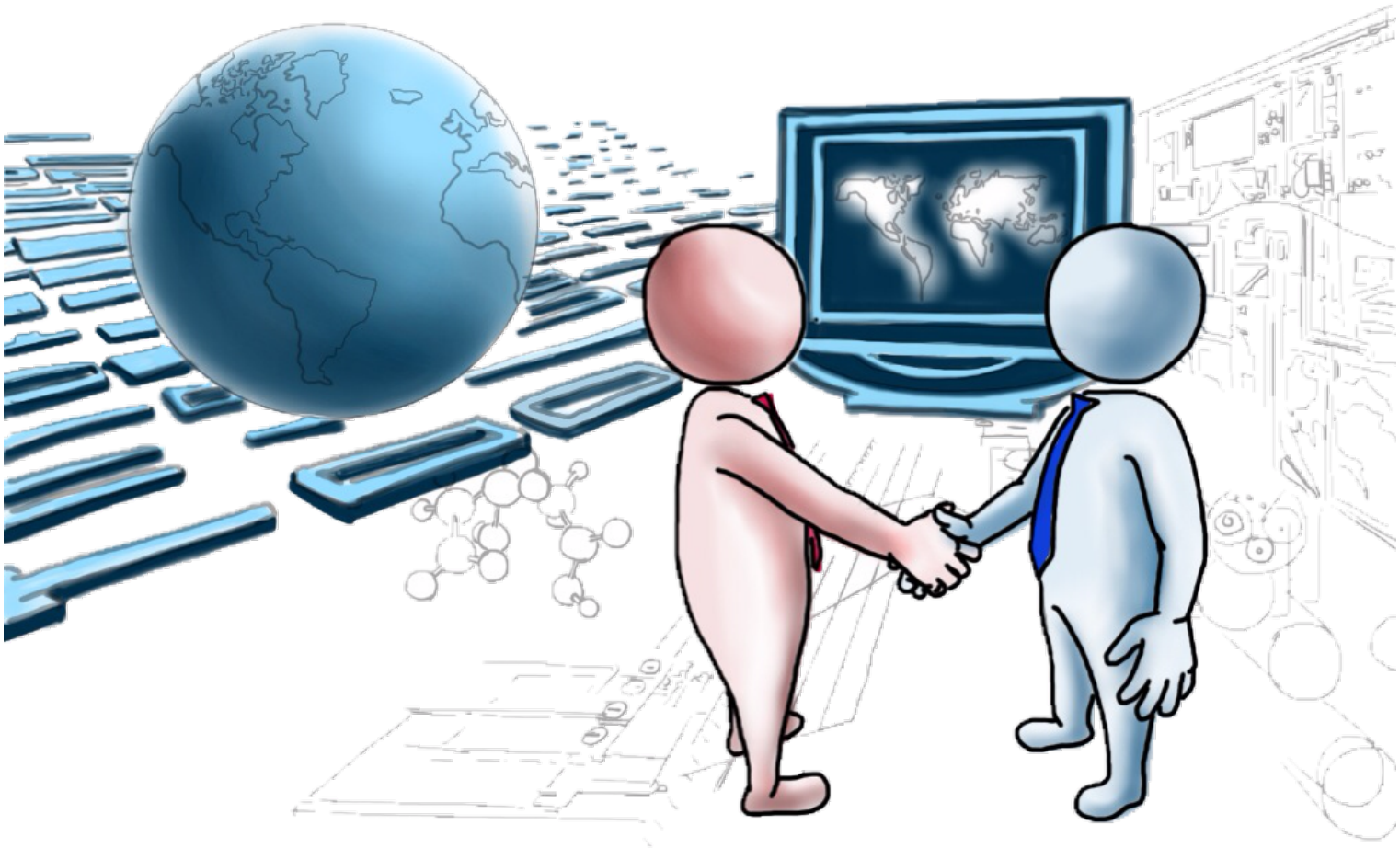
INFORMACIJSKI
POOBLAŠČENEC



Smernice Informacijskega pooblaščenca

o (pogodbeni) obdelavi osebnih podatkov

Namen dokumenta	Predstaviti pravni okvir za zakonsko skladno pogodbeno obdelavo osebnih podatkov in na podlagi praktičnih primerov podati usmeritve za dobre prakse na tem področju. Smernice so izdelane glede na določbe Splošne uredbe o varstvu podatkov (GDPR).
Ciljne javnosti	Vsi upravljavci osebnih podatkov (javni in zasebni sektor), ki želijo zaupati naloge povezane z obdelavo osebnih podatkov zunanjim izvajalcem.
Status	Javno
Verzija	1.2 (natančnejše pojasnilo glede prevajalcev in tolmačev, str. 11)
Datum izdaje	20. 3. 2020
Avtor	Informacijski pooblaščenec (Anže Novak - ilustracije)
Ključne besede	Pogodbena obdelava osebnih podatkov, pooblastila upravljavca osebnih podatkov, obdelovalec, varnost osebnih podatkov, čezmejna pogodbena obdelava osebnih podatkov, podobdelava, Splošna uredba o varstvu podatkov.

Kazalo

hitri vodič

po pogodbeni obdelavi osebnih podatkov

Preden osebne podatke zaupate zunanjemu izvajalcu - (pogodbenemu) obdelovalcu - morate vedeti:

- S kakšnimi nameni boste osebne podatke posredovali zunanjemu izvajalcu?
- Ali bo zunanji izvajalec opravljal naloge v zvezi z obdelavo osebnih podatkov samo v okviru vašega navodila ali pa bo podatke smel uporabljati tudi za svoje namene? (V tem primeru gre za prenos k drugemu upravljavcu in ne za pogodbeno obdelavo!)
- Ali zunanji izvajalec zagotavlja primerno varnost osebnih podatkov? Kakšno raven informacijske varnosti pričakujete?
- Da ste kljub posredovanju osebnih podatkov zunanjemu izvajalcu za zakonito obdelavo odgovorni vi kot upravljavec – razen v primeru, ko s primerno pogodbo in nadzorom nad pogodbenim obdelovalcem v največji razumni meri poskrbite za zakonitost obdelave osebnih podatkov, pa pogodbeni obdelovalec ravna v neskladju z vašimi navodili ali krši zakon.
- Ali bodo podatki posredovani v tujino, v tretje države ali mednarodne organizacije? V tem primeru morate spoštovati tudi določbe glede prenosa v tretje države ali mednarodne organizacije.

Skleniti morate pogodbo ali drug pravni akt o pogodbeni obdelavi, ki vsebuje določila glede na določbe 28. člena Splošne uredbe o varstvu podatkov in določa obveznosti obdelovalca do upravljavca, v katerem so določeni:

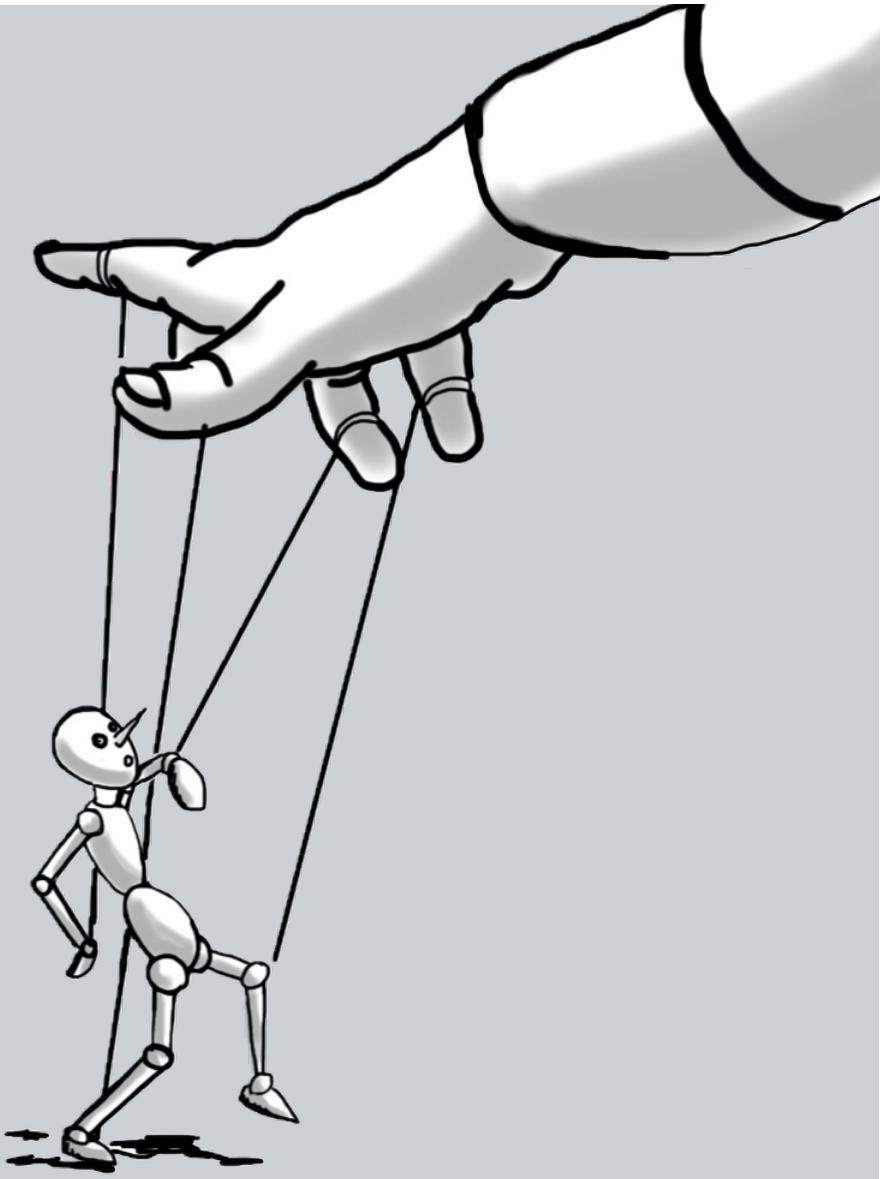
- vsebina in trajanje obdelave,
- narava in namen obdelave,
- vrste osebnih podatkov,
- kategorije posameznikov, na katere se nanašajo osebni podati,
- ukrepi zagotavljanja ustrezne ravni varstva podatkov v primeru prenosa podatkov izven EU,
- obveznosti in pravice upravljavca ter druge zahteve iz 28. člena Splošne uredbe.

Po koncu pogodbene obdelave osebnih podatkov

… vam mora obdelovalec kot zunanji izvajalec podatke vrniti in morebitne kopije izbrisati, razen če posebni predpisi zahtevajo od zunanjega izvajalca shranjevanje določenih osebnih podatkov.

Obdelovalec mora:

- izpolnjevati pogodbene obveznosti, kot jih je dorekel z upravljavcem po 28. členu uredbe,
- zagotavljati ustrezno varnost podatkov, ki so mu zaupani,
- zaposlene ustrezno sezaniti z dolžnostmi glede varovanja osebnih podatkov,
- evidentirati dejavnost obdelave po 30. členu Splošne uredbe,
- v primeru kršitev brez nepotrebnega odlašanja s tem seznaniti upravljavca,
- v določenih primerih imenovati pooblaščeno osebo za varstvo (37. člen Splošne uredbe).



Uvod

Upravljavci zbirk osebnih podatkov številne obdelave osebnih podatkov zaupajo pogodbenim obdelovalcem, kar velja tudi za največje državne registre in druge velike zbirke osebnih podatkov. Velik izziv predstavljajo tudi nove oblike izvajanja informacijskih storitev, ki so po naravi globalne in veliko bolj fluidne, kot to predvidevajo naši zakonski okviri, npr. računalništvo v oblaku, kjer gre običajno za pogodbeno obdelavo osebnih podatkov, pogodbeni partnerji so velika multi-nacionalna podjetja, osebni podatki pa se nahajajo na (pogosto) neznanih lokacijah. ZVOP-1 je uporabljal pojem »pogodbena obdelava«, medtem ko Splošna uredba o varstvu podatkov (GDPR) uporablja zgolj pojem »obdelava«. Zgolj zaradi kontinuitete in jasnosti v smernicah še vedno uporabljamo oba pojma.

V Smernicah Informacijskega pooblaščenca o pogodbeni obdelavi z mnogimi praktičnimi primeri pojasnjujemo, kaj vse sodi med pogodbeno obdelavo, kakšne so obveznosti upravljavca osebnih podatkov in njegovih pogodbenih obdelovalcev, ter katere so pasti in priporočila za zakonsko skladno ureditev zunanjega izvajanja storitev, ki vključuje osebne podatke.

Najprej je predstavljena pravna ureditev področja, skupaj s ključnimi opredelitvami in obveznostmi, ki jih nosijo subjekti pri pogodbeni obdelavi. Konkretni primeri kažejo primerne načine za zakonsko skladne ureditve. Posebej je v smernicah opredeljeno zavarovanje osebnih podatkov ter pojasnjena pristojnost Informacijskega pooblaščenca, tudi v primerih čezmejne pogodbene obdelave.

3. Pravna ureditev pogodbene obdelave osebnih podatkov

3.1 Ključne definicije: upravljavec osebnih podatkov, obdelovalec osebnih podatkov, obdelava osebnih podatkov

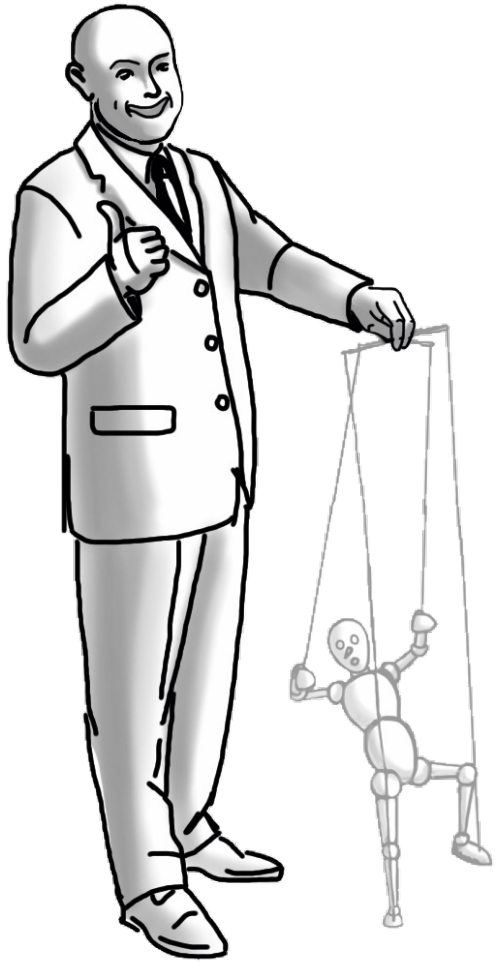
Splošna uredba v 7. točki 4. člena določa, da **upravljavec osebnih podatkov**:

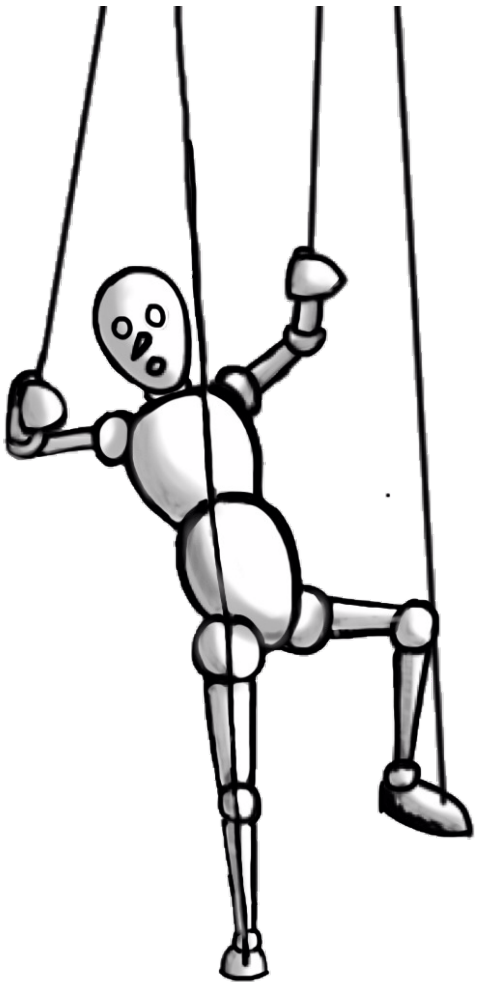
> *"pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; kadar namene in sredstva obdelave določa pravo Unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Unije ali pravom države članice".*

Obdelovalec osebnih podatkov pa glede na 8. točko 4. člena Splošne uredbe

> *"pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca."*

Obdelovalci so torej tiste organizacije oziroma posamezniki, ki po naročilu določenega upravljavca osebnih podatkov (stranka, naročnik, druga organizacija, podjetje, tudi organ iz javnega sektorja) in v skladu z njegovimi zahtevami za določeno nalogo oziroma namen zanj obdelujejo osebne podatke posameznikov.





