



Kako pravilno poskrbeti za varstvo osebnih podatkov po GDPR in ZVOP-2

mag. Andrej Tomšič

Zakaj ZVOP-2?

- Splošna uredba o varstvu podatkov (GDPR) prepušča urejanje določenih področij državam članicam
- GDPR je v uporabi že od **25.5.2018!**
- Pritiski Evropske komisije
- Zadnja država, ki še ni „pospremila“ GDPR v celoti v uporabo
- ZVOP-1 je prenašal direktivo iz leta 1995
- **Brez ZVOP-2 ni bilo možno izrekanje sankcij po GDPR – upravne globe**
 - sedaj možne tudi globe po GDPR!
- V praksi: potrebno poznavanje in spoštovanje **tako GDPR kot ZVOP-2**
- **Kompleksna naloga**
 - **GDPR: 99 členov, 173 uvodnih določb**
 - **ZVOP-2: 127 členov**

Ključni pojmi

določa jih Splošna uredba (4. člen)

1. **OSEBNI PODATEK** pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom;

določljiv posameznik je tisti, ki ga je mogoče **neposredno** ali **posredno** določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika.

KAJ (VSE) SO OSEBNI PODATKI

Kaj misliš, kateri so najbolj vredni?



PSEVDONIMIZIRANI SO OSEBNI

Anonimizirani niso

➔	VIR NI POMEMBEN SAM IZBRAL / DRŽAVA / DELODAJALEC / PODJETJE
👤	OBLIKA NI POMEMBNA ČRKE / ŠTEVILKE / SLIKE / VIDEO
🔗	KONTEKST ZELO POMEMBEN KDO, ZAKAJ, KATERE, OD KOGA, KDAJ

KLJUČNO VPRAŠANJE JE, ALI SE DA DOLOČITI POSAMEZNIKA

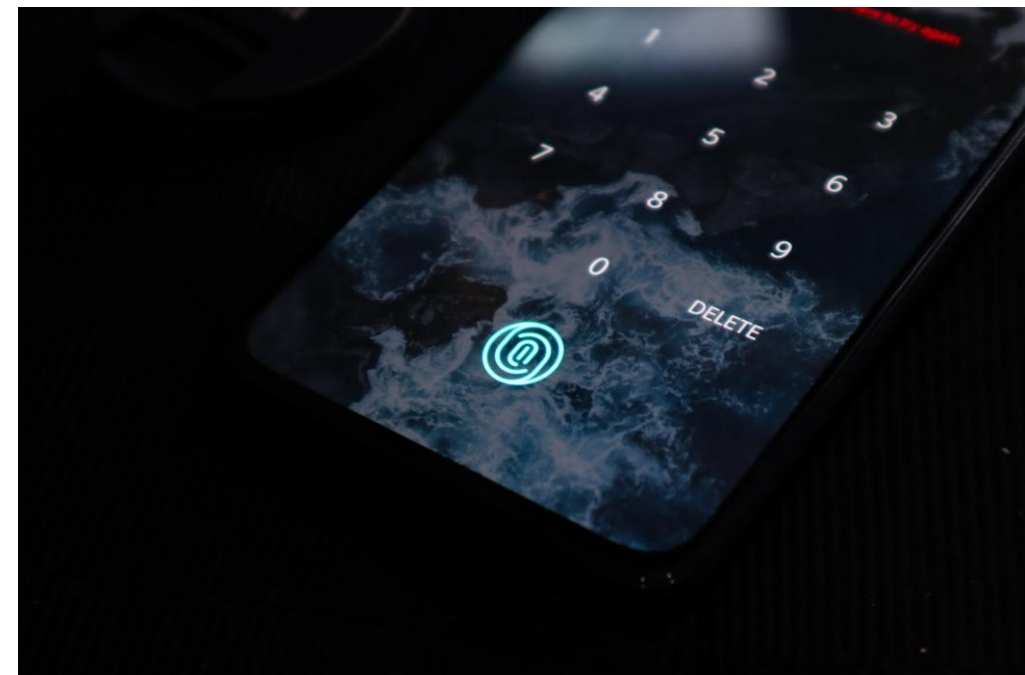
In ne, ali ga jaz/mi znamo določiti

2. ZBIRKA OSEBNIH PODATKOV - elektronsko ali na papirju vodene zbirke podatkov o fizičnih osebah (tabele, aplikacije, razvidi, šifranti, baze, personalne mape....)

- **kadrovske evidence** (evidence o stroških dela, izrabi delovnega časa itd.);
- **druge zbirke o zaposlenih** (npr. evidence dodeljene opreme, podatki u uporabi interneta, službenih vozil...);
- **podatki o strankah** (kupci, udeleženci, komitenti, zavarovanci, člani klubov zvestobe, člani društva, šolajoči, posamezniki v projektih...);
- **zbirke podatkov o tretjih osebah**, npr. druge zbirke, ki nastajajo v določenem okolju, npr. posnetki videonadzora, evidenca vstopajočih, adreme novinarjev, seznam naročnikov na e-novice...
- **Zakonodaja o varstvu OP se nanaša na zbirke, ki jih vodijo podjetja/inštitucije oz. procese obdelav**
 - med cca 5 in 50 zbirk, odvisno od sektorja, velikosti...
- **In na avtomatizirano obdelavo OP**

3. OBDELAVA OSEBNIH PODATKOV je kakršnokoli delovanje ali niz delovanj, ki se izvaja z OP, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, **priklicanje, vpogled**, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje, obdelava pa je lahko ročna ali avtomatizirana.

- **torej: kakršno koli ravnanje z osebnimi podatki!**
- **izjema domače rabe**



4. UPRAVLJAVEC - fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi **določa namene in sredstva obdelave OP** oziroma oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave.

5. OBDELOVALEC - najet s strani upravljavca na podlagi **pisne pogodbe/dogovora**, da **v imenu in za račun upravljavca** obdeluje OP: („pogodbena obdelava osebnih podatkov“)

- vzdrževalec spletne strani
- izvajalec videonadzora
- računovodski servis
- vzdrževanje podatkovnih baz...
- Osebnih podatkov **ne sme uporabljati za svoje namene.**
- **Upoštevati zahteve 28. člena Splošne uredbe – pogodba!** (vzorec na www.ip-rs.si)
 - ZVOP-2 pogodbene obdelave ne ureja/spreminja!



Temeljna načela v zvezi z obdelavo OP (5. člen Splošne uredbe)

- **zakonitost, poštenost 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*),
 - razpoložljivost?
- **odgovornost** (*accountability*)
 - odgovoren za skladnost s temeljnimi načeli in je to skladnost tudi zmožen dokazati –
Proaktivnost! Dolžnost upravljavca!

Zakonitost obdelave po GDPR in ZVOP-2

Pravne podlage (6. člen ZVOP-2): veljajo podlage iz 6. in 9. člena GDPR

- Privolitev (točka (1)a)) 6. člena GDPR
 - Pogodba (točka (1(b)))
 - Zakon (točka (1(c)))
 - Reševanje posameznika (točka (1(d)))
 - Javni interes, izvajanje javne oblasti (točka 1(e))
 - Zakoniti interesi (točka (1(f)))
-
- c) in e) 6(1) GDPR mora določati zakon
 - vsebine zakona (6(2) ZVOP-2): obdelava OP, vrste OP, ki naj se obdelujejo, kategorije posameznikov, namen obdelave in rok hrambe OP ali rok za redni pregled potrebe po hrambi ...

