

# VARSTVO OSEBNIH PODATKOV

Evropska uredba o varstvu osebnih podatkov (General Data Protection Regulation - GDPR) govori o varovanju **osebnih podatkov** in ne vseh podatkov in informacij, ki jih hranimo. Obdelava osebnih podatkov s pomočjo modernih tehnologij (kartice zaupanja, kreditna kartica, IP naslov računalnika, e-naslov, socialna omrežja) je namreč lahko tveganje za zasebnost posameznika. Namen uredbe je ozavestiti posameznika o tem, komu in zakaj bo dal na razpolago svoje osebne podatke.

Kaj so pravzaprav osebni podatki?

Zakon o varstvu osebnih podatkov (ZVOP-1) določa, da je varstvo osebnih podatkov namenjeno preprečevanju nezakonitih in neupravičenih posegov v informacijsko zasebnost posameznika na vseh relevantnih področjih. Smisel varstva osebnih podatkov torej ni varovanje osebnih podatkov kot takih, temveč varovanje pravic posameznika, na katerega se podatki nanašajo.

**Osebni podatek** je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Nanaša se lahko na lastnosti, stanja in razmerja posameznika; je tisti, ki jih vsebujejo zbirke osebnih podatkov kot javne (uradne) evidence. Mnoge javne pravne osebe imajo namreč po Zakonu o varstvu osebnih podatkov pravno podlago za vodenje in ravnanje z zbirkami osebnih podatkov.

**Občutljivi osebni podatki** – so podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali evidenc, ki se vodijo na podlagi zakona, ki ureja prekrške; občutljivi osebni podatki so tudi biometrične značilnosti (takšne telesne, fiziološke ter vedenjske značilnosti, ki jih imajo vsi posamezniki, so pa edinstvene in stalne za vsakega posameznika posebej in je možno z njimi določiti posameznika, zlasti z uporabo prstnega odtisa, posnetka papilarnih linij s prsta, šarenice, očesne mrežnice, obraza, ušesa, deoksiribonukleinske kisline ter značilne drže), če je z njihovo uporabo mogoče določiti posameznika v zvezi s kakšno od prej navedenih okoliščin.

Obdelava občutljivih osebnih podatkov je dovoljena le v izjemnih primerih.

Koliko pomembnosti se namenja zaščiti osebnih podatkov, zlasti pa občutljivih osebnih podatkov, kaže Zakon o arhivskem gradivu, ki vsebuje osebne podatke o zdravljenju pacienta (ZAGOPP, UL RS, št. 85/2016), ki dopušča prevzem tega gradiva v pristojne arhive 150 let po nastanku, dostop v njih pa je zelo omejen.

## Ureditev varstva osebnih podatkov v Republiki Sloveniji

Sistemska ureditev varstva osebnih podatkov v nacionalni zakonodaji je bila potrebna zaradi enotne določitve načel, pravil in obveznosti, kakor tudi zaradi izpolnitve pravnih praznin, ki bi lahko nastale, če bi to področje parcialno urejali

posamezni zakoni. Smiselno pa je tudi definicije, obveznosti in ukrepe v zvezi z zavarovanjem osebnih podatkov, kataloge zbirk osebnih podatkov, registracijo zbirk osebnih podatkov, pravice posameznika ter vprašanja glede nadzora in pristojnosti nadzornih organov predpisati na enem mestu.

Varstvo osebnih podatkov je pomembno predvsem s stališča posameznika, je namenjeno predvsem njemu in varovanju njegove zasebnosti, vendar pa je zadeva pomembna tudi za vlade in nevladne organizacije, za javni in zasebni sektor, Leta 2007 je Svet Evrope pod imenom Evropski dan varstva osebnih podatkov vpeljal mednarodni praznik (praznuje se vsako leto 28. januarja), ki ljudi ozavešča o varstvu osebnih podatkov in s tem povezanih pravicah. Dan varstva osebnih podatkov je praznik v Evropski uniji, v Združenih državah Amerike in v Kanadi, praznujemo pa ga na datum podpisa Konvencije 108, sprejete 28. januarja 1981, ki je bila prvi mednarodni zakon o varstvu osebnih podatkov, ki je varstvo osebnih podatkov definiral kot temeljno pravico. Zavedanje o pomenu varstva osebnih podatkov torej ni tako starodavna stvar, pa tudi v posameznih državah obstajajo različne ravni varovanja zasebnosti posameznika. To je odvisno od splošnega družbenega razvoja nekega okolja, na to pa lahko vplivajo tudi posamezne, za neko okolje stresne situacije (npr. nevarnost terorizma v ZDA je povzročila sprejem ukrepov, ki so trend zaščite zasebnosti posameznika obrnile v nasprotno smer).