Splošna uredba v 2. točki 4. člena določa, da **obdelava osebnih podatkov**

> *"pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje."*

Obdelavo osebnih podatkov moramo torej razumeti široko – to je katero koli ravnanje z osebnimi podatki, med drugim tudi vpogled, urejanje, vnašanje, uničevanje, brisanje, hramba, tudi v primeru, ko obdelovalec morda niti ne ve, da za upravljavca hrani osebne podatke. Gre namreč za dolžnost upravljavca, da ustrezno seznani obdelovalca, da mu namerava poveriti osebne podatke v obdelavo, tudi če gre zgolj za hrambo ali uničenje. Če obdelovalec ne bi vedel, da so mu bili zaupani osebni podatki, potem jih ne bi mogel ustrezno varovati.

KAJ SODI MED POGODBENO OBDELAVO?

- Najem storitev podjetja, ki bo za nas izvajalo videonadzor vhoda v poslovne prostore,
- najem storitev klicnega centra, ki bo našim naročnikom predstavljal našo ponudbo,
- najem računovodskih storitev, npr. obračun plač zaposlenih,
- najem storitev arhiviranja in hrambe osebnih podatkov,
- najem podatkovnega centra, v katerem bomo hranili osebne podatke,
- zunanje vzdrževanje spletnih strani,
- prevoz osebnih podatkov na uničenje in samo uničenje itd.

Pogosto v primerih uporabe sodobnih informacijskih rešitev ni povsem jasno, kdo je upravljavec in kdo morebitni obdelovalec osebnih podatkov, še posebej, kadar neka rešitev vsebuje široko mrežo subjektov in odnosov med njimi.

PRIMER: PONUDNIKI GOSTOVANJA KOT OBDELOVALCI.

V praksi so pojavlja vprašanje, ali so ponudniki gostovanja, ki za svoje kliente morda hranijo tudi njihove zbirke osebnih podatkov, tudi pogodbeni obdelovalci. V takem primeru ponudnika gostovanja razumemo kot obdelovalca osebnih podatkov (hramba sodi med obdelavo osebnih podatkov), kar pomeni, da bi moral njegov naročnik kot upravljavec z njim skleniti ustrezno pogodbo o pogodbeni obdelavi osebnih podatkov. Če pogodba ni sklenjena, upravljavec nosi odgovornost, ker je osebne podatke brez ustrezne pravne podlage predal v hrambo ponudniku gostovanja ter tudi odgovornost v primeru neustreznega ravnanja z osebnimi podatki s strani ponudnika gostiteljstva. Navedeno velja tudi če so hranjeni podatki kriptirani, tako da ponudnik gostovanja niti ne more prebrati osebnih podatkov. Upravljavec bo namreč praviloma vedno vedel, ali pri nekomu hrani osebne podatke ali ne, zato je njegova dolžnost, da od ponudnika zahteva sklenitev ustrezne pogodbe.

Namen ustrezne ureditve pogodbene obdelave je predvsem:

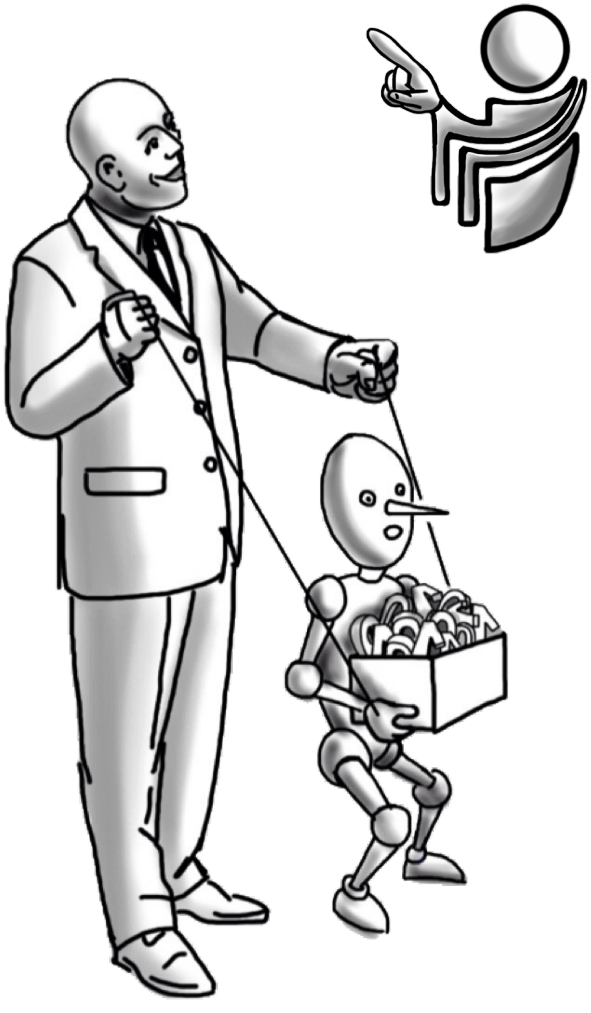
- jasnost razmerja med naročnikom in zunanjim izvajalcem (predvsem z vidika obsega nudenih storitev),
- zagotovitev ustrezne varnosti pri obdelavi osebnih podatkov,
- natančna razmejitev odgovornosti med naročnikom in izvajalcem.

Pomembno je, da upravljavec v vsakem primeru ohrani nadzor nad osebnimi podatki, katerih upravljavec je, in da tako kljub morebitnemu zunanjemu izvajanju določenih obdelav zagotavlja ustrezno varstvo.

Ustrezna ureditev pogodbene obdelave osebnih podatkov je in bi morala biti predvsem v interesu upravljavcev, saj so oni tisti, ki se odločajo za najem obdelovalcev in oni so tisti, ki morajo zagotoviti oz. zahtevati, da so osebni podatki ustrezno varovani in obdelovani. V primeru neurejenih pogodbenih razmerij lahko namreč sami nosijo odgovornost za kršitve, ki jih je storil obdelovalec ali celo z njegove strani najeti podizvajalci (npr. javna objava osebnih podatkov zaradi neustrezne varnosti, izguba osebnih podatkov ipd.). Če na vse skupaj pogledamo tudi skozi oči posameznika – ta pričakuje, da so njegovi podatki enako dobro varovani, ne glede na to, ali so pri upravljavcu ali pri njegovih morebitnih zunanjih izvajalcih, tudi če ti nudijo upravljavcu samo hrambo podatkov.

Delovna skupina za varstvo podatkov iz člena 29[1] v svojem mnenju[2]. pojasnjuje, da je vloga upravljavca predvsem ta, da določa, kdo je odgovoren za spoštovanje pravil varstva osebnih podatkov in kako lahko posamezniki v praksi uveljavljajo svoje pravice (do vpogleda, do izbrisa, itd.). Tak položaj upravljavca je posledica dejstva, da obdeluje osebne podatke za svoj namen in za svoje cilje, da skladno s tem določi nabor osebnih podatkov, načine obdelave, kdaj bodo podatki izbrisani in kdo so osebe, ki naj imajo dostop do osebnih podatkov. Kadar o namenih in sredstvih obdelave odloča več entitet, lahko govorimo tudi o več upravljavcih oziroma o skupnem upravljavcu.

Obdelovalec osebnih podatkov pa nasprotno osebne podatke obdeluje le v okviru pooblastil upravljavca. Osebnih podatkov ne sme obdelovati za svoje namene in jih mora po koncu pogodbene obdelave vrniti upravljavcu oz. jih izbrisati, razen če posebni predpisi zahtevajo od zunanjega izvajalca shranjevanje določenih osebnih podatkov tudi po tem trenutku. V tem primeru vse dolžnosti glede uveljavljanja pravic posameznikov in skladnosti z zakonodajo še vedno nosi upravljavec, pogodbeni obdelovalec pa je predvsem dolžan spoštovati zahteve Splošne uredbe po ustreznih postopkih in ukrepih za varnost osebnih podatkov.



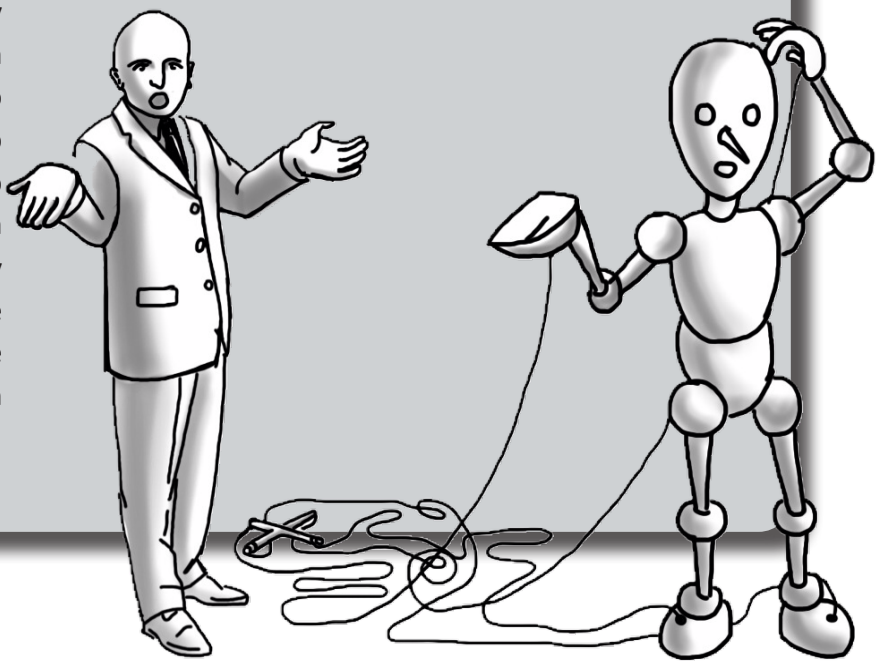
[1] Svetovalno telo Evropske komisije, v kateri so združeni vsi nadzorni organi za varstvo osebnih podatkov iz EU (Article 29 Working Party). Article 29 Working Party je z uporabo Splošne uredbe o varstvu podatkov nadomestil Evropski odbor za varstvo podatkov (European Data Protection Board – EDPB)

[2] Mnenje št. 1/2010 o konceptu upravljavca osebnih podatkov

PRIMER: UPRAVLJAVEC ALI OBDELOVALEC?

Podjetje za drugo družbo iz tujine na slovenskem trgu trži aplikacijo na podlagi franšizne pogodbe. Ali ima obveznosti upravljavca osebnih podatkov?

Pri določanju, kdo je upravljavec in kdo obdelovalec osebnih podatkov je ključno, **kakšna je vloga določenega subjekta pri pridobivanju podatkov**, izvrševanju pravic do vpogleda, brisanja posameznikov, nabora osebnih podatkov, določanja namenov in sredstev obdelave, dejanskega dostopa do baze osebnih podatkov, ki se obdelujejo. Tu velja tudi opozorilo, da določitev vlog v pogodbi v smislu določanja upravljavca ni bistvena; vedno je odločilno dejansko stanje glede namenov in sredstev za obdelavo osebnih podatkov. Če ima podjetje dostop do osebnih podatkov, ki se obdelujejo, določa namene in sredstva obdelave (lahko tudi v sodelovanju s ponudnikom iz tujine) in izvršuje pravice uporabnikov, potem ima podjetje odgovornosti upravljavca osebnih podatkov in ne le pogodbenega obdelovalca.



3.2 Meje pogodbene obdelave

Pri nekaterih subjektih in storitvah se v praksi postavljajo vprašanja, ali je tudi določenega subjekta upoštevaje storitve, ki jih ponuja upravljavcu, treba šteti za obdelovalca osebnih podatkov. Taki subjekti so npr.:

- operaterji elektronskih komunikacij,
- pošta,
- revizorji,
- prevajalci,
- sodni izvedenci in tolmači,
- organi javnega sektorja, ki drugim zagotavljajo IT storitve oz. infrastrukturo,
- odvetniki,
- ponudniki storitev taksi prevozov,
- ponudniki storitev čiščenja poslovnih prostorov,
- ponudniki storitev virtualne (npr. spletno gostovanje) ali fizične hrambe podatkov (npr. sefi) idr.

Pri ugotavljanju, ali gre za (pogodbenega) obdelovalca, so ključni naslednji faktorji:

- Ali subjekt lahko sam določa namen in sredstva obdelave osebnih podatkov?
- Ali je upravljavec zbirke osebnih podatkov subjektu poveril v izvajanje opravila obdelave, ki bi jih sicer lahko izvajal upravljavec sam?
- Kakšna je intenzivnost obdelave, vezanost na navodila in nadzor upravljavca nad dejanji subjekta?
- Ali ima subjekt zakonska pooblastila oziroma pravno podlago, ki bi ga deloma ali v celoti postavila za upravljavca v zvezi z osebnimi podatki upravljavca?
- Ali je primarni namen najema storitev subjekta katero od dejanj obdelave osebnih podatkov (npr. hramba) ali pa je obdelava osebnih podatkov zgolj posledica najetja storitve subjekta?

Vsaj te kriterije je vedno treba presojati skupaj.

V vlogi obdelovalca bo nastopala tista pravna oziroma fizična oseba, ki bo obdelavo osebnih podatkov izvrševala:

1. izključno v imenu in za račun upravljavca osebnih podatkov,
2. bo pri tem črpala podlago za obdelavo osebnih podatkov iz upravičenj upravljavca ter
3. bo v zvezi s samimi dejanji obdelave vezana na navodila upravljavca.