Inšpekcijske prijave, ki jih je prejel Informacijski pooblaščenec, so se nanašale na naslednje sume kršitev določb Splošne uredbe in ZVOP-2:

Sum kršitve	Število prijav
Nezakonito izvajanje videonadzora	203
Nezakonito razkrivanje, posredovanje osebnih podatkov nepooblaščenim uporabnikom in nezakonita objava osebnih podatkov	112
Nezakonito zbiranje oz. zahtevanje osebnih podatkov	91
Neustrezno zavarovanje osebnih podatkov	44
Nezakonit vpogled v osebne podatke	44
Nezakonita obdelava osebnih podatkov pri izvajanju neposrednega trženja	38
Kršitev pravice do informacij po 13. členu	18
Piškotki	11
Obdelava osebnih podatkov v nasprotju z namenom zbiranja	9
Hekerski napadi in vdori v informacijske sisteme	3
Razno – obdelava osebnih podatkov po poteku roka hrambe, uporaba netočnih podatkov, kršitev pravice do seznanitve z osebnimi podatki in pravice do ugovora, sumi kršitev, ki ne sodijo v pristojnost Informacijskega pooblaščenca	113
Skupaj prijav	686

Člen 30 - Evidenca dejavnosti obdelave („katalogi“)

1. Vsak **upravljavec** in predstavnik upravljavca, kadar ta obstaja, vodi **evidenco dejavnosti obdelave OP**. Ta evidenca vsebuje:

- a) **naziv ali ime in kontaktne podatke upravljavca** in, kadar obstajajo, **skupnega upravljavca, predstavnika upravljavca in pooblaščne osebe za varstvo podatkov**;
- b) **namene obdelave**;
- c) **opis kategorij** posameznikov, na katere se nanašajo OP, in **vrst OP**;
- d) **kategorije prejemnikov**, ki so jim bili ali jim bodo razkriti OP, vključno s prejemniki v tretjih državah ali mednarodnih organizacijah;
- e) kadar je ustrezno, **informacije o prenosih OP v tretjo državo ali mednarodno organizacijo**, vključno z identifikacijo te tretje države ali mednarodne organizacije, v primeru prenosov iz drugega pododstavka člena 49(1) pa tudi dokumentacijo o ustreznih zaščitnih ukrepih;
- f) kadar je mogoče, **predvidene roke za izbris** različnih vrst podatkov;
- g) kadar je mogoče, **splošni opis tehničnih in organizacijskih varnostnih ukrepov** iz člena 32(1).

Določena naj bo odgovorna oseba za vzdrževanje ažurnosti evidenc!

→ Vzorec na spletni strani IP (www.ip-rs.si)



Informiranje posameznikov (12., 13. in 14. člen GDPR)

Posameznike je treba informirati o obdelavi osebnih podatkov – načelo preglednosti.

V praksi zelo slabo spoštovano – kršitve in možne kazni!!!

Na ustrezen način, npr.:

- **Zaposlenim** ob zaposlitvi podate takšen ustrezen **izpolnjen obrazec z informacijami**, katere njihove osebne podatke boste obdelovali kot delodajalec za namene delovnega razmerja. Obrazec lahko nato **objavite tudi na intranetu** ali drugemu zaposlenim enostavno dostopnemu mestu.
- **Študentom/posameznikom v projektih** na podoben način, ob zbiranju posredujete informacije, katere njihove osebne podatke boste obdelovali (npr. tako da je ta **obrazec z informacijami enostavno dosegljiv na spletni strani, v referatu** oziroma splošnih pogojev ali na drug ustrezen način).
- **Prijavljenim na e-novice in uporabnikom spletnih strani** lahko te informacije podate **na spletni strani ob poljih, v katere vnesejo svoje podatke** ali z enostavno dostopno povezavo na takšno besedilo.

Poleg vsebine je predpisan tudi **način obveščanja – 12. člen GDPR**: v jedrnat, pregledni, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku. 12. člen **GDPR** je v tujini že predmet sankcij!

Katere informacije jim je treba dati?

Informacije, ki se zagotovijo, kadar se OP pridobijo od posameznika (člen 13.1 GDPR)

- a) identiteto in kontaktne podatke upravljavca in njegovega predstavnika, kadar ta obstaja - **(KDO STE)**;
- b) kontaktne podatke pooblaščen osebe za varstvo podatkov, kadar ta obstaja – **(ČE IMATE IMENOVANO POOBLAŠČENO OSEBO, KDO TO JE)**;
- c) namene, za katere se osebni podatki obdelujejo, kakor tudi pravno podlago za njihovo obdelavo - **(ZAKAJ VSE UPORABLJATE NJEGOVE PODATKE)**;
- d) kadar obdelava temelji na točki (f) člena 6(1), zakonite interese, za uveljavljanje katerih si prizadeva upravljavec ali tretja oseba - **(OBRAZLOŽITEV PODLAGE PREVLAJUJOČIH INTERESOV; ČE JE TO PODLAGA)**;
- e) uporabnike ali kategorije uporabnikov osebnih podatkov, če obstajajo – **(KATERIM TRETJIM PRAVNIM OSEBAM POSREDUJETE NJEGOVE PODATKE)**;
- f) kadar je ustrezno, dejstvo, da upravljavec namerava prenesti osebne podatke v tretjo državo ali mednarodno organizacijo - **(ALI PRENAŠATE PODATKE V T.I. TRETJE DRŽAVE)**.

LAHKO UPORABITE VZOREC NA SPLETNI STRANI IP:

[Vzorec obvestila posameznikom glede obdelave osebnih podatkov \(člen 13 Splošne uredbe\)](#)

Informacije, ki se zagotovijo, kadar se OP pridobijo od posameznika (člen 13.2 GDPR)

- a) **obdobje hrambe OP** ali, ko to ni mogoče, merila, ki se uporabijo za določitev tega obdobja;
- b) **obstoj pravice**, da se od upravljavca zahtevajo **dostop do OP** in **popravek ali izbris OP** ali **omejitev** obdelave, **obstoj pravice do ugovora** obdelavi in pravice do **prenosljivosti** podatkov;
- c) kadar obdelava temelji na privolitvi, **obstoj pravice**, da se lahko **privolitev kadar koli prekliče**, ne da bi to vplivalo na zakonitost obdelave podatkov, ki se je na podlagi privolitve izvajala do njenega preklica;
- d) pravico do **vložitve pritožbe pri nadzornem organu**;
- e) ali je **zagotovitev OP** **statutarna ali pogodbeni obveznost ali pa obveznost**, ki je potrebna za sklenitev pogodbe, ter ali mora posameznik zagotoviti OP ter kakšne so morebitne **posledice, če se taki podatki ne zagotovijo**, in
- f) **obstoj avtomatiziranega sprejemanja odločitev**, vključno z oblikovanjem profilov: **razlogi, pomen in predvidene posledice**.