Varstvo osebnih podatkov je v Republiki Sloveniji ena od ustavno zagotovljenih človekovih pravic in temeljnih svoboščin in spada v okvir pravic s področja zasebnosti. Določbe 38. člena **Ustave RS** zagotavljajo varstvo osebnih podatkov ter prepoveduje njihovo uporabo v nasprotju z namenom njihovega zbiranja. Za normativno urejanje varstav osebnih podatkov je zlasti pomembna določba, da zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon. Takšna ustavna določba predpisuje ureditev varstva osbnih podatkov v splošnem, sistemskem zakonu, poleg tega po dopušča možnost urejanja varstva osebnih podatkov v področnih zakonih, ki pa morajo upoštevati določbe 38. člena ustave.

**Zakon o varstvu osebnih podatkov** (Ur. l. RS št. 86/2004, 113/2005-ZInfP, 51/2007-ZUstS-A, 67/2007, 94/2007-UPB1) določa pravice, obveznosti, načela in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika oziroma posameznice; načelno torej določa, da je varstvo osebnih podatkov namenjeno preprečevanju nezakonitih in neupravičenih posegov v informacijsko zasebnost posameznika na vseh relevantnih področjih. Določa tudi, da je na ozemlju Republike Slovenije vsakemu posamezniku, ne glede na državljanstvo in prebivališče (in ne glede na narodnost, raso, barvo, veroizpoved, etnični pripadnost, spol, jezik, politično ali drugo prepričanje, spolno usmerjenost, premoženjsko stanje, rojstvo, izobrazbo, družbeni položaj ali katerokoli drugo osebno okoliščino.) zagotovljeno varstvo osebnih podatkov.

Zakon predpisuje, da se osebni podatki obdelujejo zakonito in pošteno. Pojem obdelav osebnih podatkov pa zakon opredeljuje kot kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, **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 je lahko ročna ali avtomatizirana (sredstva obdelave). Uporaba izraza "zlasti" pomeni, da so primeri obdelave naštet le primeroma in da torej kakršnokoli ravnanje z osebnimi podatki, tudi na način, ki med navedenimi primeri ni naveden, pomeni obdelavo osebnih podatkov.

Varstvo osebnih podatkov spada v sfero zasebnosti posameznika, katerega varstvo je zagotovljeno že z Ustavo RS. Tako je dolžnost države, da zagotavlja varstvo posameznika pred posegom drugega posameznika ali države s tem, da zagotavlja učinkovita pravna sredstva za njihovo varovanje. V primeru, ko posamezniku nastane škoda (npr. zaradi neupravičenega posredovanja osebnih podatkov ali izvajanja videonadzora brez obvestila), mu **Obligacijski zakonik** (Ur. l. RS št. 97/2007-UPB1) daje v možnost, da doseže preko sodišča ali drugega pristojnega organa, "da odredi prenehanje dejanja, s katerim se krši nedotakljivost človekove osebnosti, osebnega in družinskega življenja ali kakšna druga osebnostna pravica, da prepreči tako dejanje ali da odstrani njegove posledice" ter da omenjeni organ "lahko odredi, da kršitelj preneha z dejanjem, ker bo sicer moral plačati prizadetemu določen denarni znesek, odmerjen skupaj ali od časovne enote." Obligacijski zakonik tudi omogoča prizadetemu posamezniku, da pravično denarno odškodnino za pretrpljene telesne ali duševne, razžalitve dobrega imena in časti ali okrnitve svobode ali osebnostne pravice, itd.