Glede na navedeno:

- **Operaterji elektronskih komunikacij** in **pošta** se v delu, ko zagotavljajo storitve prenosa podatkov ali dokumentacije ne štetejo za obdelovalce, saj zagotavljajo regulirane storitve, ki bi jih upravljavci sami zase težko ali celo nepooblaščeno izvajali brez nesorazmerno visokih stroškov. Praviloma gre za visoko regulirane dejavnosti, kjer se zahteva od tovrstnih ponudnikov visoka stopnja varovanja zasebnosti komunikacij in podatkov.
- **Revizorje** oziroma revizijsko družbo se šteje kot obdelovalce izključno v primerih, ko pravna oseba najame storitve teh subjektov za namene izvedbe notranje revizije ali storitev na ostalih strokovnih področjih povezanih z revidiranjem, kot jih opredeljuje Zakon o revidiranju: računovodstvo, poslovne finance, notranje revidiranje, revidiranje informacijskih sistemov, davčno proučevanje in svetovanje, ocenjevanje vrednosti podjetij, nepremičnin ter strojev in opreme. O revizorju kot obdelovalcu govorimo torej kadar se upravljavec odloči izvesti notranjo revizijo ali najame revizorja za izvedbo katere druge od zgoraj navedenih storitev, ki služijo predvsem kot pomoč poslovodstvu podjetja, da bi učinkovito opravljalo naloge vodenja ter zagotavljanje strokovnih ocen stanja in priporočil za izboljšanje poslovanja na revidiranem področju. Notranja revizija je namenjena preverjanju ustreznosti notranjih sistemov poslovanja ter svetovanju poslovodstva pri izboljšanju poslovanja in je povsem fakultativne narave. Za izvedbo notranje revizije in drugih zgoraj navedenih storitev lahko pravna oseba zaposli osebo, ki bo revidiranje in drugo opravljala v okviru delovnega razmerja, lahko pa se pravna oseba posluži tudi najema zunanjih strokovnjakov z ustreznim znanjem, pri čemer je pri odločitvi ali ter koga bo pravna oseba pri tem najela, povsem svobodna in je zahteva iz 1. odstavka 5. člena ZRev-2 ne zavezuje. Kadar torej gre za izvajanje storitev v okviru notranje revizije in drugih zgoraj navedenih storitev za drugo pravno osebo (upravljavca), je mogoče šteti, da revizorji oziroma pravne osebe, najete za izvedbo notranje revizije (ali storitev na ostalih strokovnih področjih povezanih z revidiranjem, kot jih opredeljuje ZRev-2: računovodstvo, poslovne finance, notranje revidiranje, revidiranje informacijskih sistemov, davčno proučevanje in svetovanje, ocenjevanje vrednosti podjetij, nepremičnin ter strojev in opreme), nastopajo kot podaljšana roka upravljavca in s tem v vlogi pogodbenega obdelovalca. Drugače pa IP ocenjuje pri najemu revizijske družbe za izvedbo zunanje revizije v smislu ZRev-2. Že iz določbe 1. odstavka 5. člena izhaja, da revizijo v smislu ZRev-2 lahko izvaja izključno revizijska družba. ZRev-2 sicer določa, da se revidiranje opravlja v primerih, določenih z zakonom, ali na podlagi naročila pravne osebe, vendar z vidika položaja revizijske družbe glede obdelav osebnih podatkov IP meni, da ločevanje glede na »prisilnost« oziroma »prostovoljnost« pri izvedbi zunanje revizije, ni na mestu. Tako v primerih, ko revizijo izvaja revizijska družba zaradi zakonske obveze revidiranca, kot tudi kadar se revizija izvaja na podlagi povsem prostovoljne odločitve pravne osebe, bosta položaja revizijske družbe pri izvedbi ene ali druge revizije povsem izenačena, saj bo revizor, oziroma revizijska družba tako v enem, kot v drugem primeru primorana v celoti upoštevati zahteve ZRev-2 (prim 1. odstavke 4. člena ZRev-2). V obeh primerih pa je glede na položaj revizijske družbe to šteti kot upravljavca osebnih podatkov, saj revizijo izvaja sicer po naročilu pravne osebe (zakon ne predvideva izvajanja revizije po uradni dolžnosti), vendar

v svojem imenu, v takšnem svojstvu pa tudi obdeluje osebne podatke za namene, ki jih določa ZRev-2.[3]

- **Prevajalcev** in **sodnih izvedencev** ter **tolmačev** praviloma ne štejemo za obdelovalce, razen kadar na to kažejo konkretne okoliščine same dejavnosti prevajanja ali tolmačenja. Te okoliščine so lahko med drugim prevajanje besedil, ki so po svoji naravi zbirke osebnih podatkov ali podatki očitno izhajajo iz zbirke osebnih podatkov in je zato tveganje za pravice in svoboščine posameznikov večje (npr. zdravstvene diagnoze ali druga zdravstvena dokumentacija, izdana potrdila tujih organov o dejstvih, ki izhajajo iz uradnih evidenc z osebnimi podatki, upravne in sodne odločbe, itd.). Praviloma pa, kadar ne gre za tovrstna besedila, je morebiten stik prevajalcev in tolmačev z osebnimi podatki le "kolateralna škoda" storitve in ne namen storitve, zato se jih ne šteje za obdelovalce. Presoja ali gre v konkretnem primeru za obdelavo osebnih podatkov, pa je v odgovornosti upravljavca osebnih podatkov. Vsi prevajalci in sodni tolmači morajo ne glede na razmerje upravljavec-obdelovalec, vselej ob stiku z osebnimi podatki poskrbeti in zagotoviti potrebne ukrepe varnosti osebnih podatkov.
- **Organe javnega sektorja, ki drugim zagotavljajo IT storitve oz. infrastrukturo,** kot so storitve elektronske pošte, hrambe in gostovanja podatkov ipd., se v tem delu šteje za pogodbene obdelovalce in ne za upravljavce, saj samostojno ne določajo namena in sredstev obdelave osebnih podatkov, temveč je to v domeni organov, ki uporabljajo storitve. Ministrstvo za javno upravo, ARNES, IZUM in njim podobni organi javnega sketorja, ki drugim organom nudijo IT in druge storitve, se v tem delu štejejo za pogodbene obdelovalce.
- **Odvetnikov** se v delu, ko zastopajo svoje stranke in se pri tem seznanijo z osebnimi podatki, ne šteje za obdelovalce, temveč za upravljavce dokumentacije oziroma osebnih podatkov, saj jih kot take določa Zakon o odvetništvu (podobno kot pri najemu revizijske družbe za izvedbo zunanje revizije v smislu ZRev-2)[4] . Podobno velja za **notarje**.
- **Ponudnikov storitev taksi prevozov** in ponudnikov **storitev čiščenja poslovnih prostorov**, se ne šteje za obdelovalce, saj primarni namen storitev subjekta ni obdelava osebnih podatkov, temveč je obdelava osebnih podatkov zgolj posledica najetja storitve subjekta, t.j. storitev praviloma ni možna brez osebnih podatkov (taksi služba se npr. seznani z osebnimi podatki zaposlenih, katerih prevoze opravlja za naročnika. Pri opravljanju storitev čiščenja poslovnih prostorov bi se zaposleni sicer lahko seznanili z določenimi osebnimi podatki pri upravljacu, kjer zaposleni niso vestno poskrbeli za varnost dokumentacije, a namen storitve ni obdelava osebnih podatkov).
- **Ponudnike** storitev **virtualne** (npr. spletno gostovanje) ali **fizične hrambe podatkov** (npr. sefi, skladiščni prostori) moramo obravnavati kot obdelovalce, saj so s strani upravljavca najeti za dejanje, ki sodi med obdelavo osebnih podatkov (hramba podatkov). Ponudniki teh storitev ne morejo nositi odgovornosti glede varstva osebnih podatkov, vse dokler jih upravljavec ne seznani z dejstvom, da namerava pri njih hraniti osebne podatke (ti so lahko za ponudnika tudi v neberljivi obliki) – upravljavec osebnih podatkov pa je dolžan ponudnike hrambe seznaniti z dejstvom, da bo pri njih hranil osebne podatke iz svojih zbirk in da morata njuno razmerje urediti skladno z 28. členom Splošne uredbe. Prav tako iz inšpekcijske prakse izhaja, da je prišlo do zlorab osebnih podatkov (npr. javnega razkritja, omogočanja dostopa nepooblaščenim osebam) ravno zaradi dejstva, ker upravljavci niso ustrezno uredili pogodbenega razmerja z obdelovalci, slednji pa se niso zavedali, da se pri njih hranijo osebni podatki, za katere bi morali zagotovoti ustrezno raven varnosti.

[3] Podrobnejša razlaga v mnenju št. 0712-3/2018/503, ki je dostopno na spletni strani IP.

[4] Glej tudi Mnenje št. 1/2010 o konceptu upravljavca osebnih podatkov, str. 28.

3.3 Ureditev pogodbenega razmerja z obdelovalci

Dolžnosti in pravice upravljavcev, ki najemajo storitve obdelovalcev, vključno s podobdelovalci, podrobneje ureja **28. člen Splošne uredbe**, ki določa:

1. Kadar se obdelava izvaja v imenu upravljavca, ta sodeluje zgolj z obdelovalci, ki zagotovijo zadostna jamstva za izvedbo ustreznih tehničnih in organizacijskih ukrepov na tak način, da obdelava izpolnjuje zahteve iz te uredbe in zagotavlja varstvo pravic posameznika, na katerega se nanašajo osebni podatki.

2. Obdelovalec ne zaposli drugega obdelovalca brez predhodnega posebnega ali splošnega pisnega dovoljenja upravljavca. V primeru splošnega pisnega dovoljenja obdelovalec upravljavca obvesti o vseh nameravanih spremembah glede zaposlitve dodatnih obdelovalcev ali njihove zamenjave, s čimer se upravljavcu omogoči, da nasprotuje tem spremembam.

3. Obdelavo s strani obdelovalca ureja pogodba ali drug pravni akt v skladu s pravom Unije ali pravom države članice, ki določa obveznosti obdelovalca do upravljavca, v katerem so določeni vsebina in trajanje obdelave, narava in namen obdelave, vrsta osebnih podatkov, kategorije posameznikov, na katere se nanašajo osebni podatki, ter obveznosti in pravice upravljavca. Ta pogodba ali drug pravni akt zlasti določa, da obdelovalec:

(a) osebne podatke obdeluje samo po dokumentiranih navodilih upravljavca, vključno glede prenosov osebnih podatkov v tretjo državo ali mednarodno organizacijo, razen če to od njega zahteva pravo Unije ali pravo države članice, ki velja za obdelovalca; v slednjem primeru obdelovalec o tej pravni zahtevi pred obdelavo podatkov obvesti upravljavca, razen če zadevno pravo prepoveduje takšno obvestilo na podlagi pomembnih razlogov v javnem interesu;

(b) zagotovi, da so osebe, ki so pooblaščene za obdelavo osebnih podatkov, zavezane k zaupnosti ali jih k zaupnosti zavezuje ustrezen zakon;

(c) sprejme vse ukrepe, potrebne v skladu s členom 32;

(d) spoštuje pogoje iz odstavkov 2 in 4 za zaposlitev drugega obdelovalca;

(e) ob upoštevanju narave obdelave pomaga upravljavcu z ustreznimi tehničnimi in organizacijskimi ukrepi, kolikor je to mogoče, pri izpolnjevanju njegovih obveznosti, da odgovori na zahteve za uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki, iz poglavja III;

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

(g) v skladu z odločitvijo upravljavca izbriše ali vrne vse osebne podatke upravljavcu po zaključku storitev v zvezi z obdelavo ter uniči obstoječe kopije, razen če pravo Unije ali pravo države članice predpisuje shranjevanje osebnih podatkov;

(h) da upravljavcu na voljo vse informacije, potrebne za dokazovanje izpolnjevanja obveznosti iz tega člena, ter upravljavcu ali drugemu revizorju, ki ga pooblasti upravljavec, omogoči izvajanje revizij, tudi pregledov, in pri njih sodeluje.

V zvezi s točko (h) prvega pododstavka obdelovalec nemudoma obvesti upravljavca, če po njegovem mnenju navodilo krši to uredbo ali druge določbe Unije ali predpisov držav članic o varstvu podatkov.

4. Kadar obdelovalec zadolži drugega obdelovalca za izvajanje specifičnih dejavnosti obdelave v

imenu upravljavca, za tega drugega obdelovalca na podlagi pogodbe ali drugega pravnega akta v skladu s pravom Unije ali pravom države članice veljajo enake obveznosti varstva podatkov, kot so določene v pogodbi ali drugem pravnem aktu med upravljavcem in obdelovalcem iz odstavka 3, zlasti za zagotovitev zadostnih jamstev za izvajanje ustreznih tehničnih in organizacijskih ukrepov na tak način, da bo obdelava izpolnjevala zahteve iz te uredbe. Kadar ta drugi obdelovalec ne izpolni obveznosti varstva podatkov, prvi obdelovalec še naprej v celoti odgovarja upravljavcu za izpolnjevanje obveznosti drugega obdelovalca.

5. Zavezanost k odobrenemu kodeksu ravnanja iz člena 40 ali izvajanje odobrenega mehanizma potrjevanja iz člena 42 s strani obdelovalca se lahko uporabi za dokazovanje zagotavljanja zadostnih jamstev iz odstavkov 1 in 4 tega člena.

6. Brez poseganja v individualno pogodbo med upravljavcem in obdelovalcem lahko pogodba ali drug pravni akt iz odstavkov 3 in 4 tega člena v celoti ali delno temelji na standardnih pogodbenih določilih iz odstavkov 7 in 8 tega člena, tudi ko so del potrdila, izdanega upravljavcu ali obdelovalcu v skladu s členoma 42 in 43.

7. Komisija lahko določi standardna pogodbena določila za zadeve iz odstavkov 3 in 4 tega člena ter v skladu s postopkom pregleda iz člena 93(2).

8. Nadzorni organ lahko sprejme standardna pogodbena določila za zadeve iz odstavkov 3 in 4 tega člena ter v skladu z mehanizmom za skladnost iz člena 63.

9. Pogodba ali drug pravni akt iz odstavkov 3 in 4 je v pisni obliki, vključno z elektronsko obliko.

10. Brez poseganja v člene 82, 83 in 84, če obdelovalec krši to uredbo s tem, ko določi namene in sredstva obdelave, se obdelovalec šteje za upravljavca v zvezi s to obdelavo.

Upravljavec osebnih podatkov torej lahko zaupa podatke obdelovalcem, ki zagotovijo zadostna jamstva za izvedbo ustreznih tehničnih in organizacijskih ukrepov.

Med elementi, ki bi jih morali upravljavci upoštevati pri ugotavljanju, ali gre za zadostna jamstva, so npr.:

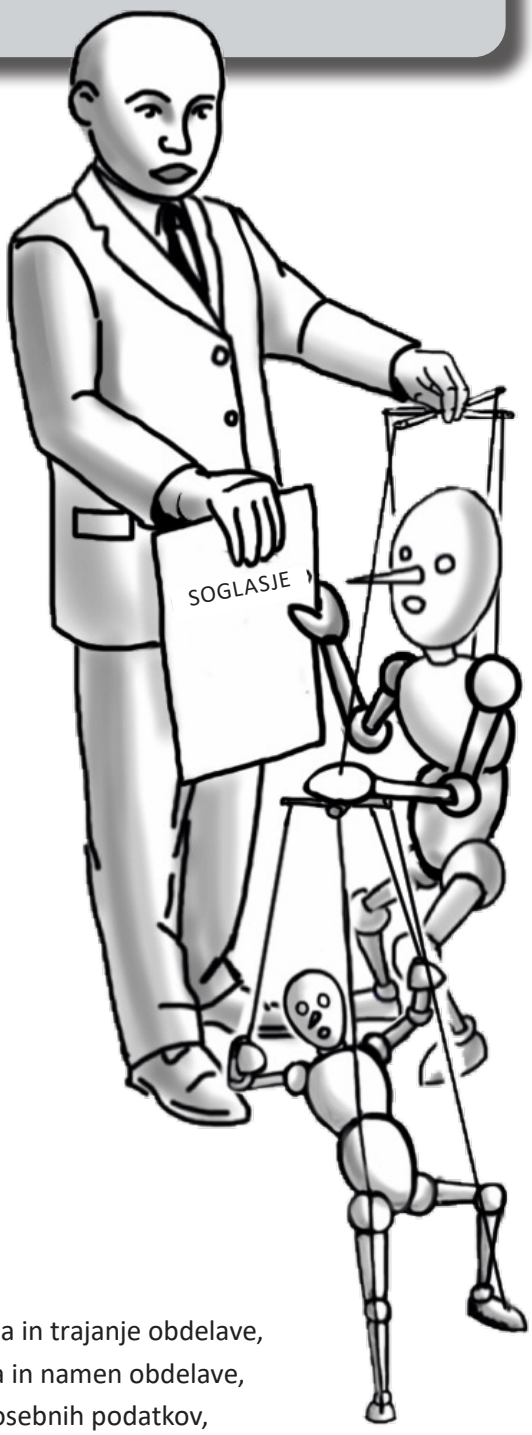
- reference obdelovalca,
- prisotnost in zaupanje, ki ga obdelovalec uživa na trgu,
- zagotavljanje ustreznih pogojev nudenja storitve.

Pogoj iz ZVOP-1, da se obdelava lahko poveri le tistemu subjektu, ki je registriran za opravljanje določene dejavnosti ni več relevanten.

2. odstavek 28. člena Splošne uredbe določa pomembne pogoje glede najemanja storitev podobdelovalcev.

PRIMER: KLUB ZVESTOBE

Trgovec najema IT podjetje za vzdrževanje kluba zvestobe, IT podjetje pa podatkov iz kluba zvestobe ne hrani na svojih strežnikih, temveč naprej najema storitve pri ponudniku gostovanja. Pri obsežnih obdelavah se lahko »veriži« tudi več deset obdelovalcev in njihovih podobdelovalcev.