Postopek pred upravljavcem in obdelovalcem

2. Poglavje (12. – 20. člen ZVOP-2) - Postopek pred upravljavcem in obdelovalcem

- glede pravic ali zahtev posameznika velja **GDPR in to poglavje ZVOP-2**
- **smiselna uporaba ZUP, roki iz GDPR**
- ZVOP-2 določa: postopek obravnavanja zahtevkov (13.-14.člen), sestavine odločbe (15. člen)
 - Kadar upravljavec **ugodi zahtevi** ne izda posebne odločbe, temveč o tem napravi **uradni zaznamek in posameznika seznani z odločitvijo**.
 - Kadar upravljavec zahtevi **ne ugodi, izda odločbo**, ki poleg sestavin po ZUP vsebuje tudi sestavine, ki jih določa ZVOP-2.
 - če posameznik to zahteva, ga lahko z osebnimi podatki seznani tudi ustno.
- **stroški seznaitve – brezplačno** (* razen če očitno neutemeljene ali pretirane: **razumne stroške**. t.j. samo materialne stroške posredovanja informacij, sporočil, odgovorov oziroma izvajanja zahtevanega ukrepanja - > **bo pravilnik: o višini stroškov, načinu zaračunavanja, obveščanja o stroških**)
 - vnaprej obvestiti posameznika o stroških,
- **omejitev pravic posameznika le z zakonom**

Zavarovanje OP, ki so predmet postopka (21. člen ZVOP-2)

- prepoved brisanja ipd. od trenutka prejema zahtevka posameznika dokler o zadevi ni pravnomočno odločeno
- nadzorni organ lahko zaradi učinkovitega izvajanja poslovanja, nalog ali pooblastil upravljavca ali obdelovalca **odredi izdelavo kopije OP ali kopije postopkov** obdelave

Varnost osebnih podatkov in ocena učinka

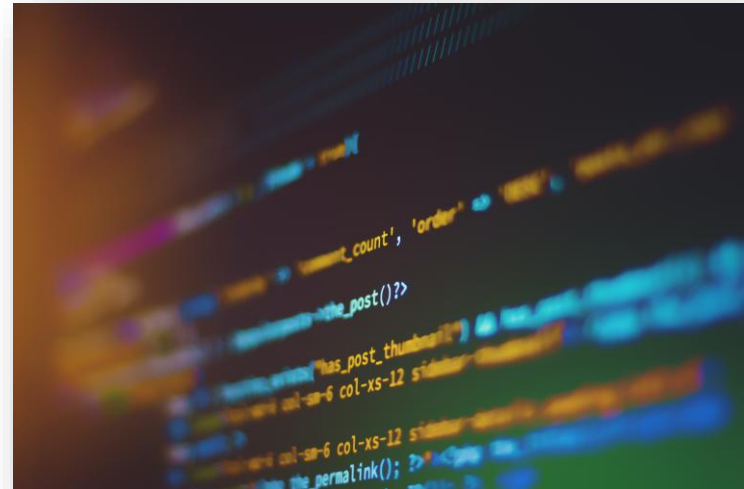
Vodenje dnevnika obdelave (22. člen ZVOP-2)

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

Zabeleži se (za vse vrste obdelav):

- **vrsto** dejanja obdelave,
- **datum in čas** obdelave,
- **identifikacijo osebe**, ki je izvedla obdelavo, ter
- identifikacijo **uporabnikov** OP.

Prehodno obdobje se je izteklo! (26.1.2025)



Vodenje dnevnikov obdelav

Uporaba:

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

Hramba:

- Vsebina dnevnika obdelave se hrani **dve leti od zaključka koledarskega leta, v katerem so bila zabeležena dejanja obdelave**, če drug zakon ne določa drugače.
 - Kadar je z oceno učinka ali analize upoštevni tveganj **ugotovljeno tveganje, ki ga je mogoče učinkovito upravljati s podaljšanjem roka hrambe**, se sme dnevnik obdelave hraniti **največ pet let od zaključka koledarskega leta**, v katerem so bila zabeležena dejanja obdelave.
 - Kadar so za seznanitev s podatki iz dnevnika določene omejitve (pravic posameznika) iz 17. člena, se vsebina dnevnika obdelave hrani **dve leti po prenehanju omejitev**, če drug zakon ne določa drugače.
- Kaj se preverja pri inšpekcijskem nadzoru glede dnevnikov obdelave?

Varnost osebnih podatkov na področju posebnih obdelav

Varnost osebnih podatkov na področju posebnih obdelav (23. člen ZVOP-2)

Za določene posebej občutljive zbirke (zaradi velikosti, podatkov ali drugih lastnosti), **se določa poseben sistem varovanja**.
Za informacijske sisteme, v katerih se izvajajo obdelave OP:

1. določenih v zakonih, ki urejajo področja upravnih notranjih zadev, finančne uprave, državljanstva, Slovenske obveščevalno-varnostne agencije, obrambe, zdravstvenega varstva, obveznega zdravstvenega zavarovanja, uveljavljanja pravic iz javnih sredstev ter kazenskih in prekrškovnih evidenc, ali
2. kadar se **na podlagi zakonov** (razen obdelave z videonadzorom - 3. poglavje 2. dela ZVOP-2) v zbirki OP obdelujejo OP **več kot 100.000 posameznikov**, ali
3. upravljavec ali obdelovalec **kot svojo temeljno dejavnost izvaja obsežne obdelave posebnih vrst OP** ali
4. kadar se v zbirki osebnih podatkov obdeluje **posebne vrste OP več kot 10.000 posameznikov**.

se smiselno uporabljajo **določbe o varnostnih zahtevah in priglasitvi incidentov iz Zakona o informacijski varnosti (ZInfV)**, ki se nanašajo na **izvajalce bistvenih storitev**, če upravljavec glede teh obdelav ni dolžan izvajati ukrepov po zakonu, ki ureja informacijsko varnost.

-> **glej 11., 12. in 13. člen ZInfV**

- **Sprejem novega ZinfV-1**
- **Predhodno obdobje do 26.1.2026! (116. člen ZVOP-2)**

Kaj mora o informacijski varnosti vedeti vsak zaposleni?

Ne gre samo za varnost IT! IT ne more sam zagotoviti informacijske varnosti.

Pomemben del informacijske varnosti smo ljudje in kako ravnamo.

Držimo se nekaj osnovnih načel varnostne higiene – TOP 10:

1. Poznam pravila za izbiro dobrih (in slabih) **gesel**.
2. Držim se **politike čiste mize** in čistega zaslona.
3. Vem, kaj se varnostno kopira in kam...**občasno preverim**.
4. Ni zastonj kosila.
5. Premislim, preden kliknem na povezavo...
6. Znam prepoznati nevarne priponke v e-pošti in vire, ki jim zaupam.. **.EXE, .BAT., .ZIP**
7. Če sem v dvomih, raje dvakrat preverim.
8. O varnostnih incidentih takoj poročam. **Poznam naš(e) pravilnik(e)**. Oziroma vsaj vem, kje jih najdem, če bo treba.
9. Prepoznam poskus phishinga.
10. **Brezplačen 30-minutni tečaj o informacijski varnosti za zaposlene:** <https://www.varninainternetu.si/kibernetska-varnost-podjetja-je-v-rokah-zaposlenih/>



Bodite pozorni na:

Za: **Info** <info@sibit.si>

Od: **Moja Banka** <mojabanka@neznano.si>

Predmet: **Nedovoljen poskus prijave**

IME

CEL NASLOV

- **Preverite PRAVO ime pošiljatelja!**

- Trik je **preprost in učinkovit**, ker nekateri programi za branje pošte ne pokažejo celotnega **naslova**. Zato v polju »Od« (»From«) vedno **preverite celoten naslov pošiljatelja**. Če je pošiljatelj npr. mojabanka.com, se mora ujemati tudi domena (del naslova za znakom @) ne le ime.