Nadzor nad izvajanjem zakona in drugih predpisov, ki urejajo varstvo ali obdelavo osebnih podatkov izvaja **Informacijski pooblaščenec**, ki je samostojen in neodvisen državni organ. Po Zakonu o Informacijskem pooblaščenču (Uradni list RS, št. 113/2005, 51/2007-ZUstS-A, 14/2010 Odl.US: U-I-303/08-9) pristojen za:

- odločanje o pritožbi zoper odločbo, s katero je organ zavrgel ali zavrnil zahtevo ali drugače kršil pravico do dostopa ali ponovne uporabe informacije javnega značaja ter v okviru postopka na drugi stopnji tudi za nadzor nad izvajanjem zakona, ki ureja dostop do informacij javnega značaja, in na njegovi podlagi izdanih predpisov;

- inšpekcijski nadzor nad izvajanjem zakona in drugih predpisov, ki urejajo varstvo ali obdelavo osebnih podatkov oziroma iznos osebnih podatkov iz Republike Slovenije, ter opravljanje drugih nalog, ki jih določajo ti predpisi;

- odločanje o pritožbi posameznika, kadar upravljavec osebnih podatkov ne ugodí zahtevi posameznika glede pravice posameznika do seznanitve z zahtevanimi podatki, do izpisov, seznamov, vpogledov, potrdil, informacij, pojasnil, prepisovanja ali kopiranja po določbah zakona, ki ureja varstvo osebnih podatkov.

Zakon o varstvu osebnih podatkov določa pristojnosti Informacijskega pooblaščenca bolj podrobno.

Splošna pravna podlaga za dopustno obdelavo osebnih podatkov je določena v prvem odstavku 8. člena ZVOP-1, na podlagi katere se lahko osebni podatki obdelujejo le, če obdelavo podatkov in osebnih podatkov, ki se obdelujejo, določa zakon, ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika. V 9. členu ZVOP-1 pa je natančneje posebej urejena pravna podlaga

za obdelavo osebnih podatkov v javnem sektorju, kamor sodijo tudi javne osnovne šole.

V javnem sektorju se lahko osebni podatki obdelujejo le, če tako določa zakon, ki lahko tudi določi, da se določeni osebni podatki obdelujejo le na podlagi osebne privolitve posameznika.

## **Bistvene spremembe pri varstvu osebnih podatkov ob uvedbi GDPR**

Posameznikom – več pravic

Upravljalcem – več dolžnosti

### **Pravice posameznika**

V uredbi so navedene pravice posameznika, na katerega se nanašajo osebni podatki, tj. posameznika, katerega osebni podatki se obdelujejo. Med temi pravicami so pravica do dostopa do osebnih podatkov ter pravice do popravka, pozabe, izbrisa, omejitve obdelave, ugovora in prenosljivosti podatkov:

**pravica do obveščенosti** o obdelavi vaših osebnih podatkov

**pravica dostopa do osebnih podatkov** pomeni, da ima posameznik pravico od upravljalca dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki, in kadar je tako, dostop do teh osebnih podatkov in dodatnih informacij (nameni obdelav, vrste podatkov, uporabnike podatkov, obstoj pravic in možnosti pritožbe, viri podatkov, morebitno avtomatizirano odločanje ali posebno profiliranje);

**pravica do popravka** pomeni, da ima posameznik pravico doseči, da upravljalec brez nepotrebnega odlašanja popravi netočne osebne podatke v zvezi z njim; ob upoštevanju namenov obdelave ima tudi pravico do dopolnitve nepopolnih osebnih podatkov, vključno s predložitvijo dopolnilne izjave;

**pravica do izbrisa**, imenovana tudi »pravica do pozabe«, pomeni, da ima posameznik pravico doseči, da upravljalec brez nepotrebnega odlašanja izbriše osebne podatke v zvezi z njim, če so izpolnjeni predpisani pogoji (obdelava ni več potrebna, preklic privolitve in neobstoj druge pravne podlage, utemeljen ugovor, nezakonita obdelava, izbris po zahtevah veljavnih predpisov...);