Upravljavec namreč **mora ohraniti nadzor** nad subjekti, ki imajo stik z osebnimi podatki iz zbirk upravljavca – veriženje obdelave lahko pomeni izgubo nadzora in kateri koli subjekt v verigi lahko zagreši zlorabo osebnih podatkov. Zato je ključnega pomena, da lahko upravljavec odloča, s katerimi obdelovalci bo sodeloval in katere podobdelovalce bo dopuščal. Splošna uredba zato določa, da obdelovalec **ne sme zaposliti drugega obdelovalca brez predhodnega posebnega ali splošnega pisnega dovoljenja upravljavca**. Posebno soglasje se nanaša na vsakega podobdelovalca, splošno soglasje pa lahko upravljavec izda obdelovalcu, ki mu dovolj zaupa, da bo najemal le zaupanja vredne podobdelovalce in z njimi skladno s Splošno uredbo ustrezno uredil medsebojno pogodbeno razmerje. V primeru splošnega pisnega dovoljenja mora obdelovalec upravljavca obvestiti o vseh nameravanih spremembah glede zaposlitve dodatnih obdelovalcev ali njihove zamenjave, s čimer se upravljavcu omogoči, da nasprotuje tem spremembam. Upravljavec mogoče ne želi pristati na to, da bi podobdelovalec osebne podatke prenašal v tretje države, ne uživa zaupanja upravljavca ali obstaja kakšen tretji razlog, da upravljavec ne dovoli uporabe storitev določenega podobdelovalca.

Pravice in obveznosti morata upravljavec osebnih podatkov in njegov pogodbeni sodelavec urediti s pisno pogodbo ali drugim pravnim aktom (npr. dogovor, sporazum) – obličnost pravnega akta ni predpisana, vendar pa Splošna uredba predpisuje, da mora določati obveznosti obdelovalca do upravljavca, v katerem so določeni:

- vsebina in trajanje obdelave,
- narava in namen obdelave,
- vrste osebnih podatkov,
- kategorije posameznikov, na katere se nanašajo osebni podatki ter
- obveznosti in pravice upravljavca.

Pogodba ali drug pravni akt nadalje določa, katere sestavine so obvezne v točkah a) do h), ki jih pojasnjujemo **v naslednji tabeli**:

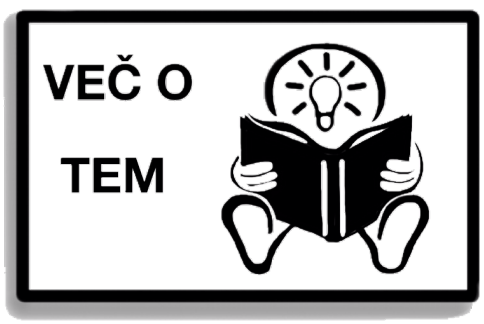
Obvezna sestavina	Kratko pojasnilo
(a) osebne podatke obdeluje samo po dokumentiranih navodilih upravljavca, vključno glede prenosov osebnih podatkov v tretjo državo ali mednarodno organizacijo, razen če to od njega zahteva pravo Unije ali pravo države članice, ki velja za obdelovalca; v slednjem primeru obdelovalec o tej pravni zahtevi pred obdelavo podatkov obvesti upravljavca, razen če zadevno pravo prepoveduje takšno obvestilo na podlagi pomembnih razlogov v javnem interesu;	Obdelovalec se mora držati navodil upravljavca glede obdelave osebnih podatkov, navodila pa lahko vključujejo dopustna in nedopustna ravnanja z osebnimi podatki, podrobneje opredeljene postopke, načine varovanja podatkov itd.
(b) zagotovi, da so osebe, ki so pooblaščene za obdelavo osebnih podatkov, zavezane k zaupnosti ali jih k zaupnosti zavezuje ustrezen zakon;	Upoštevaje načelo vgrajenega varstva osebnih podatkov (25. člen Splošne uredbe) bi moral obdelovalec osebne podatke dati na voljo samo tistim zaposlenim, ki jih dejansko potrebujejo za izvajanje nalog, za katere je obdelovalca najel upravljavec. Dobra praksa je, da so zaposleni pri obdelovalcu seznanjeni z varnostnimi postopki in ukrepi, ter da glede varovanja zaupnosti podatkov, s katerimi se seznanijo, podpišejo ustrezno izjavo.
(c) sprejme vse ukrepe, potrebne v skladu s členom 32;	Obdelovalec mora za osebne podatke, ki so mu bili zaupani v obdelavo, zagotoviti ustrezno tehnične in organizacijske ukrepe za njihovo varnost, t.j. zagotavljanje celovitosti, zaupnosti in razpoložljivosti osebnih podatkov (VEČ O VARNOSTI, glej spodaj).
(d) spoštuje pogoje iz odstavkov 2 in 4 za zaposlitev drugega obdelovalca;	Obdelovalec ne sme najemati podobdelovalcev brez posebnega ali splošnega soglasja upravljavca. Tovrstna klavzula mora biti sestavni del pogodbe o pogodbeni obdelavi.
(e) ob upoštevanju narave obdelave pomaga upravljavcu z ustreznimi tehničnimi in organizacijskimi ukrepi, kolikor je to mogoče, pri izpolnjevanju njegovih obveznosti, da odgovori na zahteve za uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki, iz poglavja III;	Glede na to, da se osebni podatki lahko nahajajo pri obdelovalcu in ne pri upravljavcu, bo moral zahtevo posameznika glede njegovih pravic (npr. zahtevo po seznanitvi s podatki, zahtevo po kopiji podatkov, popravku itd.) v ustreznem roku obravnavati obdelovalec, zato je primerno, da se ta postopek dogovori z upravljavcem. Primerno je tudi, da je obdelovalc seznanjen s tem, katere pravice lahko uveljavlja posameznik, da se pravočasno zaveda, katere aktivnosti lahko to terja od obdelovalca. Prav tako je v izogib kasnejšim nesporazumom priporočljivo jasno določiti odgovornosti obdelovalca za izvedbo posameznih nalog v zvezi z uveljavljanjem pravic posameznikov kot tudi vprašanja kritja stroškov v zvezi z izvajanjem teh nalog.

Obvezna sestavina	Kratko pojasnilo
(f) upravljavcu pomaga pri izpolnjevanju obveznosti iz členov 32 do 36 ob upoštevanju narave obdelave in informacij, ki so dostopne obdelovalcu;	Členi 32 do 36 določajo zahteve glede (informacijske) varnosti – tako upravljavec kot obdelovalec in njegovi podobdelovalci so dolžni zagotoviti ustrezne postopke in ukrepe za varnost podatkov (člen 32) oziroma ustrezno reagirati v primeru kršitev varnosti (člena 33 in 34). Obdelovalec bo v določenih primerih moral pomagati upravljavcu pri izvedbi ocene učinka (člena 35 in 36); VEČ O OCENAH UČINKA, glej spodaj..
(g) v skladu z odločitvijo upravljavca izbriše ali vrne vse osebne podatke upravljavcu po zaključku storitev v zvezi z obdelavo ter uniči obstoječe kopije, razen če pravo Unije ali pravo države članice predpisuje shranjevanje osebnih podatkov;	Po poteku pogodbe obdelovalec ne razpolaga več s pravno podlago za hrambo ali drugačno obdelavo osebnih podatkov (razen če to od njega zahteva zakonodaja, vendar se potem v tem delu šteje za upravljavca osebnih podatkov, ki jih še hrani), zato mora osebne podatke bodisi uničiti bodisi vrniti upravljavcu. Hramba podatkov brez vednost upravljavca po preteku pogodbe in brez druge pravne podlage pomeni kršitev.
(h) da upravljavcu na voljo vse informacije, potrebne za dokazovanje izpolnjevanja obveznosti iz tega člena, ter upravljavcu ali drugemu revizorju, ki ga pooblasti upravljavec, omogoči izvajanje revizij, tudi pregledov, in pri njih sodeluje.	Upravljavec mora nadzornemu organu izkazati skladnost ureditve pogodbene obdelave, zato bo včasih za to potreboval pojasnila, dokumentacijo in in druge informacije s strani obdelovalca. Upravljavec ima pravico do nadzora nad svojimi obdelovalci, nadzor pa lahko izvaja sam ali ga poveri tretjim osebam, ki jih zato ustrezno pooblastil (npr. revizorjem).

Posebej priporočamo, da v pogodbo upravljavec doda **tudi kontakte svoje pooblaščene osebe za varstvo osebnih podatkov** (ang. DPO), če jo je imenoval (v določenih primerih - kriteriji so isti kot za upravljavce - mora tudi obdelovalec imenovati pooblaščeno osebo z (37. člen Splošne uredbe); več o pooblaščenih osebah glej spodaj). Kontaktni podatek o pooblaščeni osebi sicer ni obvezen, vendar pa morajo biti obdelovalci s tem seznanjeni, saj morajo ta podatek voditi v svojih evidencah dejavnosti obdelave po 30. členu Splošne uredbe. Tako upravljavec kot obdelovalec sta dolžna voditi evidence dejavnosti obdelave po 30. členu Splošne uredbe.

V pomoč pri evidentiranju dejavnosti obdelave sta vzorca IP:

- Vzorec evidence dejavnosti obdelave za UPRAVLJAVCE (člen 30 Splošne uredbe),
- Vzorec evidence dejavnosti obdelave za OBDELOVALCE (člen 30 Splošne uredbe).



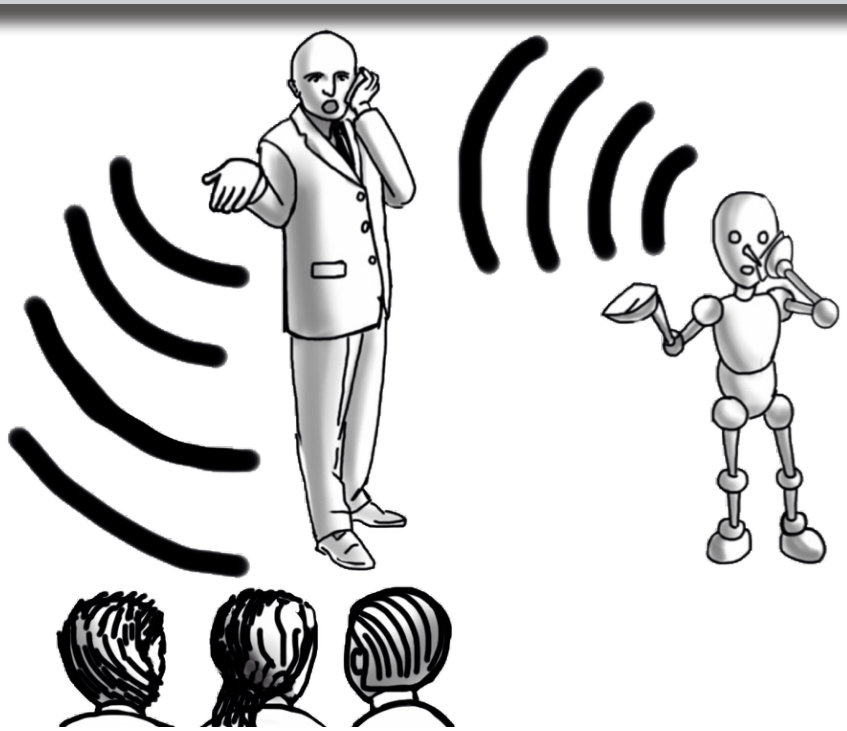
VEČ O VARNOSTI oz. zavarovanju osebnih podatkov si lahko preberete v smernicah informacijskega pooblaščenca Smernice o zavarovanju osebnih podatkov.

VEČ O OCENAH UČINKA najdete na podstrani IP:

VEČ O POOBLAŠČENIH OSEBAH za varstvo osebnih podatkov si lahko preberete na posebni podstrani IP.

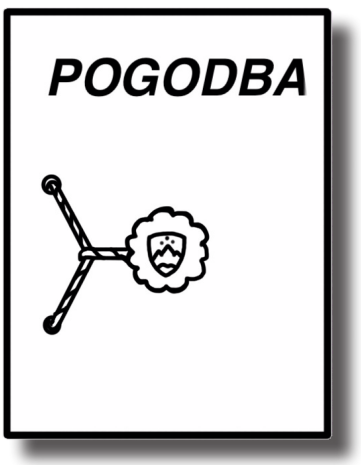
PRIMER: DOLŽNOSTI POGODBENEGA OBDELOVALCA V ZVEZI Z OBVEŠČANJEM POSAMEZNIKOV.
Oglaševalska agencija za naročnika izvaja raziskavo, pri kateri zbira osebne podatke mimoidočih pri trgovskem centru in informacije o njihovem zadovoljstvu z določenimi produkti. Zbrane podatke bo agencija analizirala in naročniku predlagala primerno akcijo. Kakšne so dolžnosti agencije pri obveščanju posameznikov, glede prijave zbirk osebnih podatkov, itd.?

V konkretnem primeru mora informacije o upravljavcu osebnih podatkov (naročniku) in namenu obdelave ter rokih hrambe podatkov posameznikom sporočiti agencija, ki zbira podatke neposredno od posameznikov.



Obstoječe **pogodbe po 11. členu ZVOP-1 je torej nujno treba dopolniti oz. skleniti nove** ali pa predpisane sestavite dogovoriti v aneksu k splošni pogodbi o uporabi storitev zunanjih izvajalcev. Dolžnost nadzora nad tem, ali so osebni podatki ustrezno varni, ima še vedno upravljavec osebnih podatkov. Osebne podatke lahko obdelovalec obdeluje le tako, kot je bilo dogovorjeno z upravljavcem osebnih podatkov in nikakor ne še za kak drug ali celo svoj lastni namen. Izjema so primeri, ko določeno obdelavo zahteva zakonodaja.

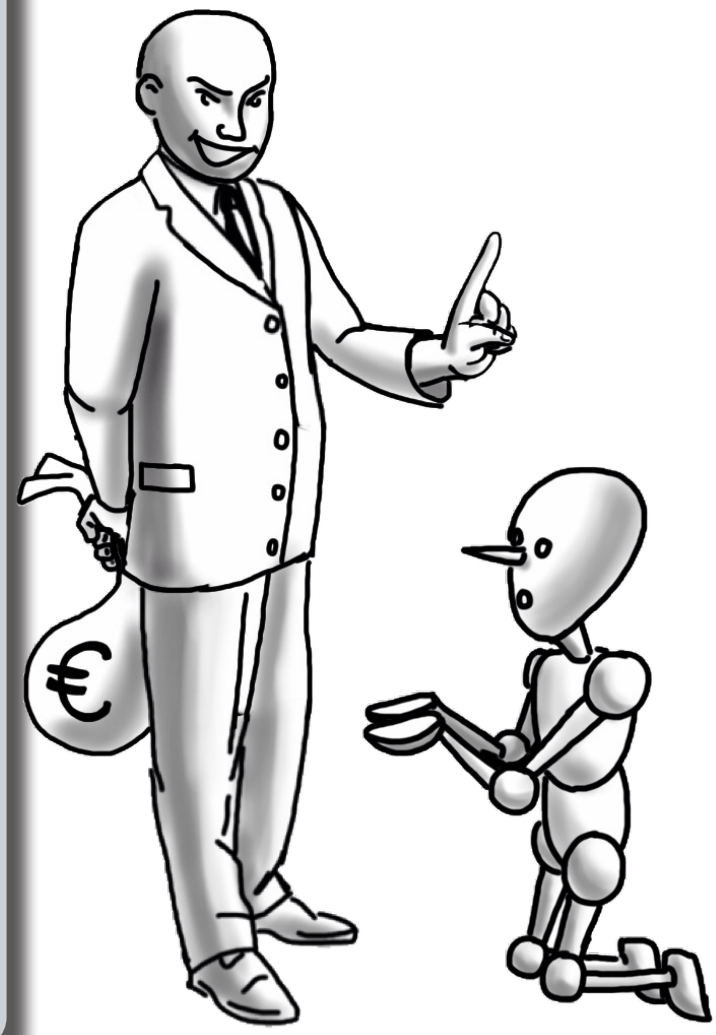
V primeru spora med upravljavcem osebnih podatkov in pogodbenim obdelovalcem mora slednji osebne podatke nemudoma vrniti upravljavcu, če ta tako zahteva in uničiti vse morebitne kopije, ki jih hrani pri sebi oz. jih mora predati organom pregona, sodišču ali drugemu pristojnemu državnemu organu, če tako določa zakon. Prav tako mora vse podatke vrniti upravljavcu obdelovalec, ki (statusno) preneha obstajati.