- **Preverite, kam DEJANSKO vodijo povezave!**

- **Premaknite kurzor** nad povezavo v poštnem sporočilu in se prepričajte, da povezava vodi tja, kamor mora. **Pogosto bodo povezave z lažnim predstavljanjem dolge in zapletene, s presežkom posebnih znakov. Če ni jasno, kam vodijo težave, ne kliknite nanjo.**



- **Poiščite personalizacijo!**

- Vsak pošiljatelj, s katerim si dopisujete, bi praviloma moral poznati vaše ime. Če ste naslovljeni s čim drugim, kot vašim imenom, potem lahko obravnavate to poštno sporočilo kot sumljivo.

- Posebej bodite pozorni na priponke tipa **.exe, .bat, .zip, .js**. **Ne jih odpirati, če niste prepričani!**

Posebne določbe

Posredovanje osebnih podatkov (javni sektor) 39. člen ZVOP-2

- **če obstaja podlaga (po 6. oz. 9. členu GDPR), ter na podlagi zahteve** po 41(1) členu ZVOP-2, razen če drug zakon določa drugače
- prejemnik podatkov sme OP obdelovati **samo za namen**, za uresničevanje katerega se mu posredujejo.
- **brezplačno** če zakon ne določa drugače.

Posebne določbe

Postopek posredovanja OP (41. člen ZVOP-2)

- **kaj mora vsebovati zahteva** (vlagatelj, pravna podlaga, namen, katere podatke, številko zadeve, navedba organa, oblika in način pridobitve),
 - **rok 15 dni** od popolne zahteve,
 - ob zavrnitvi/molku lahko zahteva odločitev nadzornega organa, sodno varstvo
 - ne posega v pravico do pregleda in prepisa spisa
 - sledljivost posredovanja 2 leti
 - ne velja za varnost države
- uporaba povezovalnih znakov (EMŠO, davčna...) – ne samo ta znak za pridobivanje OP (razen izjemoma).

Posebne določbe

Rok hrambe osebnih podatkov, določitev roka in vezanost na rok (43. člen ZVOP-2)

- rok hrambe podatkov – minimizacija glede na namen obdelave, razen če drug zakon za posamezne obdelave določa rok hrambe
 - Kdo določa rok hrambe in kakšni so?
- redno dokumentirano preverjanje
 - Določitev rokov hrambe – 2. odst. 13. člena GDPR
 - Redno?
 - Dokumentirano?
 - DPO?
- če drug zakon ne določa drugače: **izbris, uničenje ali anonimizacija po preteku rokov**, oziroma se izvede drug postopek, ki onemogoča identifikacijo posameznika, na katerega se nanašajo osebni podatki , zlasti omejevanje dostopa do njih, njihovo blokiranje ali arhiviranje.

Pooblaščene osebe za varstvo osebnih podatkov

Obveznost določitve pooblaščene osebe (45. člen ZVOP-2)

- **zavezanci za imenovanje:** iz 37. člena GDPR + 22. (1-4. odst.) člen ZVOP-2; definicija “javni sektor”!
- lahko prostovoljno in lahko namestnika
- **rok za vpis v evidenco dejavnosti in objavo ter sporočanje IP:** 8 dni
- **evidenca DPO pri IP ni javna.**

Pogoji za določitev pooblaščene osebe (46. člen ZVOP-2)

- poslovna sposobnost, znanje/izkušnje, neobsojenost
- DPO državnega organa mora biti iz javnega sektorja
- **JS razen državnih organov in zasebni sektor: lahko zunanji DPO (iz javnega ali zasebnega) – s pogodbo**
- ne sme biti **konflikta interesov**
- **natančneje opredeljen konflikt interesov:** upravljavec/skrbnik IS, vodja informacijske varnosti, predstojnik, če je član organov upravljanja/nadzora, če njene druge naloge vključujejo sistemsko odločanje o obdelavi OP, če zastopa upravljavca oziroma obdelovalca v sodnih ali arbitražnih postopkih.

Skupna določitev pooblaščene osebe in določitev pooblaščene osebe sindikata (47. člen ZVOP-2)

- skupna določitev dovoljena: odvetniki, sindikati, notarji (**GDPR: in javni organi/telesa**)

Pooblašcene osebe za varstvo osebnih podatkov

Naloge pooblašcene osebe (48. člen ZVOP-2)

- DPO opravlja **naloge iz 39. člena GDPR**

DPO ima vsaj naslednje naloge:

- a) obveščanje upravljavca ali obdelovalca in zaposlenih**, ki izvajajo obdelavo, ter **svetovanje** navedenim o njihovih **obveznostih** glede uredbe in **drugimi določbami** prava Unije ali prava države članice o varstvu podatkov;
- b) spremljanje skladnosti** s to uredbo, drugimi določbami prava Unije ali prava države članice o varstvu podatkov in **politikami upravljavca** ali obdelovalca v zvezi z varstvom OP, vključno z **dodeljevanjem nalog, ozaveščanjem** in **usposabljanjem** osebja, vključenega v dejanja obdelave, ter s tem povezanimi **revizijami**;
- c) svetovanje**, kadar je to zahtevano, glede **ocene učinka** v zvezi z varstvom podatkov in spremljanje njenega izvajanja;
- d) sodelovanje z nadzornim organom**;
- e) delovanje kot kontaktna točka za nadzorni organ** pri vprašanjih v zvezi z obdelavo, vključno s **predhodnim posvetovanjem**, in, kjer je ustrezno, posvetovanje glede katere koli druge zadeve.

II. DEL ZVOP-2

PODROČNE UREDITVE OBDELAVE OSEBNIH PODATKOV

Posebna pravila glede obdelave OP za znanstvenoraziskovalne, zgodovinskoraziskovalne, statistične in arhivske namene

Obdelava osebnih podatkov za raziskovalne namene (68.-70. člen ZVOP-2)

- **obdelava OP za raziskovanje (znotraj zavezanca) dopustna** če tako obdelavo **dovoljuje drug zakon**, *ali* če
 - **posameznik ni prepovedal obdelave svojih OP** za namen raziskovanja ali prepovedal obdelave svojih OP na določenem raziskovalnem področju, ki vključuje tudi namene raziskave,
 - *ali* je posameznik za OP, ki pomenijo poklicno skrivnost, za obdelavo dal pisno soglasje.