**pravica do omejitve obdelave** pomeni pravico, da posameznik doseže, da upravljalec omeji obdelavo vaših podatkov, če oporeka točnosti podatkov ali če vloži ugovor ali če je obdelava nezakonita ali če obdelava ni več potrebna za upravljalca, temveč za uveljavljanje, izvajanje ali obrambo vaših pravnih zahtevkov;

**pravica do prenosljivosti** pomeni pravico, da posameznik prejme osebne podatke v zvezi z njim, ki jih je posredoval upravljalcu, v strukturirani, splošno uporabljani in strojno berljivi obliki, in pravico, da posameznik te podatke posreduje drugemu upravljavcu, ne da bi ga pri tem upravljalec kakorkoli ovirali (velja za podatke, ki jih upravljalec obdeluje avtomatizirano na podlagi privolitve ali pogodbenega razmerja);

**pravica do ugovora** pomeni, da posameznik lahko proti nekaterim vrstam obdelav njegovih osebnih podatkov (javni interesi, zakoniti interesi upravljavca, nameni trženja) kadarkoli ugovarja in mora upravljalec dokazati legitimne interese za obdelavo oziroma prenehati z obdelavo (vedno v primeru trženja);

**pravica glede samodejne obdelave in profiliranja** pomeni, da za posameznika ne velja odločitev, ki temelji zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov, ki ima pravne ali podobne učinke v zvezi s posameznikom, če ni to nujno potrebno, predpisano ali če v to posameznik ne privoli.

## **Obveznosti upravljavcev in obdelovalcev podatkov**

Za obdelavo osebnih podatkov potrebujete osebno privolitev posameznika. Uredba v 32. členu pravi, da mora privolitev biti podana z jasnim pritrdilnim dejanjem, ki pomeni, da je posameznik prostovoljno, specifično, ozaveščeno in nedvoumno izrazil soglasje k obdelavi osebnih podatkov. Določena je tudi obveznost upravljavcev (oseb, odgovornih za obdelavo podatkov) glede zagotavljanja preglednih in lahko dostopnih informacij posameznikom, na katere se nanašajo osebni podatki, o obdelavi njihovih podatkov.\_

V uredbi so podrobno opredeljene splošne obveznosti upravljavcev in oseb, ki osebne podatke obdelujejo v njihovem imenu (obdelovalci). Med temi obveznostmi sta obveznost izvajanja ustreznih varnostnih ukrepov in obveznost **uradnega obveščanja o kršitvah** varstva osebnih podatkov. V skladu z uredbo bodo javni sektor ter podjetja, katerih temeljne dejavnosti zajemajo ali dejanja obdelave, ki pomenijo redno in sistematično obsežno spremljanje posameznikov, ali pa obsežno obdelavo posebnih vrst podatkov, morali imenovati **uradno (odgovorno) osebo za varstvo podatkov (DPO)**, ki bo stalno spremljala skladnost obdelav z veljavnimi predpisi in mednarodnimi standardi, ocenjevala učinke obdelave osebnih podatkov in sodelovala z nadzornimi organi.

Upravljavci ne bodo več dolžni prijavljati zbirk osebnih podatkov v register zbirk osebnih podatkov, ostajajo pa dolžnosti sprejema **katalogov**, te dolžnosti se krepijo in uvajajo tudi za (pogodbene) obdelovalce.

Večji poudarek daje uredba tudi (predhodnim) izvedbam **analiz učinkov na varstvo osebnih podatkov**, v primeru varnostnih incidentov, kot je npr. izguba osebnih podatkov, pa se uvaja **obveznost poročanja nadzornemu organu** in v določenih primerih tudi obveščanja vseh prizadetih posameznikov.

## Nadzorni organi

V uredbi je potrjena obstoječa obveznost držav članic glede ustanovitve **neodvisnega nadzornega organa** na nacionalni ravni. Njegov cilj je tudi vzpostavitev mehanizmov, s katerimi bi zagotovili doslednost pri izvajanju zakonodaje o varstvu podatkov v vsej EU. Bistveno je, da bo v primeru, ko obdelava osebnih podatkov poteka v več kot eni državi članici, načeloma en sam ti. vodilni nadzorni organ pristojen za spremljanje vseh teh dejavnosti. To načelo, imenovano **vse na enem mestu**, pomeni, da bo pristojni vodilni nadzorni organ v vsakem primeru, ko gre za čezmejno obdelavo osebnih podatkov organ države članice, v kateri je glavni ali edini sedež upravljavca ali obdelovalca.