PRIMER: UPRAVLJAVEC NE PLAČUJE OBDELOVALCEV.

Obdelovalec za naročnika upravlja spletno mesto, kjer lahko posamezniki vodijo in delijo svoje podatke. Vzdrževanje in upravljanje spletnega mesta stane, naročnik pa storitve ne plačuje in pogodbenemu obdelovalcu dolguje veliko vsoto denarja. Pogodbenik zato razmišlja o ukinitvi baze osebnih podatkov oziroma prekinitvi dostopa naročnika do baze. Posameznike iz baze bi obvestil o tem, da bo baza izbrisana in s tem tudi njihovi osebni podatki, kljub temu, da jih naročnik o tem noče obvestiti in jim tako ponuditi možnost, da svoje podatke izvozijo in ohranijo.

Obdelovalec ne sme obdelovati osebnih podatkov, ki mu jih je v obdelavo zaupal upravljavec, za noben drug namen kakor za tistega, ki ga je določil upravljavec. Obveščanje uporabnikov o tem, da bo baza ukinjena, mimo volje upravljavca, je z vidika zahtev določb Splošne uredbe nedopustno, saj gre za obdelavo osebnih podatkov, ki presega osnovni namen. Podobno velja tudi za morebitno brisanje baze osebnih podatkov brez navodil s strani upravljavca. Podatke lahko le vrne upravljavcu. Pogodbeni upravljavec lahko uporabi institute, ki jih za izterjavo dolgov predvidevata civilno ali kaznovalno pravo (kazensko in prekrškovno).



V mnogih primerih se pojavljajo tudi vprašanja drugih **dolžnosti in obveznosti upravljavca oziroma obdelovalca** osebnih podatkov, še posebej, kadar obdelovalec po naročilu upravljavca zbira osebne podatke neposredno od posameznika in **ni povsem jasno, kdo mora denimo posameznika obvestiti o obdelavi osebnih podatkov in kdo izvajati pravice posameznikov.**

Splošna uredba v **13. členu** določa, katere informacije in dostop do osebnih podatkov je treba zagotoviti posamenziku, kadar se osebni podatki zberejo neposredno od njega[5]:

1. Kadar se osebni podatki v zvezi s posameznikom, na katerega se nanašajo osebni podatki, pridobijo od tega posameznika, upravljavec zadevnemu posamezniku takrat, ko pridobi osebne podatke, zagotovi vse naslednje informacije:

(a) | identiteto in kontaktne podatke upravljavca in njegovega predstavnika, kadar ta obstaja;

(b) | kontaktne podatke pooblaščene osebe za varstvo podatkov, kadar ta obstaja;

(c) | namene, za katere se osebni podatki obdelujejo, kakor tudi pravno podlago za njihovo obdelavo;

(d) | kadar obdelava temelji na točki (f) člena 6(1), zakonite interese, za uveljavljanje katerih si prizadeva upravljavec ali tretja oseba;

[5] *14. člen Splošne uredbe dalje določa, katere informacije je treba posredovati posamezniku, kadar osebni podatki niso bili pridobljeni od posameznika, na katerega se ti nanašajo.*

(e) | uporabnike ali kategorije uporabnikov osebnih podatkov, če obstajajo;

(f) | 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.

2. Poleg informacij iz odstavka 1 upravljavec takrat, ko pridobi osebne podatke posamezniku, na katerega se ti nanašajo, zagotovi naslednje dodatne informacije, ki so potrebne za zagotovitev poštene in pregledne obdelave:

(a) | obdobje hrambe osebnih podatkov ali, kadar to ni mogoče, merila, ki se uporabijo za določitev tega obdobja;

(b) | obstoj pravice, da se od upravljavca zahtevajo dostop do osebnih podatkov in popravek ali izbris osebnih podatkov ali omejitev obdelave v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali obstoj pravice do ugovora obdelavi in pravice do prenosljivosti podatkov;

(c) | kadar obdelava temelji na točki (a) člena 6(1) ali točki (a) člena 9(2), 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;

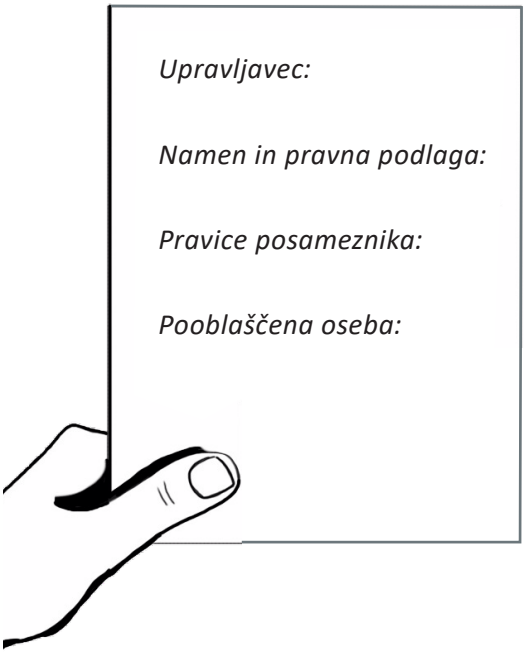
(d) | pravico do vložitve pritožbe pri nadzornem organu;

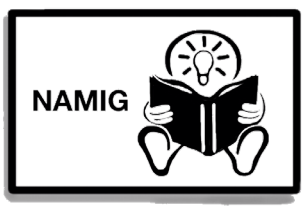
(e) | ali je zagotovitev osebnih podatkov statutarna ali pogodbena obveznost ali pa obveznost, ki je potrebna za sklenitev pogodbe, ter ali mora posameznik, na katerega se nanašajo osebni podatki, zagotoviti osebne podatke ter kakšne so morebitne posledice, če se taki podatki ne zagotovijo, in

(f) | 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.

3. Kadar namerava upravljavec nadalje obdelovati osebne podatke za namen, ki ni namen, za katerega so bili osebni podatki zbrani, upravljavec posamezniku, na katerega se nanašajo osebni podatki, pred tako nadaljnjo obdelavo podatkov zagotovi informacije o tem drugem namenu in vse nadaljnje relevantne informacije iz odstavka 2.

4. Odstavki 1, 2 in 3 se ne uporabljajo, kadar in kolikor posameznik, na katerega se nanašajo osebni podatki, že ima informacije.





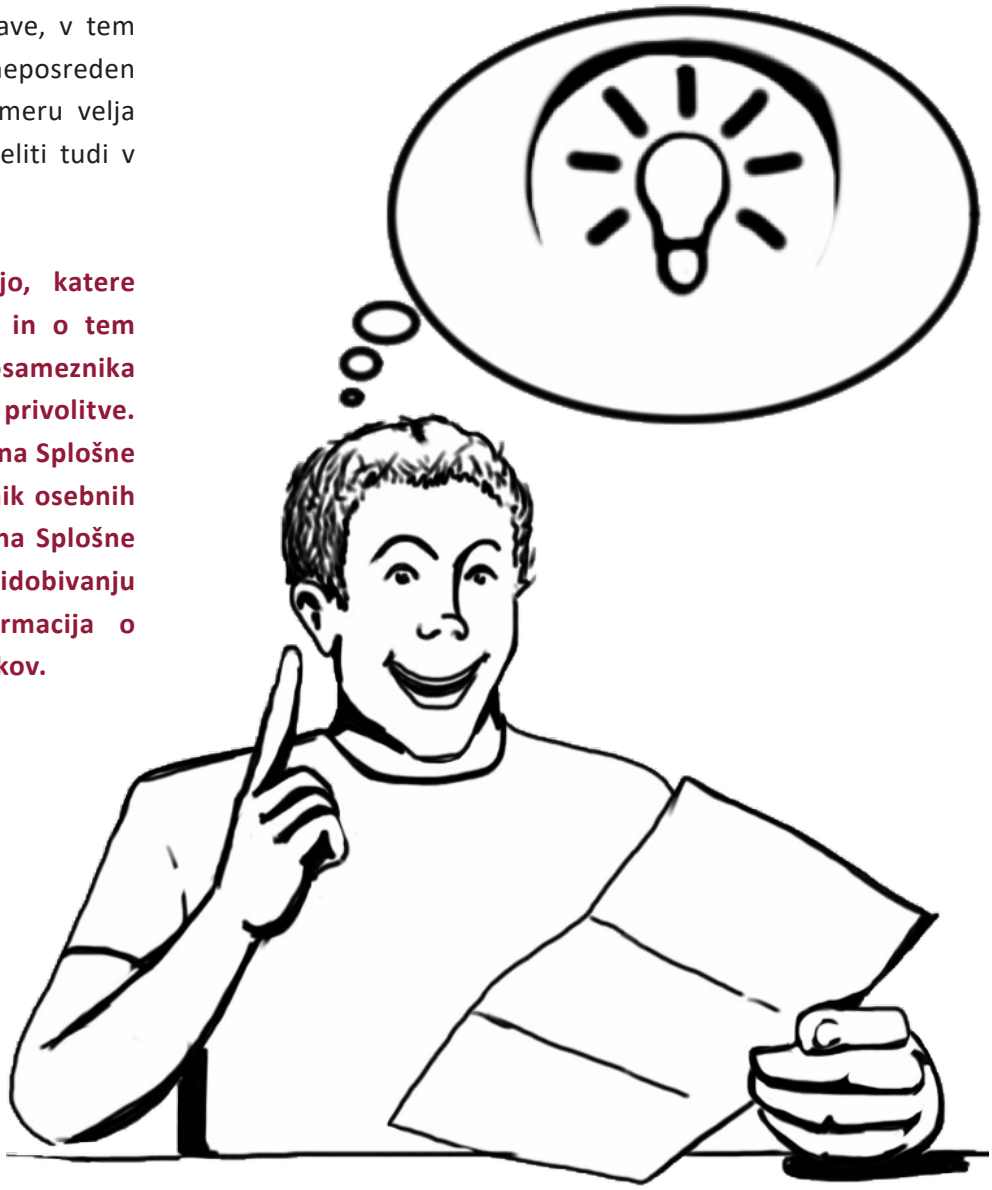
V pomoč upravljavcem pri informiranju posameznikov je lahko vzorec obvestila o obdelavi osebnih podatkov.

Informacije morajo biti jasne in razumljive, saj se bo posameznik, na katerega se podatki nanašajo, lahko le na podlagi takšnih informacij odločil o tem, ali bo za obdelavo osebnih podatkov podal svojo osebno privolitev oz., ali bo svoje osebne podatke sploh posredoval, v primeru drugih pravnih podlag pa je na ta način seznanjen, zakaj mora posredovati določene osebne podatke upravljavcu (npr. zaradi zahtev delovno-pravne zakonodaje).

Kot je razvidno iz navedenega, ima **dolžnost obveščanja posameznikov načeloma upravljavec osebnih podatkov**. Kadar zbiranje podatkov zaupa obdelovalcu, to ne spremeni dejstva, da morajo biti posamezniki obveščeni o upravljavcu osebnih podatkov in namenih obdelave, v tem primeru s strani pogodbenika, ki ima neposreden dostop do posameznikov. V tem primeru velja to nalogo obdelovalca izrecno opredeliti tudi v pogodbi z upravljavcem.

Upravljavci se lahko sami odločajo, katere konkretne obdelovalce bodo najeli in o tem praviloma ni treba seznanjati posameznika oziroma za to pridobivati njegove privolitve. Glede na določbo 8. in 9. točke 4. člena Splošne uredbe, je obdelovalec tudi uporabnik osebnih podatkov. Po določbi 13. in 14. člena Splošne uredbe pa se posamezniku pri pridobivanju osebnih podatkov posreduje informacija o uporabnikih ali kategorijah uporabnikov.

Tudi dolžnost izvajanja drugih pravic posameznikov (npr. pravica do vpogleda, izbrisa, popravka podatkov) je na strani upravljavca, ki mora zagotoviti (npr. s pogodbenimi določili), da mu bo obdelovalec omogočil izvajanje teh pravic tudi v primeru, da so podatki shranjeni le pri obdelovalcu, upravljavec pa potrebuje dostop do njih za namen izvrševanja pravic posameznika.



3.4 Varnost osebnih podatkov

32. člen Splošne uredbe določa, da morata **upravljavec in obdelovalec** z izvajanjem ustreznih **tehničnih in organizacijskih ukrepov** zagotoviti ustrezno raven varnosti glede na tveganje. Pri tem upoštevata:

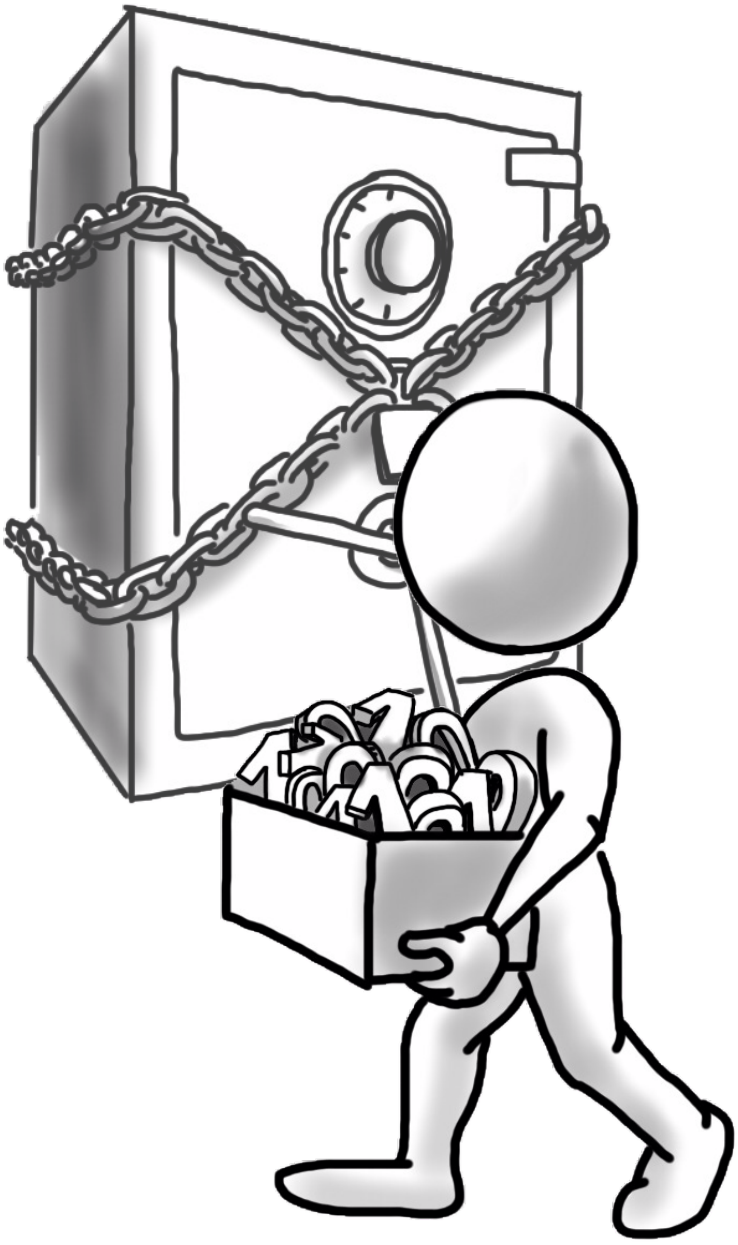
- stanje najnovejšega tehnološkega razvoja,
- stroške izvajanja,
- naravo,
- obseg,
- okoliščine,
- namene obdelave ter
- tveganj za pravice in svoboščine posameznikov.