Raziskovalne organizacije pridobijo OP, vključno s posebnimi vrstami OP:

- morajo predložiti **opis raziskave** – kaj mora **vsebovati** (po 69(2). člena ZVOP-2) + **ocena učinka (69(3))**, če **obvezna po GDPR**
- **upravljavec zavrne posredovanje ***
 1. če niso izpolnjeni pogoji iz 2. in 3. odstavka 69. člena;
 2. če oceni, da zahtevani OP niso primerni za izvedbo raziskave;
 3. če oceni, da nameni oziroma cilji raziskave ne upravičujejo posega v pravice posameznikov;
 4. če upravljavec iz zasebnega sektorja in raziskovalna organizacija oziroma raziskovalec ne dosežeta soglasja o ceni posredovanja podatkov;
 5. če oceni, da ukrepi za varnost OP niso ustrezni, ali
 6. če gre za tajne podatke v skladu z zakonom o tajnih podatkih.

Posebna pravila glede obdelave OP za znanstvenoraziskovalne, zgodovinskoraziskovalne, statistične in arhivske namene

- **Posameznikov se ne obvešča o obdelavah njihovih OP za te namene, razen če zakon določa drugače.**
- OP, ki so bili predmet raziskave, se **ob zaključku raziskave uničijo ali nepovratno anonimizirajo**, razen če zakon določa drugače, če je posameznik privolil v nadaljnjo hrambo osebnih podatkov ali je nadaljnja hramba pomembna za izvršitev namena raziskave.
- **Rezultati raziskave se objavijo v anonimizirani obliki.** Rezultati raziskave se lahko objavijo tudi v psevdonimizirani obliki, če objava podatkov v anonimizirani obliki iz tehničnih razlogov ali zaradi zasledovanja ciljev raziskave ni mogoča.
- **Psevdonimizacija vs. anonimizacija?**

Varstvo svobode izražanja v razmerju do pravice do varstva osebnih podatkov (73. člen ZVOP-2)

- obdelava OP namene obveščanja javnosti s strani **medijev, književnega, umetniškega ali raziskovalnega ustvarjanja, resne kritike, obrambe kakšne pravice ali varstva upravičene koristi in izobraževanja** je dopustna:
 1. je posameznik za obdelavo, objavo ali razkritje OP dal **privolitev**;
 2. je posameznik OP **že javno objavil ali dal na razpolago javnosti**;
 3. so OP **na zakonit način že bili dostopni javnosti**;
 4. so bili **OP pridobljeni na podlagi prisotnosti posameznika na javno dostopnih krajih ali dogodkih**, kjer posameznik glede na vse okoliščine ne more razumno pričakovati varstva zasebnosti, ter na način, ki ne pomeni občutnega posega v razumno pričakovano zasebnost;
 5. gre za **zakonito objavo mnenja ali vrednostne ocene**, kjer je **objava OP nujna** za utemeljitev tega mnenja ali vrednostne ocene;
 6. so bili **OP pridobljeni na drug zakonit način**;
 7. **javni interes** po obveščanju javnosti, pravica do obveščenosti ter svoboda izražanja prevladajo nad upravičenimi interesi varstva zasebnosti in drugih osebnostnih pravic posameznika ali
 8. tako **določa drug zakon**.
- uveljavljanje pravic pred **sodišči**.
- za namene izvajanja svobode izražanja ni dopustno nezakonito razkrivanje OP.

Varstvo svobode izražanja in dostopa do informacij javnega značaja v razmerju do varstva osebnih podatkov

Varstvo pravice do dostopa do informacij javnega značaja v razmerju do pravice do varstva osebnih podatkov (74. člen ZVOP-2)

- zavezanci po ZDIJZ javnosti posredujejo OP, **če so ti po zakonu javni**
- ali če je **za njihovo razkritje dan prevladujoč javni interes** v skladu z ZDIJZ
- Kadar zakon določa javnost podatkov ali kadar gre za podatke, ki so IJZ, jih upravljavec, ki z njimi razpolaga, lahko javno objavi.

Izjema glede obveščanja posameznika (75. člen ZVOP-2)

Če so OP javni na podlagi zakona, posameznika *ni treba obveščati v skladu s 13. in 14. členom GDPR* ali vabiti k stranski udeležbi v skladu z določbami zakona, ki ureja splošni upravni postopek. *SPORNO

Splošne določbe o videonadzoru in varstvu osebnih podatkov (76. člen ZVOP-2)

- Določbe **tega poglavja** se uporabljajo za izvajanje videonadzora, če **drug zakon** ne določa drugače.
- **Odločitev o uvedbi** videonadzora sprejme **predstojnik, direktor** ali **drug pooblaščen posameznik** osebe javnega sektorja ali osebe zasebnega sektorja kot upravljavca. V **pisni odločitvi** morajo biti **obrazloženi razlogi za uvedbo** videonadzora. *Obrazloženi?*
- Upravljavec videonadzornega sistema o odločitvi **objavi obvestilo**.
- Obvestilo se **vidno in razločno objavi** na način, ki omogoča posamezniku, da se seznani z izvajanjem videonadzora in da se lahko vstopu v nadzorovano območje odpove. *Barva, velikost, pisave, število?*
- Obvestilo **poleg informacij iz prvega odstavka (*in drugega!) 13. člena GDPR** vsebuje informacije:
 1. pisno ali nedvoumno grafično opisano **dejstvo, da se izvaja videonadzor**;
 2. **namene** obdelave, navedbo **upravljavca** videonadzornega sistema, **telefonsko številko ali naslov elektronske pošte ali spletni naslov** za potrebe uveljavljanja pravic posameznika s področja varstva OP;
 3. **informacije o posebnih vplivih obdelave**, zlasti nadaljnje obdelave;
 4. **kontaktne podatke pooblaščne osebe** (DPO/pooblaščen oseba; telefonska številka ali naslov e-pošte);
 5. **neobičajne nadaljnje obdelave**, kot so prenosi subjektom v tretje države, spremljanje dogajanja v živo, možnost zvočne intervencije v primeru spremljanja dogajanja v živo.

- Namesto objave v obvestilu se lahko obveščanje posameznika izvede tudi na način, da upravljavec informacije iz **prvega (*in drugega!) odstavka 13. člena GDPR** in informacije iz 3. do 5. točke prejšnjega odstavka objavi **na spletnih straneh**. V tem primeru mora na obvestilu iz prejšnjega odstavka **objaviti spletni naslov**, kjer so te informacije dostopne.
- Šteje se, da je **z obvestilom** iz tretjega in prejšnjega odstavka **posameznik obveščen** o obdelavi OP.
- **Zbirka posnetkov videonadzornega sistema vsebuje posnetek posameznika (slika), podatek o lokaciji, datum in čas posnetka, izjemoma, če je to posebej nujno potrebno, pa tudi zvok.** *Tudi zvok?*
- Videonadzorni sistem **mora biti zavarovan**, kot to določata 24. in 32. člen **GDPR**.
- Posnetki videonadzora se lahko ob upoštevanju načel iz 5. člena **GDPR** hranijo **največ eno leto** od trenutka nastanka posnetka.
- Videonadzora **ni dovoljeno izvajati v dvigalih, sanitarijah, prostorih za preoblačenje, hotelskih sobah in drugih podobnih prostorih**, v katerih posameznik **utemeljeno pričakuje višjo stopnjo zasebnosti**. *Garderobe?*
- 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**.
- Upravljavec 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. Te podatke hrani v dnevniku obdelave iz 22. člena ZVOP-2 **dve leti po koncu leta, ko so nastali**. *Primer?*

