetki se smejo uporabljati za uveljavljanje ali obrambo pravnih zahtevkov ali za izvrševanje nalog policije.



# Videonadzor po ZVOP-2

## Videonadzor na javnih površinah (NOVO)

### **NAMEN:**

- le, kadar je to potrebno zaradi obstoja resne in utemeljene nevarnosti za življenje, osebno svobodo, telo ali zdravje ljudi, varnost premoženja upravljavca ali varovanje tajnih podatkov upravljavca ali obdelovalca v prenosu in teh namenov ni mogoče doseči z drugimi sredstvi, ki manj posegajo v pravice iz prvega odstavka 1. člena tega zakona.
- tudi za namene varovanja varovanih oseb ter posebnih objektov in okolišev objektov, ki jih varuje policija, Slovenska vojska, pristojni organi za področje varnosti države, pravosodna policija, oziroma varovanja drugih prostorov, zgradb ali območij, ki jih je treba varovati na podlagi zakona, in sicer samo v obsegu in trajanju, potrebnem za doseganje namena.

**OMEJITEV NAMENA UPORABE POSNETKOV:** Vpogled, uporaba ali posredovanje posnetkov so dopustni le za te namene.

### **KJE SE SME SNEMATI:**

- na javnih površinah, kot jih določa zakon, ki ureja urejanje prostora
- le glede tistih bližnjih ali povezanih delov javne površine in v obsegu, kjer je treba varovati interese iz namena

**UPRAVLJAVEC:** oseba javnega ali zasebnega sektorja, ki upravlja z javno površino ali na njej zakonito opravlja dejavnost.

# Videonadzor po ZVOP-2

## Videonadzor na javnih površinah (NOVO)

### **POSEBNI POGOJI SNEMANJA IN SPREMLJANJA**

- za javni sektor izvajati le uradne osebe ali pooblaščen varnostno osebje, za zasebni sektor pa pooblaščen varnostno osebje, ki je izrecno pooblaščen za izvajanje videonadzora.
- lahko tudi na način spremljanja dogajanja v živo (podaljšano oko).

**TELESNE KAMERE** - za namen varovanja oseb, tajnih podatkov v prenosu, poslovnih skrivnosti ali premoženja večje vrednosti lahko opravlja tudi z uporabo telesne kamere, če jo uporablja za to posebej usposobljena oseba.

**ROK HRAMBE POSNETKOV:** največ šest mesecev od trenutka nastanka posnetka.

**OB ZAZNAVI DOGODKA** ki ogroža zdravje ali življenje posameznika, **OBVEZNA PRIJAVA NA POLICIJO**

**POSEBNI POGOJI ZA VIDEONADZOR CESTNEGA PROMETA** (le upravljavec cest, na vnaprej določenih odsekih, ki jih opredeli v skladu z zakonom, kjer z drugimi sredstvi ni mogoče doseči nujnega in učinkovitega varovanja cestnega prometa ali njegovega upravljanja, obvezna ocena učinka in predhodno posvetovanje z IP)

**PREPOVED UPORABE SISTEMOV ZA AVTOMATSKO PREPOZNAVO REGISTRSKIH TABLIC** (po razlagi IP velja le za javni sektor) in **SISTEMOV, S KATERIMI SE OBDELUJEJO BIOMETRIČNI OSEBNI PODATKI** (velja povsod).

# Hvala za vašo pozornost

Anže Novak

[anze.novak@ip-rs.si](mailto:anze.novak@ip-rs.si)