Ob upoštevanju **tveganj**, ki se razlikujejo po verjetnosti in resnosti, zagotovita med drugim naslednje ukrepe[6], kot je ustrezno[7]:

d. psevdonimizacijo in šifriranje osebnih podatkov;
e. zmožnost zagotoviti stalno zaupnost, celovitost, dostopnost in odpornost sistemov in storitev za obdelavo;
f. zmožnost pravočasno povrniti razpoložljivost in dostop do osebnih podatkov v primeru fizičnega ali tehničnega incidenta;
g. postopek rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave.

Pri določanju ustrezne ravni varnosti se upoštevajo **zlasti tveganja**, ki jih pomeni obdelava, zlasti zaradi nenamernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

Upravljavec in obdelovalec zagotovita, da katera koli fizična oseba, ki ukrepa pod vodstvom upravljavca ali obdelovalca, ki ima dostop do osebnih podatkov, slednjih ne sme obdelati brez navodil upravljavca, razen če to od nje zahteva pravo Unije ali pravo države članice.



[6] 3. odstavek 32. člena Splošne uredbe določa, da se lahko zavezanost k odobrenemu kodeksu ravnanja iz člena 40 ali izvajanje odobrenega mehanizma potrjevanja iz člena 42 uporabi za dokazovanje izpolnjevanja zahtev iz odstavka 1 tega člena.

[7] »Kot je ustrezno« je treba razumeti tako, da se upoštevajo konkretne okoliščine in ne, da so vsi našteti ukrepi vedno obvezni. Primerno je npr. šifrirati prenosne nosilce podatkov, saj se lažje izgubijo oz. odtujijo, šifriranje vseh podatkov organizaciji pa bi bilo precej zahtevno.

Do sprejma ZVOP-2 veljajo tudi določbe ZVOP-1 glede zavarovanja (t.j. varnosti) osebnih podatkov.

24. in 25. člen ZVOP-1 podrobneje določata zahteve za zavarovanje osebnih podatkov, ki obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava teh podatkov tako, da se:

1. varujejo prostori, oprema in sistemsko programska oprema, vključno z vhodno-izhodnimi enotami;

2. varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;

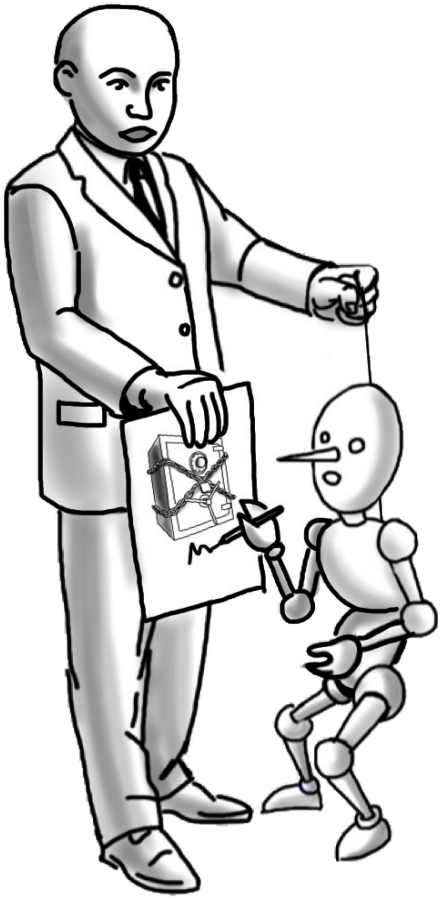
3. preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;

4. zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;

5. omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

3. odstavek 24. člena ZVOP-1 tudi določa, da morajo biti *postopki in ukrepi za zavarovanje*

Glede zavarovanja oz. varnosti priporočamo ***smernice IP o zavarovanju osebnih podatkov***, ki vsebujejo primere dobrih in slabih praks ter kontrolni seznam osnovnih varnostnih ukrepov za manjše upravljavce in obdelovalce.



osebnih podatkov **ustrezni glede na tveganje,** *ki ga predstavlja obdelava in narava določenih osebnih podatkov, ki se obdelujejo*.

Glede pisne pogodbe med upravljavcem osebnih podatkov in obdelovalcem osebnih podatkov je treba opozoriti, da pogodbe, v katerih je določeno zgolj to, *da bo izvajalec vse podatke, pridobljene s strani naročnika varoval v skladu z Zakonom o varstvu osebnih podatkov, Splošno uredbo ali v skladu s kakšnim drugim zakonom oz. jih bo varoval kot poslovno skrivnost*, **ne zadostijo zahtevam določb iz 28. člena Splošne uredbe**.

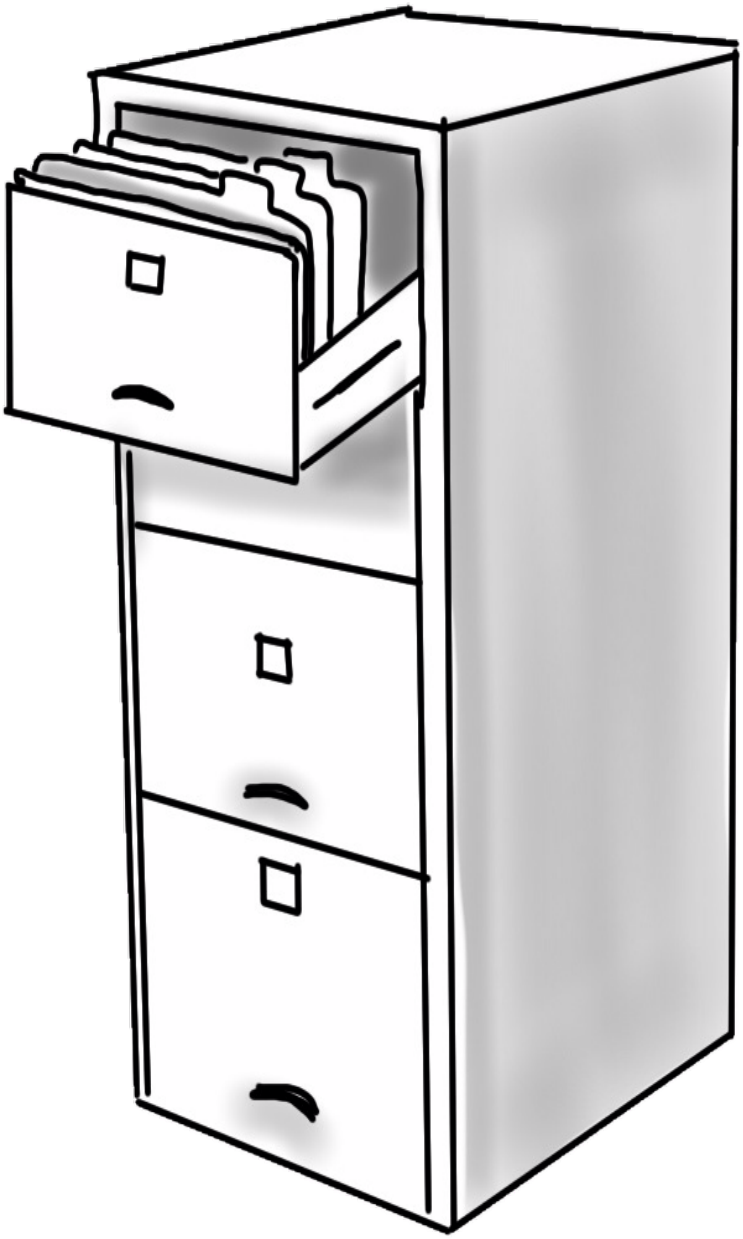
V pogodbah mora biti **jasno in konkretno določeno, s kakšnimi postopki in ukrepi** bo obdelovalec dosegel zasledovane varnostne cilje, npr.:

- s politiko dodeljevanja, uporabe in spreminjanja gesel,
- z zaklepanjem prostorov, pisarne, predalov, omar itd. izven delovnega časa,
- z rednim posodabljanjem programske in sistemske opreme itd.

Kadar ima bodisi upravljavec osebnih podatkov bodisi obdelovalec ustrezne organizacijske, tehnične in logično tehnične postopke in ukrepe za varnost osebnih podatkov **že predpisane v svojem NOTRANJEM AKTU**, lahko namesto ponovnega opisovanja vseh postopkov in ukrepov, v pogodbi zgolj citira ta akt in navede, da je ta akt sestavni del te pogodbe ter da mora obdelovalec zagotoviti varnost osebnih podatkov v skladu z določbami takšnega akta, ki ga je treba priložiti k pogodbi. V teh primerih je treba poskrbeti, da se **s tem aktom seznanijo** vsi tisti zaposleni pri upravljavcu osebnih podatkov ter pri obdelovalcu, ki odgovarjajo za izvajanje dogovorjenih postopkov in ukrepov ter tiste osebe, ki zaradi narave svojega dela pri upravljavcu osebnih podatkov oz. pri obdelovalcu obdelujejo določene osebne podatke.

Poleg določitve postopkov in ukrepov za varnost osebnih podatkov mora biti v pogodbi ali aneksu k pogodbi določeno tudi, **na kakšen način bo upravljavec osebnih podatkov pri obdelovalcu nadzoroval izvajanje dogovorjenih postopkov in ukrepov za zavarovanje osebnih podatkov**, ter katere osebe, ki so zaposlene pri upravljavcu osebnih podatkov, bodo opravljale takšen nadzor. V pogodbi ali aneksu bo moralo biti tudi določeno, katere osebe, ki so zaposlene pri upravljavcu osebnih podatkov oz. pri obdelovalcu, lahko opravljajo posamezna opravila v zvezi z obdelavo osebnih podatkov, kakšna so njihova pooblastila v zvezi s tem ter dolžnost varovanja zaupnosti podatkov. Določeno mora biti tudi, da je nadaljnje posredovanje osebnih podatkov, pridobljenih v okviru pogodbene obdelave, tretjim osebam mogoče le z dovoljenjem upravljavca osebnih podatkov.

Posebej opozarjamo, da glede na ugotovitve inšpekcijskih nadzorov upravljavci pogosto spregledajo svoje dolžnosti glede **revidiranja ravnanja svojih obdelovalcev**, zaradi česar se povečuje verjetnost za kršitve, zato priporočamo, da upravljavci redno, najmanj pa na letni



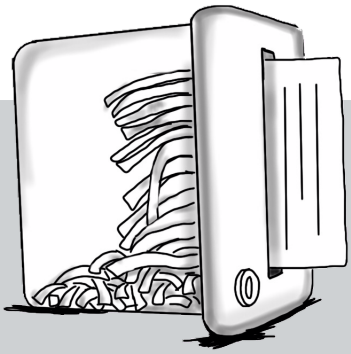
ravni preverjajo ustreznost ravnanja svojih obdelovalcev glede na pogodbena določila[8].

[8] Nadzor je lahko tudi bolj pogost, ni pa nujno, da je vsakič celovit, temveč je lahko posamezen nadzor usmerjen na različne vidike varnosti – rednost nadzora je pomembna predvsem z vidika ozaveščenosti tako upravljavca kot obdelovalcev.

PRIMER: KDO JE ODGOVOREN ZA KRŠITVE?

Podjetje A najame zunanjega izvajalca videonadzora za namen varovanja premoženja. Z izvajalcem sklene tipsko pogodbo, ki jo ta ponudi in je z vidika 28. člena Splošne uredbe pomanjkljiva, saj postopke in ukrepe za varnost določa le z dikcijo, da bo izvajalec podatke varoval v skladu s Splošno uredbo. Kasneje se izkaže, da zaposleni pri izvajalcu dostopajo do videonadzornih posnetkov tudi za zasebne in nezakonite namene, da npr. preverijo, kdaj se je določena oseba nahajala pred stavbo podjetja. Kdo je v tem primeru odgovoren za kršitve? Podjetje ali zunanji izvajalec videonadzora?

Ker podjetje z zunanjim izvajalecem ni sklenilo ustrezne pogodbe o pogodbeni obdelavi, v kateri bi jasno opredelilo meje pooblastila izvajalca ter ukrepe za varnost, s katerimi bi se preprečila nezakonita obdelava osebnih podatkov na posnetkih videonadzornega sistema in ukrepov za varnost tudi ni nadzorovalo, je odgovornost za kršitve na strani Podjetja A, lahko pa je kaznovan tudi zunanji izvajalec in posamezniki pri zunanjem izvajalcu, ki so kršili Splošno uredbo (nezakonita obdelava osebnih podatkov ali obdelava osebnih podatkov za druge namene). V primeru, da bi svoj pogodbeni odnos z izvajalcem primerno uredilo ter tudi nadzorovalo izvajanje ustreznih ukrepov za varnost, pa bi odgovornost nosil pogodbeni izvajalec videonadzora, saj bi prekoračil pooblastila iz pogodbe oz. podatkov ne bi zavaroval skladno s Splošno uredbo.



PRIMER: UNIČENJE DOKUMENTACIJE Z OSEBNIMI PODATKI.

Organ iz javnega sektorja je najel zunanjega izvajalca za uničenje dokumentacije, pri tem pa z njim ni sklenil pogodbe o pogodbeni obdelavi osebnih podatkov. Zunanji izvajalec je pri prevozu dokumentacijo slabo fizično zavaroval in ta se je iz prevoznega sredstva stresala na avtocesto. Kdo je odgovoren za nezakonito razkritje dokumentacije nepooblaščenim?

Ker organ s pogodbo zunanjemu izvajalcu ni predpisal ustreznih ukrepov za varnost osebnih podatkov, ki so bili namenjeni na uničenje, kamor sodi primarno tudi seznanitev izvajalca z dejstvom, da gre za prevoz varovanih osebnih podatkov, odgovornost za nezakonito razkritje nosi sam. Če je bil s tem dejstvom seznanjen, je kljub odsotnosti pogodbe o pogodbeni obdelavi, lahko odgovoren tudi prevoznik, saj mora kot pogodbeni obdelovalec izvajati postopke in ukrepe za varnost osebnih podatkov ne glede na to, ali je pogodba sklenjena in ustrezna ali ne. Tudi prenos osebnih podatkov namreč sodi med obdelavo osebnih podatkov.

3.5 Pogodbena obdelava v javnem sektorju

Tudi v javnem sektorju mora biti pogodbena obdelava osebnih podatkov skladna z 28. členom Splošne uredbe. Ključno je, da je med organom javnega sektorja in pogodbenim partnerjem sklenjena ustrezna **pisna pogodba** v smislu 28. člena Splošne uredbe, ki vsebuje vse predpisane vsebine, ali enakovredni **pisni dogovor oziroma sporazum**.

PRIMER: POGODBENA OBDELAVA V JAVNEM SEKTORJU.
Organ iz javnega sektorja je na podlagi svoje področne zakonodaje sklenil s posameznikom dogovor o pripravi mnenja o vzpostavitvi določene informacijske rešitve. Posameznik pa nato ni zgolj pripravil mnenja o vzpostavitvi informacijske rešitve, temveč je v okviru vzpostavljene informacijske rešitve tudi dejansko izvajal obdelavo osebnih podatkov, ne da bi bil glede tega sklenjen ustrezen dogovor v smislu pogodbene obdelave osebnih podatkov.

Ker gre v tem primeru dejansko za pogodbeno obdelavo osebnih podatkov, bi lahko posameznik na podlagi pooblastila organa izvajal le tisto obdelavo osebnih podatkov, ki bi jo opredeljeval ustrezen dogovor z vsemi bistvenimi sestavinami, ki jih za pogodbeno obdelavo osebnih podatkov določa 28. člen Splošne uredbe.

V javnem sektorju je predvsem pomembno tudi, da mora za določen namen obdelave osebnih podatkov obstajati pravna podlaga v zakonu (6.c člen Splošne uredbe), oz. je obdelava potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe (6.b člen Splošne uredbe) ali pa mora biti obdelava potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu (6.e člen Splošne uredbe). Če upravljavec osebnih podatkov nima ene od naštetih podlag, da za določen namen obdeluje osebne podatke, jih prav tako ne sme za tak namen posredovati v obdelavo pogodbenemu partnerju, misleč, da pravno podlago za obdelavo predstavlja pogodba v smislu 28. člena Splošne uredbe. Za določen namen obdelave mora najprej s pravno podlago razpolagati upravljavec – šele potem lahko obdelavo zaupa pogodbenem partnerju.