Videonadzor dostopa v uradne službene oziroma poslovne prostore (77. člen ZVOP-2)

- Določbe tega poglavja se uporabljajo za izvajanje videonadzora, če drug zakon ne določa drugače.
- Upravitelji videonadzornega sistema v javnem in zasebnem sektorju lahko izvajajo videonadzor dostopa v uradne službene oziroma poslovne prostore, 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. *Kaj sodi pod „dostop“?*
- Videonadzor se izvaja **brez snemanja** delov stanovanjskih stavb, ki niso prostori iz prvega odstavka in **snemanja vhodov v stanovanja**.
- O izvajanju videonadzora in o vsebinah iz četrtega odstavka prejšnjega člena so **pisno obveščeni vsi zaposleni**, ki opravljajo delo v nadzorovanem prostoru.
- Videonadzor je **dovoljen**, če soglašajo lastniki, ki imajo v lasti več kot **70-odstotni delež skupnih delov**.
- **Zbirka OP** po tem členu **lahko vsebuje** poleg podatkov iz člena 76(7) tudi podatke za evidenco vstopov, če se navedeni OP zbirajo skupaj s posnetkom videonadzornega sistema. *Primer?*

Videonadzor znotraj delovnih prostorov (78. člen ZVOP-2)

- le, kadar je to **nujno potrebno** za **varnost ljudi ali premoženja ali preprečevanja ali odkrivanja kršitev na področju iger na srečo ali za varovanje tajnih podatkov ali za varovanje poslovnih skrivnosti**, teh namenov pa ni mogoče doseči z milejšimi sredstvi.
- Videonadzor se lahko izvaja **le glede tistih delov prostorov in v obsegu, kjer je treba** varovati interese iz prejšnjega odstavka.
- Prepovedano je z videonadzorom **snemati delovna mesta, kjer delavec po navadi dela, razen če je to nujno** v skladu s prvim odstavkom tega člena. *Primeri iz prakse?*
- **Neposredno spremljanje dogajanja pred kamerami** je pod pogoji iz prvega in drugega odstavka tega člena dopustno **le, če ga izvaja izrecno pooblaščen osebje upravljavca**. *Pooblastila, certifikati?*
- Zaposleni so pred začetkom izvajanja videonadzora po tem členu **vnapij pisno obveščeni** o njegovem izvajanju.

- Pred uvedbo videonadzora v osebi javnega ali zasebnega sektorja se mora **delodajalec posvetovati z reprezentativnimi sindikati pri delodajalcu in svetom delavcev oziroma delavskim zaupnikom**.
 - Posvetovanje se izvede v roku **30 dni** ali v drugem daljšem roku, ki ga določi delodajalec.
 - Kadar gre za uvedbo **videonadzora s snemanjem na delovnem mestu, se posvetovanje izvede v roku 60 dni** ali v drugem daljšem roku, ki ga določi delodajalec.
 - Posvetovanje ni potrebno:
 - na področju **varnosti države in varovanja tajnih podatkov**, razen za varovanje tajnih podatkov najnižje stopnje tajnosti, in
 - za **koncesionarje po zakonu, ki ureja igre na srečo** v delih prostorov, kjer se izvajajo igre na srečo.
- Videonadzor **skupnih prostorov** v poslovnih zgradbah je dovoljen, če s tem **soglašajo lastniki, ki imajo v lasti več kot 70-odstotni delež skupnih delov**.

Videonadzor na javnih površinah (80. člen ZVOP-2)

- Videonadzor na javnih površinah, kot jih določa **zakon, ki ureja urejanje prostora**, je dovoljen 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. *Lastništvo ali dostopnost površine?*

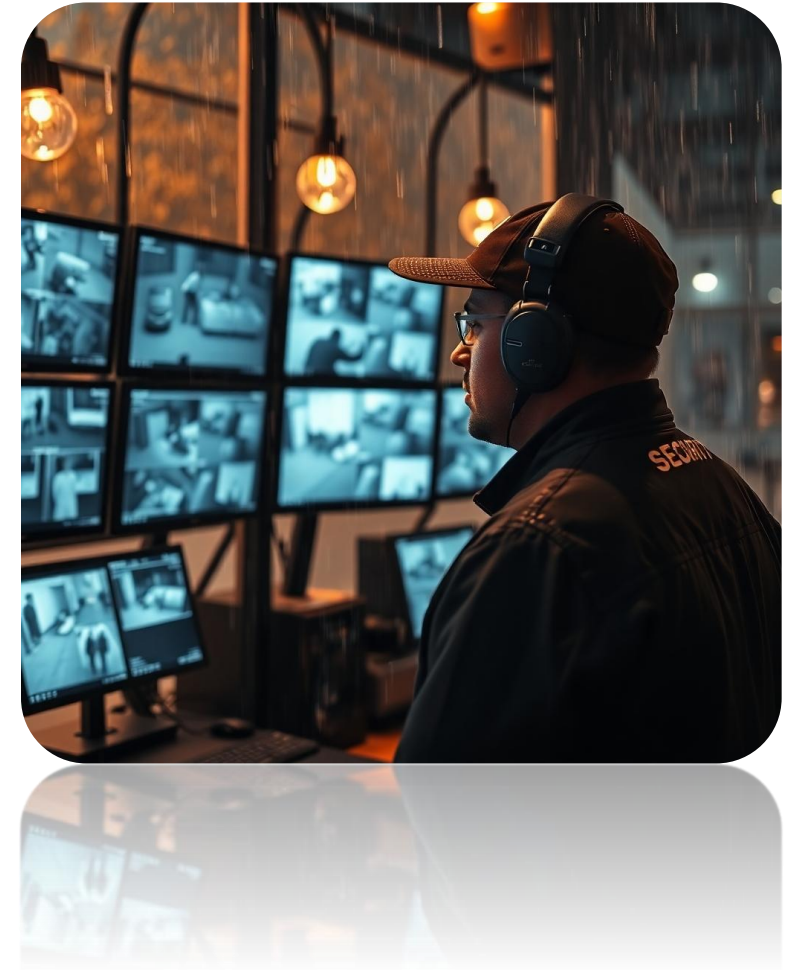
Videonadzor na javnih površinah je dovoljen tudi **za namene varovanja varovanih oseb ter posebnih objektov** in okolišev objektov, ki jih varuje policija, Slovenska vojska, pristojni organi za področje varnosti države, pravosodna policija, oziroma varovanja drugih prostorov, zgradb ali območij, ki jih je treba varovati na podlagi zakona, in sicer **samo v obsegu in trajanju, potrebnem za doseganje namena**. Vpogled, uporaba ali posredovanje posnetkov so dopustni le za te namene.