PRIMER: POSREDOVANJE OSEBNIH PODATKOV IZTERJEVALCU DOLGOV.
Občina želi najeti pogodbenega obdelovalca za izterjavo terjatev iz naslova najemnin in drugih naslovov. Ali mu sme posredovati osebne podatke, potrebne za ta namen?

Občina kot del javnega sektorja na podlagi 28. člena Splošne uredbe lahko posreduje osebne podatke pogodbenemu izterjevalcu dolga, ki to dejavnost opravlja zakonito. Pri določanju obsega posredovanih osebnih podatkov pa jo veže načelo sorazmernosti – posredovati sme le tiste osebne podatke, ki so ustrezni in po obsegu primerni glede na namen izterjave dolga, izterjevalec pa osebnih podatkov ne sme uporabljati za druge namene.

V določenih primerih **zakon predstavlja tudi neposredno podlago** za izvajanje nalog, ki vključujejo pogodbeno obdelavo osebnih podatkov, kot. npr. na področju zagotavljanja storitev centralnega informacijsko komunikacijskega sistema in elektronskega poslovanja državnih organov, javnih agencij, organov lokalnih skupnosti in nosilcev javnih pooblastil, kjer Zakon o državni upravi (Uradni list RS, št. 113/05, s spremembami in dopolnitvami) v 74.a členu to dolžnost nalaga ministrstvu, pristojnemu za javno upravo, ki za vse omenjene subjekte iz javnega sektorja zagotavlja izvajanje informacijskega sistema in s tem povezano obdelavo osebnih podatkov. Pri tem je treba opozoriti, da pravna podlaga v zakonu še ne pomeni, da je subjekt hkrati upravljavec osebnih podatkov in je treba upoštevati, ali nudi storitve v imenu in za račun drugih subjektov ter da morajo kljub zakonski podlagi za obdelavo biti sklenjeni ustrezni dogovori, saj zakon kot tak ne določa vseh podrobnosti, kot jih terja 28. člen Splošne uredbe.

4. Pogosta vprašanja iz prakse

4.1 Gre za prenos osebnih podatkov k drugemu upravljavcu ali prenos k pogodbenemu obdelovalcu?

V praksi pogosto ni enostavno odgovoriti na vprašanje, ali gre pri določenem posredovanju osebnih podatkov za prenos k obdelovalcu ali pa je organizacija, ki prejme osebne podatke, dejansko upravljavec osebnih podatkov. Take situacije se zlasti pojavljajo v primerih **povezanih družb**, kjer določene naloge v zvezi z obdelavo osebnih podatkov izvajajo za celotno skupino le določene družbe ali družba mati, pa tudi v primerih uporabe sodobnih komunikacijskih platform in storitev, kjer ponudnik take storitve zbrane podatke obdeluje tudi za lastne namene (npr. izboljšavo svojih storitev, neposredno trženje).

Prav tako gre lahko za situacijo, ko lahko govorimo o **skupnih upravljavcih v smislu 26. člena Splošne uredbe**, gre pa za situacije, ko dva ali več upravljavcev skupaj določijo namene in načine obdelave.

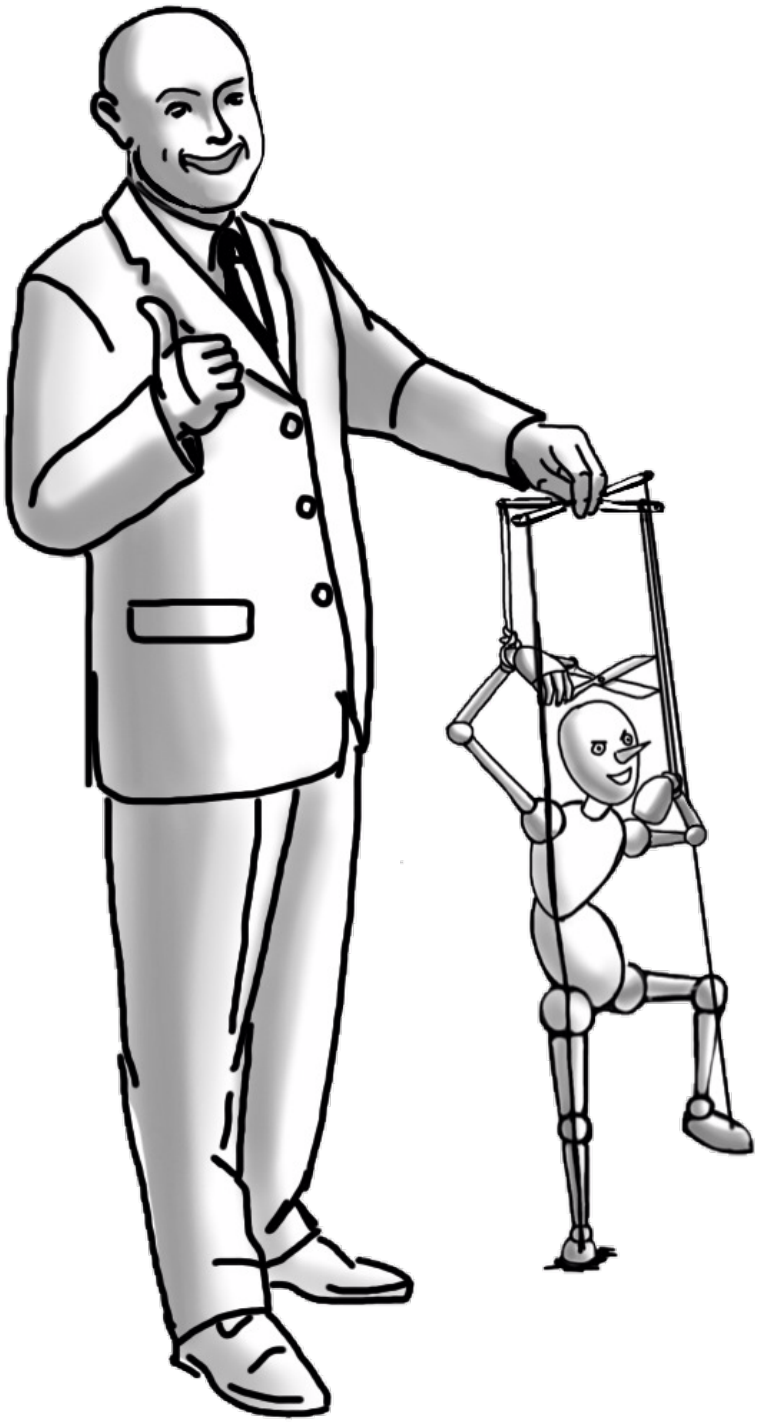
Kot pojasnjeno zgoraj, se **vlogi upravljavca in pogodbenega obdelovalca bistveno razlikujeta**. Upravljavec osebnih podatkov sam ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov, medtem ko je **obdelovalec vezan zgolj na navodila upravljavca** in osebnih podatkov nikakor ne sme obdelovati za noben svoj namen. Obdelovalec pravzaprav le izvaja določene

naloge, ki bi jih drugače izvajal upravljavec osebnih podatkov, pa se je ta odločil, da za to pooblasti pogodbenega partnerja. Upravljavec je prav tako tisti, ki nosi druge dolžnosti in odgovornosti iz Splošne uredbe (npr. izvajanje posameznikovih pravic do vpogleda, izbrisa osebnih podatkov). Prav tako upravljavec, kljub temu, da je podatke zaupal v obdelavo pogodbenemu partnerju, še vedno nosi odgovornost, da s pogodbo uredi primerne ukrepe za varnost osebnih podatkov ter da izvajanje teh ukrepov nadzoruje.

Posamezen subjekt je seveda lahko tako v vlogi obdelovalca kot v vlogi upravljavca, seveda pa načeloma ne za iste podatke: *kadrovska agencija npr. dela po pogodbi za svoje naročnike kot obdelovalec, obenem pa vodi lastne evidence podatkov kot upravljajvec*.

V praksi to pomeni, da mora upravljavec pred prenosom osebnih podatkov razmisliti, **za kakšne namene** se bodo podatki pri pogodbenemu partnerju ali povezani družbi obdelovali. Če bo druga organizacija le izvedla določeno nalogo, ki bi jo drugače izvedel upravljavec sam, potem gre za pogodbeno obdelavo. Podobno velja, če druga organizacija ne bo osebnih podatkov obdelovala za noben drug namen, potem gre v takem primeru lahko za pogodbeno obdelavo, kot jo določa 28. člen Splošne uredbe in jo je treba primerno urediti s pogodbo.

Če pa bo druga organizacija podatke uporabljala **predvsem za svoje namene**, **izven pooblastila in namenov upravljavca osebnih podatkov**, potem v takem primeru oz. v tem delu ni primerno govoriti o pogodbeni obdelavi osebnih podatkov, temveč gre za prenos osebnih podatkov med upravljavci osebnih podatkov. Za prenos osebnih podatkov taki organizaciji (drugim upravljavcem) mora obstajati primerna pravna podlaga, npr. privolitev posameznikov ali katera izmed drugih pravnih podlag.



CENTRALNI KADROVSKI SISTEMI IN EVIDENCE.

V skupini povezanih družb bi radi obdelavo osebnih podatkov za obračun plač centralizirali, tako da bi eno od članic skupine pooblastili, da izvaja to nalogo za vse ostale članice. Poleg tega bi na ravni družbe matere radi obdelovali osebne podatke zaposlenih, ki so potrebni za izvajanje sistema nagrajevanj in napredovanj. Ali mora upravljavec – članica skupine pridobiti soglasja svojih zaposlenih za posredovanje njihovih osebnih podatkov družbi materi in drugi članici, ki bo izvajala obračune plač?

Pogodbena obdelava osebnih podatkov je za opisano situacijo primeren institut v primeru, da družba mati oziroma članica, ki naj bi izvajala naloge v povezavi z obračunom plač, dejansko pridobljenih podatkov ne bosta uporabljali za nobene svoje namene, izven dogovorjenih z upravljavcem osebnih podatkov. V tem primeru pravne podlage za prenos osebnih podatkov ni treba iskati v 6. oz. 9. členu Splošne uredbe oz. v 9. členu ZVOP-1, pač pa mora biti sklenjena ustrezna pogodba o pogodbeni obdelavi.

Če pa bi šlo pri prenosu osebnih podatkov k družbi materi oz. kaki drugi članici skupine za širši obseg nalog in pooblastil, tudi takih, ki jih sam upravljavec osebnih podatkov ne bi mogel izvajati, pač pa jih **na ravni celotne skupine** izvaja npr. družba mati, potem je težko govoriti o pogodbeni obdelavi osebnih podatkov, saj gre dejansko za prenos podatkov k drugemu upravljavcu, za kar mora obstajati **primerna pravna podlaga.** V primeru povezanih družb je to za posredovanje podatkov znotraj povezane družbe lahko zakoniti interes (točka f člena 6(1) v povezavi z uvodno določbo 48).

UPORABA OSEBNIH PODATKOV ZA IZBOLJAŠAVE STORITEV IN POSREDOVANJE OSEBNIH PODATKOV TRETJIM STRANKAM.

Ponudnik priljubljenega sistema e-pošte in pisarniških aplikacij svojim strankam-organizacijam ponuja tipske pogodbe. V pogojih uporabe svojih storitev navaja, da podatke končnih uporabnikov analizira tudi za namen izboljšave svojih storitev in jih lahko deli s tretjimi strankami. Nikjer ne opredeljuje, da po prekinitvi sodelovanja podatke vrne oz. jih iz svojih sistemov izbriše. Ali gre tu za pogodbeno obdelavo osebnih podatkov?

Glede na to, da ponudnik osebne podatke obdeluje tudi za svoje lastne namene (za izboljšavo svojih storitev, posredovanje tretjim osebam) je težko trditi, da osebne podatke obdeluje le v okviru naročila in pooblastila upravljavca osebnih podatkov. Poleg tega pogodba ne daje nikakršnih zagotovil glede vrnitve ali izbrisa osebnih podatkov po koncu obdelave. Za posredovanje osebnih podatkov ponudniku je tako potrebna pravna podlaga, najbolj običajno privolitev posameznikov (pri čemer morajo imeti v primeru uporabe sistema v okviru podjetja, zaposleni možnost takšno privolitev odkloniti). Druga možnost je 48. člen ZDR-1, če gre za obdelavo v okviru delovnega razmerja, a le če je taka obdelava osebnih podatkov potrebna zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem.

4.2 Naš pogodbeni parter je iz tujine. Kakšne omejitve moramo upoštevati pri čezmejni pogodbeni obdelavi osebnih podatkov?

Pogosto se pogodbeni partnerji nahajajo v tujini, bodisi **v EU**, bodisi **v tretjih državah**, kjer veljajo drugačni predpisi glede zagotavljanja ustrezne ravni varstva osebnih podatkov. Zakonodaja s področja varstva osebnih podatkov v Evropi je osredotočena na obveznosti, ki jih ima pri ravnanju z osebnimi podatki upravljavec osebnih podatkov. Ta mora primarno upoštevati svojo nacionalno zakonodajo - v Sloveniji torej Zakon o varstvu osebnih podatkov, npr. upravljavec v Franciji pa zakonodajo Francije. Skladno s Splošno uredbo in s svojo domačo zakonodajo mora pripraviti pogodbena določila za pogodbeno obdelavo za vse pogodbene partnerje, katerim posreduje osebne podatke, pa naj bodo to npr. izvajalci računovodskih storitev, storitev strežniške hrambe, drugih storitev informacijske družbe. Prav tako morajo imeti upravljavci urejene pogodbene odnose s svojimi morebitnimi podružnicami oz. materinskimi družbami, če jim posredujejo v pogodbeno obdelavo osebne podatke, katerih upravljavci so (npr. podatke zaposlenih).

Obdelovalec pa je na drugi strani pri ravnanju z osebnimi podatki glede na evropsko zakonodajo primarno zavezan s pogodbenimi določili v pogodbi o obdelavi osebnih podatkov, ki jo sklene z upravljavcem. Poleg tega mora obdelovalec, ki je ustanovljen v državi članici EU, upoštevati nacionalno zakonodajo glede varnosti osebnih podatkov.

V primerih, ko v zvezi s pogodbeno obdelavo pride tudi do prenosa osebnih podatkov izven EU morajo upravljavci in obdelovalci za zakonit prenos osebnih podatkov v tretjo državo poleg pogodbe o obdelavi zagotoviti tudi enega izmed načinov zagotavljanja ustreznega varstva podatkov v tretji državi po prenosu, kakor to podrobneje ureja V. poglavje Splošne uredbe. Ena izmed možnosti za to je obstoj sklepa o ustreznosti, ki ga skladno s 45. členom Splošne uredbe lahko izda

Evropska komisija, če ugotovi da zadevna tretja država, ozemlje, eden ali več določenih sektorjev v tej tretji državi ali mednarodna organizacija zagotavlja ustrezno raven varstva podatkov. Druga možnost pa je predvsem uporaba zaščitnih ukrepov za zagotavljanje ustrezne ravni varstva po prenosu osebnih podatkov v tretjo državo na enega od drugih možnih načinov, kot jih določa člen 46 Splošne uredbe.

Zahteve s področja **iznosa osebnih podatkov v tretje države** podrobneje pojasnjujemo v smernicah, ki so na voljo na tukaj.

RAČUNALNIŠTVO V OBLAKU.

Izzive v smislu zakonsko skladnega izvajanja pogodbene obdelave osebnih podatkov predstavljajo tudi nove oblike izvajanja informacijskih storitev, ki so po naravi globalne in veliko bolj fluidne, kot to predvidevajo naši zakonski okvir, npr. računalništvo v oblaku, kjer gre običajno za pogodbeno obdelavo osebnih podatkov, obdelovalci in osebni podatki pa se nahajajo na (pogosto) neznanih lokacijah, prisotno je tudi veriženje obdelave (uporaba storitev podobdelovalcev). Prav tako je zapleteno izvrševanje dolžnosti upravljavca, da nadzoruje ustreznost varnosti osebnih podatkov pri ponudniku storitve v oblaku, ki je običajno velika multi-nacionalna družba.

Podrobnejše informacije glede zakonsko skladne uporabe računalništva v oblaku najdete **v smernicah Informacijskega pooblaščenca**.

4.3 Podatke želimo za določen namen posredovati pogodbenemu obdelovalcu. Ali moramo o tem obvestiti posameznike?

Običajno upravljavci niso obvezani, da pred posredovanjem osebnih podatkov obdelovalcem obveščajo posameznike oz. pridobivajo njihove privolitve. Obdelovalec namreč predstavlja zgolj nekakšno preslikavo ali **podaljšano roko upravljavca**, zanj in izključno zanj izvaja neko konkretno obdelavo osebnih podatkov, in to za namen, ki ga je določil upravljavec. Uporaba storitev zunanjih izvajalcev je v praksi zelo pogosta in številna podjetja uporabljajo širok nabor zunanjih izvajlcev – pretirano obveščanje posameznika o tem, kdaj in zakaj je bil najet določen zunanji izvajalec bi tudi za posameznika pomenilo pretirano zasipanje z informacijami, ki ne bi imelo bistvenega pomena za njegove pravice – te namreč vedno lahko zahteva in uveljavlja pred upravljavcem osebnih podatkov. Zato upravljavec praviloma **izven obveznosti po 13., 14. oz. 15. členu Splošne uredbe ni dolžan obveščati posameznikov**, če določena opravila v zvezi z obdelavo njihovih osebnih podatkov zaupa pogodbenemu partnerju, dokler ta delajo v imenu in za račun upravljavca. V določenih primerih pa je to smiselno zaradi izgradnje zaupanja do svojih strank – če npr. zavarovalnica uporablja klicni

center za oglaševanje svojih storitev ali izvajanje anket, je primerno, da agent v klicnem centru strankam pove, za katerega naročnika delajo.

4.4 Naša storitev zajema predvsem pogodbeno obdelavo osebnih podatkov za stranke. Na kaj moramo biti pozorni?

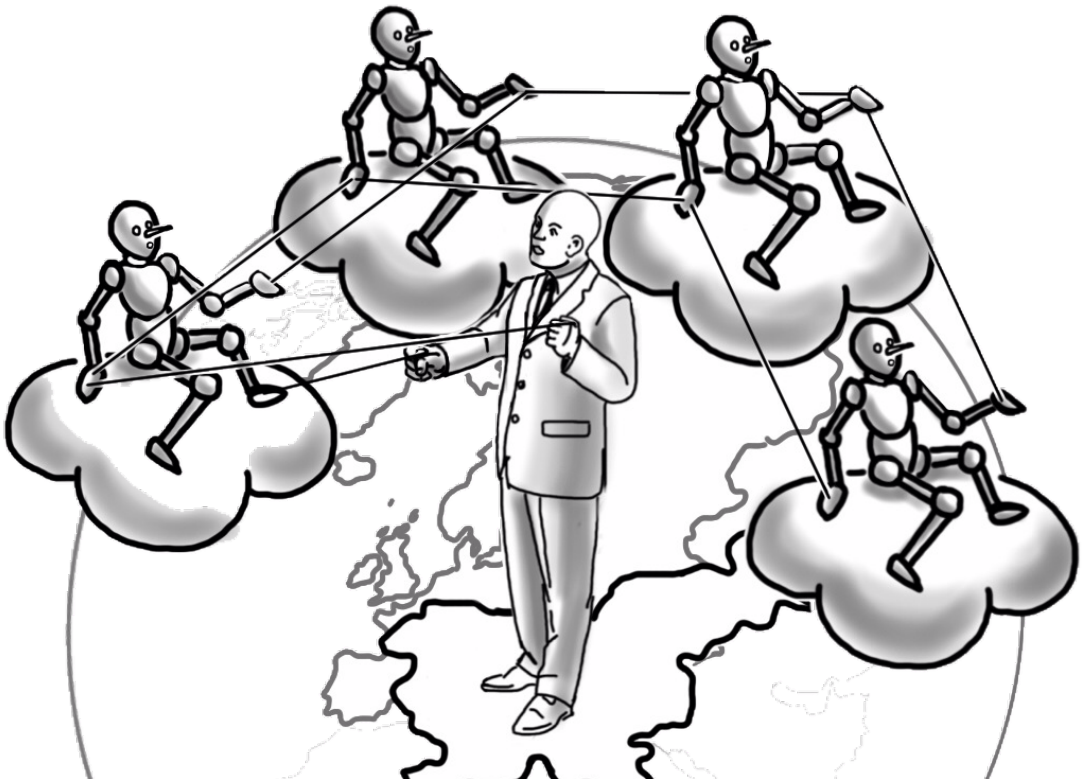
Pri organizacijah, ki predvsem izvajajo naloge po naročilu drugih organizacij (npr. revizorji, računovodje, hramba podatkov, itd.) se najprej pojavi dilema o tem, ali je organizacija obdelovalec osebnih podatkov, ali pa je morda upravljavec osebnih podatkov. Kot pojasnjeno zgoraj, je tu ključen razmislek o tem, **kdo določa namene** in **sredstva obdelave osebnih podatkov** ter ostali zgoraj navedeni **kriteriji**. Če namene in sredstva določa upravljavec osebnih podatkov, kot običajno v primeru najemanja storitev knjigovodstva in računovodstva, gre za izvajanje nalog v imenu, za račun in po navodilih naročnika (upravljavca) – zato bi izvajalca šteli za pogodbenega obdelovalca.

Pri organizacijah, ki večinoma opravljajo storitve po naročilu naročnika, se pogosto pojavi tudi dilema katero zakonodajo morajo upoštevati. Le svojo domačo ali tudi zakonodajo, ki zavezuje njene stranke. Po evropski zakonodaji je dolžnost glede ustreznega urejanja pogodbene obdelave

osebnih podatkov primarno na strani upravljavcev osebnih podatkov in ne na strani obdelovalca. Upravljavci osebnih podatkov morajo pri tem slediti tudi svoji nacionalni zakonodaji, ki jim predpisuje pravila glede posredovanja osebnih podatkov in torej morajo z obdelovalci skleniti pogodbe, ustrezne glede na svojo nacionalno zakonodajo. Dolžnost pogodbenega partnerja v Sloveniji pa je je upoštevanje pogodbenih določil (da npr. osebnih podatkov ne obdeluje izven pooblastil naročnika, itd.) ter zagotovitev varnosti osebnih podatkov skladno s Splošno uredbo.

4.5 Ali lahko obdelovalec najema podizvajalce za določene obdelave osebnih podatkov?

Ureditev pogodbene obdelave osebnih podatkov, kot jo določa Splošna uredba, je primarno namenjena temu, da **ima (in ohrani) upravljavec nadzor** nad obdelavo osebnih podatkov, tj. komu bo zaupal osebne podatke v zunanje izvajanje. S tega vidika mora biti **v vsakem primeru vnaprej seznanjen in se strinjati s tem, katere podizvajalce najemajo njegovi obdelovalci**, pa tudi s tem, **kako posamezni podizvajalci zagotavljajo ustrezno varnost osebnih podatkov** ter na kakšen način **bo upravljavec izvajal nadzor** nad izvajanjem postopkov in ukrepov za zagotavljanje varnosti osebnih podatkov. Obdelovalci namreč ne smejo samostojno najemati podizvajalcev, ki bodo za njih izvajali določene obdelave osebnih podatkov, ki so jih prejeli s strani upravljavca. Če npr. podjetje A najame podjetje B, ki nudi izvajanje storitev neposrednega trženja za podjetje A, potem podjetje B ne sme samovoljo najeti podjetja C, pri katerem bo hranilo osebne podatke strank podjetja A (upravljavca). Obdelovalci morajo za to bodisi pridobiti **predhodno posebno ali splošno pisno pooblastilo** upravljavca, da lahko posamezna opravila obdelave osebnih podatkov prenesejo na pod-obdelovalca in z njim sklenejo ustrezno pogodbo, ali pa morajo upravljavec, obdelovalec in pod-obdelovalec skleniti ustrezno tripartitno pogodbo.

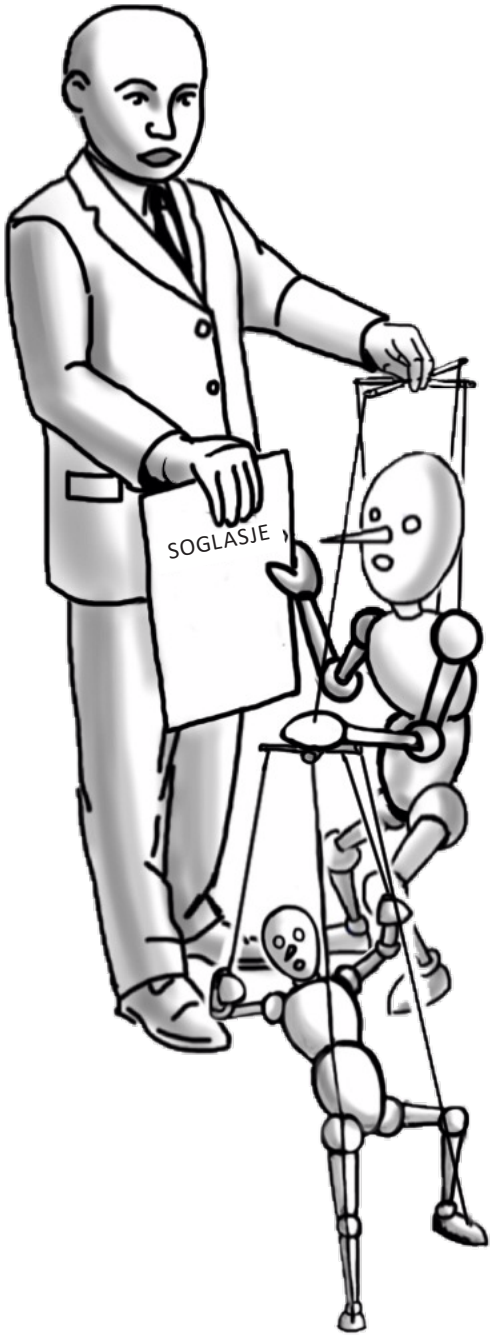


V vsakem primeru mora torej najemanje podizvajalcev potekati **z vnaprejšnjim soglasjem upravljavca in ob upoštevanju zahtev iz 28. člena Splošne uredbe**; posebej mora biti zagotovljena **ustrezna varnost** osebnih podatkov, in sicer tako, da je podizvajalec zavezan enakim ukrepom, kot jih mora upoštevati obdelovalec. Posebej je pomembno, da so **jasno opredeljene tudi odgovornosti obdelovalcev in njihovih morebitnih podizvajalcev**, npr. kdo bo odgovarjal v primeru neustrezne varnosti podatkov s strani podizvajalca.

V primeru kršitev varnosti mora obdelovalec skladno z določbami 33. člena Splošne uredbe po seznanitvi s kršitvijo varstva osebnih podatkov brez nepotrebnega odlašanja uradno obvestiti upravljavca. Takšni primeri so lahko:

- Ponudnik programske opreme za osnovne šole ugotovi varnostno ranljivost, zaradi katere bi lahko bile ocene otrok javno dostopne, zato mora brez nepotrebnega odlašanja obvestiti vse šole, katerim zagotavlja programsko opremo.
- Računovodski servis doživi požar, v katerem zgori dokumentacija z osebnimi podatki podjetij, katerim izvaja obračun plač.
- Ponudnik oblačne hrambe podatkov doživi hekerski vdor, zaradi katerega so v nepooblaščene roke prišli osebni podatki njegovih naročnikov.

Upravljavec ima nato dolžnost o kršitvi varnosti obvestiti Informacijskega pooblaščenca.



Upravljavci se prav tako morajo zavedati, da imajo ne glede na to, ali izvajajo obdelavo sami ali s pomočjo drugih, določene zakonske dolžnosti in odgovornosti. Mednje sodi tudi ta, **da v zakonsko predvidenih rokih in obsegu uresničujejo pravice posameznik**a do seznanitve, popravka, brisanja in ugovora. Omenjene pravice namreč posameznik uveljavlja **pri upravljavcu**, zato mora ta zagotoviti, da bodo kljub morebitni (pod)obdelavi pravice posameznika izvršene v zakonsko predvidenih rokih in obsegu, sicer lahko sam odgovarja za morebitne zastoje ali pomanjkljivosti, ki bi jih povzročili izbrani (pod)obdelovalci.

Več o kršitvah varnosti si lahko preberete na posebni podstrani IP.

Najpogostejše napake

pri pogodbeni obdelavi osebnih podatkov

- Upravljavec s pogodbenim obdelovalcem ni sklenil pisne pogodbe ali drugega pravnega akta.
- Pisna pogodba obstaja, ne vsebuje pa zahtevanih določb po 28. členu Splošne uredbe.
- V pisni pogodbi je zgolj sklic na »ustrezno ravnanje z osebnimi podatki in spoštovanje določb zakonodaje o varstvu osebnih datkov«, postopki in ukrepi pa niso konkretizirani.
- Upravljavec nima pregleda nad tem, katere pogodbene obdelovalce vse uporablja.
- Upravljavec napačno oceni zunanjega izvajalca, češ da ne gre za pogodbeno obdelavo osebnih podatkov (npr. zgolj nudenje storitev hrambe osebnih podatkov ali prevoz na uničenje).
- Upravljavec zunanjega izvajalca ne seznani s tem, da mu bo v obdelavo poveril osebne podatke (npr. v hrambo ali v uničenje), zunanji izvajalec pa posledično ne sprejme in ne izvaja ustreznih ukrepov za varnost.
- Upravljavec ne nadzira svojih pogodbenih obdelovalcev.
- Upravljavec iznaša osebne podatke obdelovalcu v tretji državi, pri čemer pa zanemari dolžnosti glede prenosa osebnih podatkov v tretje države.
- Obdelovalci uporabljajo storitve drugih (pod)izvajalcev brez vednosti in brez vnaprejšnje odobritve s strani upravljavca in upoštevanja določb Splošne uredbe.
- Posamezni zaposleni pri obdelovalcu ne poznajo dolžnosti po Splošni uredbi.

Zaključek

V smernicah na podlagi mnogih praktičnih primerov pojasnjujemo, kaj vse sodi med pogodbeno obdelavo, kakšne so obveznosti upravljavca osebnih podatkov in njegovega pogodbenega partnerja ter katere so pasti in priporočila za zakonsko skladno ureditev zunanjega izvajanja storitev, ki vključuje osebne podatke.

Preden upravljavec osebne podatke zaupa pogodbenemu partnerju, mora tako nujno vedeti, za kakšen namen bo osebne podatke posredoval in zagotoviti, da bo pogodbeni partner dejansko opravljal naloge v zvezi z obdelavo sebnih podatkov samo v okviru navodila. Ključnega pomena je ustrezna ureditev pogodbenega razmerja z obdelovalcem in morebitnimi podobdelovalci, kot to določa 28. člen Splošne uredbe ter primerna varnost osebnih podatkov pri pogodbenem partnerju, kar mora upravljavec zagotoviti s pisno pogodbo, v kateri podrobno določi varnostne postopke in ukrepe (kako bodo osebni podatki fizično varovani, kako bo varovana aplikativna in programska oprema, kako bo preprečen nepooblaščen dostop do podatkov pri prenosu, kako bodo podatki učinkovito izbrisani, kako bo urejena sledljivost dostopa do podatkov).

Upravljavec osebnih podatkov je vedno odgovoren za zakonitost obdelave osebnih podatkov, čeprav jih posreduje v obdelavo pogodbenemu partnerju. Zato mora opredeliti tudi na kakšen način bo nadzoroval obdelavo pri obdelovalcu. Po koncu pogodbene obdelave osebnih podatkov mora pogodbeni partner podatke vrniti upravljavcu in morebitne kopije izbrisati, razen če poseben predpis od njega zahteva drugače (v tem primeru postane v tem delu upravljavec teh podatkov).