- Videonadzor se lahko izvaja **le glede bližnjih ali povezanih delov javne površine in v obsegu, kjer je treba varovati interese iz prejšnjega odstavka**.
- Videonadzor na javnih površinah lahko izvaja **oseba javnega ali zasebnega sektorja, ki upravlja z javno površino ali na njej zakonito opravlja dejavnost**. Videonadzor smejo za javni sektor izvajati **le uradne osebe ali pooblaščen varnostno osebje**, za zasebni sektor pa **pooblaščen varnostno osebje**. Mora biti izrecno pooblaščen za izvajanje videonadzora. *Pooblaščen?*
- Videonadzor se **lahko izvaja** tudi na način, da se ob snemanju izvaja **spremljanje dogajanja v živo**.

- Videonadzor iz prvega odstavka tega člena se 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.
- Posnetki videonadzora na javnih površinah se lahko **hranijo največ šest mesecev** od trenutka nastanka posnetka.
- Upravljavec videonadzornega sistema, ki izvaja videonadzor javnih površin, mora v primeru, **ko videonadzorni sistem posname dogodek, ki ogroža zdravje ali življenje posameznika, o tem nemudoma obvestiti policijo ali drug pristojni subjekt.** *24/7 spremljanje?*
- Na področju **videonadzora cestnega prometa** sme upravljavec izvajati videonadzor **le na vnaprej določenih odsekih cest v svojem upravljanju**, tako da se ne izvaja sistemsko nadzorovanje gibanja posameznikov ali poseganje v zasebnost posameznikov. Upravljavec mora **v skladu z zakonom določiti tiste odseke ceste** v svojem upravljanju, kjer z drugimi sredstvi ni mogoče doseči nujnega in učinkovitega varovanja cestnega prometa ali njegovega upravljanja. *→ ZCes-2*
 - Upravljavec videonadzornega sistema iz prejšnjega odstavka mora pred dokončno določitvijo lokacij iz prejšnjega odstavka **izdelati oceno učinka**, ki vsebuje lokacijo odsekov cest, in jo posredovati v predhodno mnenje nadzornemu organu.
- Na javnih površinah je **prepovedana uporaba sistemov za avtomatsko prepoznavo registrskih tablic in sistemov**, s katerimi se obdelujejo **biometrični OP**. – le če tako določa drug zakon (glej 76(1)). *Primeri v praksi?*

Kaj bo preverjal inšpektor?

- **Obvestilo**
 - Ali imate nameščeno obvestilo?
 - Ali je na vidnem mestu?
 - Ali ima predpisane sestavine?
 - 12. in 13. člen GDPR! *Največ 2 klika stran?*
- **Področje snemanja (sorazmernost: lokacijska in časovna)**
- **Pisna odločitev o uvedbi, sestavine**
- **Zavarovanje/varnost**
 - Kako je zavarovan videonadzorni sistem?
 - Kdo ima dostop do njega?
 - Kje in kako dolgo se podatki hranijo?
 - Ali obstajajo možnosti iznosa posnetkov?
 - Ali so se iznašali posnetki – komu, kdaj, s kakšnim namenom?
 - Ali se vodi evidenca dostopov in uporabe posnetkov?
- **Namenskost uporabe posnetkov**
- **Ostale zahteve po ZVOP-2 (npr. glede obveščanja zaposlenih, posvetovanja, omejitev dostopa, pooblaščenih oseb...)**

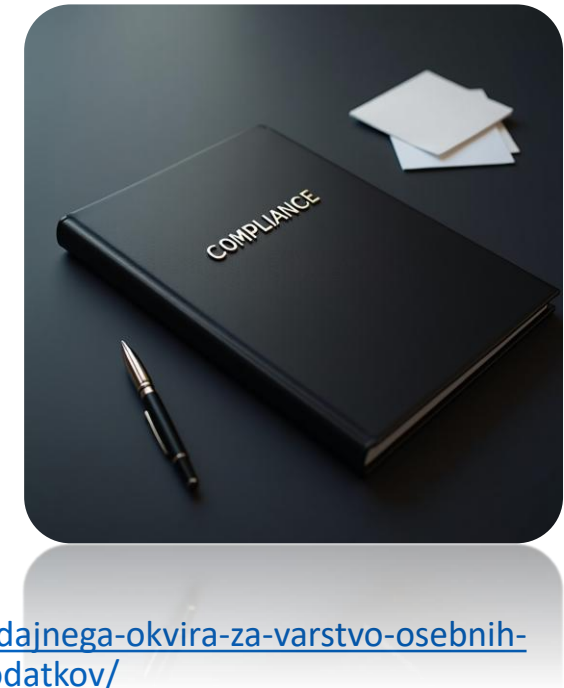


Videonadzor in GDPR

→ [Smernice EDPB](#)

GDPR se nanaša na vse zbirke, tudi na videonadzor. Ne pozabite na dolžnosti po GDPR:

- Informiranje posameznikov (12. in 13. člen)
- Vgrajeno in privzeto varstvo osebnih podatkov (25.člen)
- Ureditev skupnega/zunanjega izvajanja (25./28. člen)
- Vzpostavitev evidence dejavnosti obdelave (30. člen)
- Varnost (32. člen)
- Obveščanje o kršitvah varnosti (33. člen) *tudi izguba posnetkov?*
- Ocena učinka* (35. člen)
 - Vse informacije o ocenah učinka: <https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebni-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/ocena-u%C4%8Dinka-v-zvezi-z-varstvom-podatkov/>
- Vloga DPO (37.-39. člen)
- Pravice posameznika!
- Certifikacija po GDPR / ZVOP-2?



Obdelava kontaktnih podatkov in osebnih dokumentov

92. člen (javni kontaktni podatki)

- Osebe javnega ali zasebnega sektorja lahko javnosti posredujejo in javno objavijo:
 - **osebno ime, naziv ali funkcijo, službeno telefonsko številko in naslov službene elektronske pošte**
 - **vodilnih oseb in tistih zaposlenih, katerih delo je potrebno zaradi poslovanja s strankami.**

93. člen (obdelava osebnih podatkov za izvajanje določenih dejavnosti osebe javnega ali zasebnega sektorja)

- Za namene organiziranja uradnih srečanj, izobraževanj, ipd., dajanja izjav za javnost, razen izvajanja neposrednega trženja dovoljena uporaba kontaktnih podatkov posameznikov iz javno dostopnih virov ali v okviru izvrševanja svojih javnih nalog, če
 - so ji jih posamezniki prostovoljno razkrili,
 - ali dali privolitev,
- Te zbirke morajo biti ločene od drugih zbirk OP (oblastnega delovanja).
- **Le naslednje OP:** osebno ime, telefonsko številko, naslov elektronske pošte ali drugo komunikacijsko številko/oznako, podatke o delodajalcu/ organizaciji ter podatke o področju dela, položaju, funkciji, članstvu v klubu ali hobiju posameznika.
- Na podlagi **privolitve posameznika** lahko oseba javnega sektorja za iste namene obdeluje **tudi naslov stalnega ali začasnega prebivališča in druge OP, posebne vrste OP pa le izjemoma in če ima za to izrecno privolitev posameznika.**
- Za **namene obveščanja javnosti** sme oseba javnega ali zasebnega sektorja obdelovati, vključno z objavo: **osebna imena, nazive, fotografije in videoposnetke posameznikov, pridobljene na dogodkih,** ki jih v okviru svojih nalog, pristojnosti ali dejavnosti organizira ta oseba, **če posameznik te obdelave ni prepovedal.**

III. DEL

KAZENSKE DOLOČBE

- Ključne novosti/elementi
 - **Sankcije za kršitve, ki jih predpisuje GDPR**, se izrekajo **pravnim osebam**, samostojnim podjetnikom posameznikom in posameznikom, ki samostojno opravljajo dejavnost kot globe za prekrške, **v višini in razponih, kot jih določa GDPR.**
 - **Z ZVOP-2 se predpisujejo tudi sankcije za kršitve GDPR, ki so jih storile odgovorne osebe ali posamezniki:**
 - **200 do 8.000 eurov odgovorna oseba**
 - **200 do 2.000 eurov posameznik**
 - **Kršitve določb ZVOP-2**
 - **1.000 do 8.000 eurov za pravno osebo**
 - **100 do 5.000 eurov odgovorna oseba**

Kje dobimo več informacij?

Obrazci

- Informacije za posameznike (13.čl.)
- Vzorec pogodbe za pogodbeno obdelavo (28. čl.)
- Evidentiranje dejavnosti (30. čl.)
- Prijava kršitev varnosti (33. čl.)
- Imenovanje DPO (37. čl.)

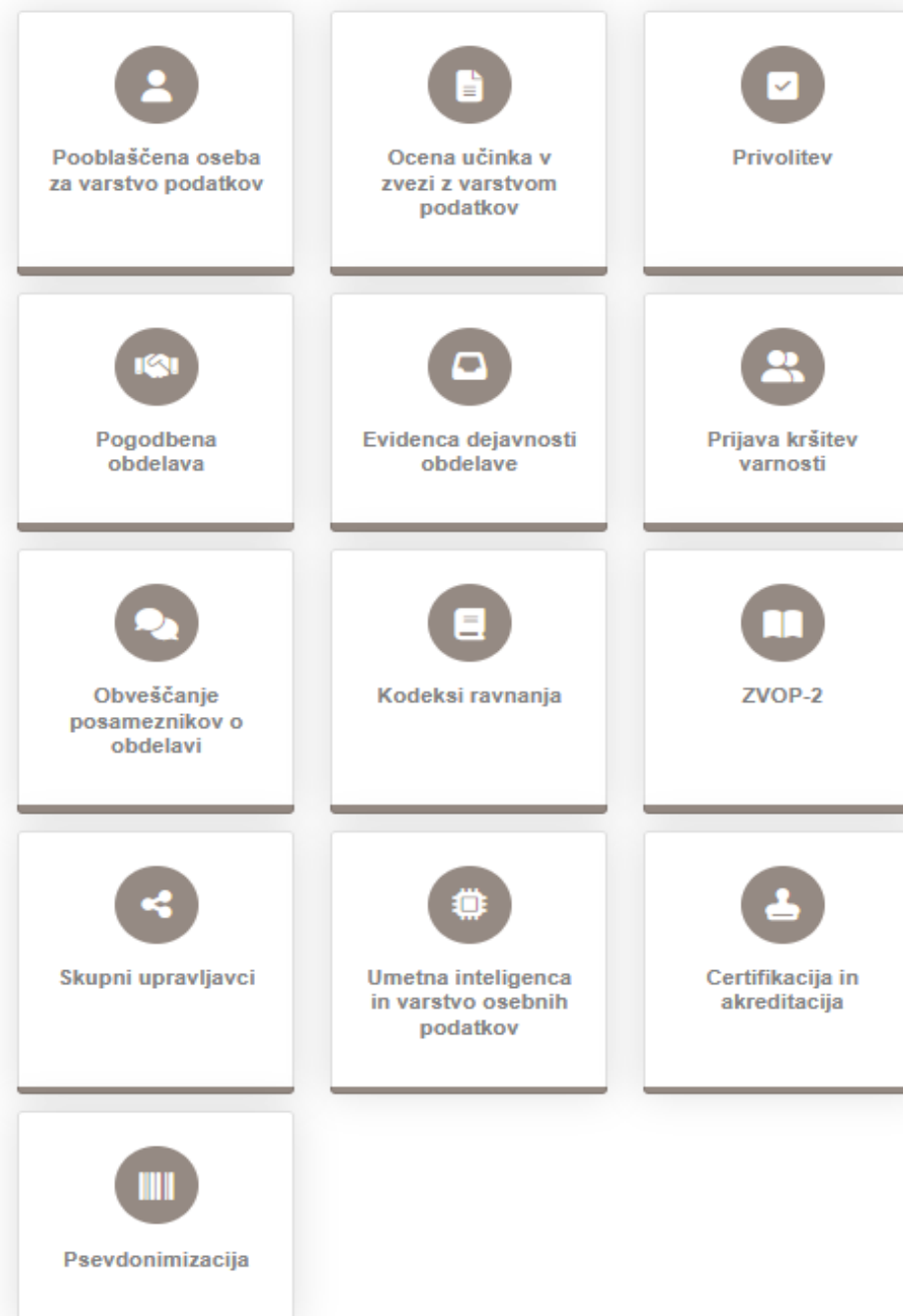
Smernice

www.ip-rs.si

Iskalnik po mnenjih (8000+)

Infografike

- GDPR na kratko - [PDF](#) | [PNG](#)
- Skupni upravljavci - [PDF](#) | [PNG](#)
- Pogodbena obdelava - [PDF](#) | [PNG](#)
- Prijava kršitev varnosti - [PDF](#) | [PNG](#) | ([angl.: PDF](#))
- Neupravičeni vpogledi v osebne podatke - [PDF](#) | [PNG](#)
- Prenos v tretje države - [PDF](#) | [PNG](#)
- Kako izbrati (še kar) dobro geslo...- [PDF](#) | [PNG](#)



Kako izbrati (še kar) dobro geslo?



DOBRE PRAKSE

- Enostavno za zapomniti, težko za uganiti
- Geslo ni zaporedje na tipkovnici
- Gesla ni v slovarju
- Gesel ne posojamo
- Gesel ne pišemo na listke
- Uporabi velike in male začetnice, številke in posebne znake



SLABE PRAKSE

- Imena partnerjev, ljubljenčkov, firm, besede iz slovarjev, filmov, knjig, letnice
- Vaši osebni podatki, kot so uporabniška imena, EMŠO, davčna, telefonske številke...
- Enostavni vzorci (npr. qwerty, abababab)
- Gesla, krajša od 6 znakov
- Geslo, ki se tako ali drugače nahaja v bližini (npr. model monitorja)



DOBRO GESLO V 3 KORAKIH

1. Izmisli si en stavek, ki si ga enostavno zapomniš, a ga je težko uganiti, npr.: „Nikoli ti ne povem mojega gesla, nepridiprav!“
2. Uporabi prve črke in ločila: Nikoli ti ne povem mojega gesla, nepridiprav!
→ Ntnpmg,n!
3. Dodaj številko, ki jo težko pozabiš, npr. 193.

Imaš super geslo, enostavno si ga zapomniš, težko ga je uganiti: **Ntnpmg,n!193**

In seveda – ne uporabljalj tega, ustvari si svoje geslo!



Hvala za
pozornost!