Uredba zajema tudi ustanovitev Evropskega odbora za varstvo podatkov (angl. European Data Protection Board, EDPB). Ta odbor naj bi sestavljali predstavniki vseh 28 neodvisnih nadzornih organov in bo nadomestil sedanjo Delovno skupino za varstvo podatkov iz člena 29 (Article 29 Working Party).

## Pravica do pravnega sredstva in sankcije

Nova uredba ureja tudi pravico posameznikov, na katere se nanašajo osebni podatki, do **vložitve pritožbe** pri nadzornem organu, pa tudi njihovo pravico do pravnih sredstev zoper odločitve nadzornega organa ali v primeru neukrepanja nadzornega organa, pravico do odškodnine in odgovornosti.

Zoper upravljavce ali obdelovalce, ki kršijo pravila o varstvu podatkov, so določene zelo ostre sankcije. Te **upravne sankcije** izrečejo nacionalni organi za varstvo podatkov.

## Predlagane aktivnosti upravjalcev

### **Preveriti obstoječe privolitve (čl. 6 in 7, uvodne določbe 32, 42, 43 in 171)**

Obdelava je zakonita le in kolikor je izpolnjen vsaj ena od naslednjih šestih možnih pravnih podlag (privolitev, sklepanje ali izvajanje pogodbe, zakonske obveznosti, zaščita življenjskih interesov posameznika, naloge v javnem interesu, zakoniti interesi upravljavca ali tretjih oseb) ter točno določen čas, ko je to potrebno. Kadar obdelava temelji na privolitvi, mora biti upravljavec zmožen dokazati, da je posameznik, na katerega se nanašajo osebni podatki, privolil v obdelavo svojih osebnih podatkov. Pogoji glede otrok do 16 leta (čl. 8).

**Preverite načine pridobivanja privolitev v bodoče (čl. 12, 13 in 14)** Pregledne informacije, sporočila in načini za uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki; informacije, ki se zagotovijo, kadar se osebni podatki pridobijo od posameznika, na katerega se nanašajo osebni podatki; informacije, ki jih je treba zagotoviti, kadar osebni podatki niso bili pridobljeni od posameznika, na katerega se ti nanašajo.

## **Prilagodite pogodbe s pogodbenimi obdelovalci (čl. 28)**

### **Preverite in prilagodite popis zbirk osebnih podatkov – evidence dejavnosti obdelave (čl. 30)**

Vsak upravljavec in predstavnik upravljavca, kadar ta obstaja, vodi evidenco dejavnosti obdelave osebnih podatkov v okviru svoje odgovornosti. Ta evidenca vsebuje več informacij (katalog zbirke osebnih podatkov!)

## **Preglejte postopke za zagotavljanje pravic posameznika (čl. 12–22)**

### **Preglejte in prilagodite vaše varnostne politike in njihovo izvajanje (čl. 24)**

Ob upoštevanju narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti, upravljalec izvede ustrezne tehnične in organizacijske ukrepe, da zagotovi in je zmožen dokazati, da obdelava poteka v skladu s to uredbo. Ti ukrepi se pregledajo in dopolnijo, kjer je to potrebno. Kadar je to sorazmerno glede na dejavnosti obdelave, omenjeni ukrepi vključujejo izvajanje ustreznih politik za varstvo podatkov s strani upravljavca. Zavezanost k odobrenim kodeksom ravnanja iz člena 40 ali izvajanje odobrenega mehanizma potrjevanja iz člena 42 se lahko uporabi za dokazovanje izpolnjevanja obveznosti upravljalca.

### **Določite, kdo bo poročal v primeru varnostnega incidenta (čl. 33)**

V primeru kršitve varstva osebnih podatkov upravljavec brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah po seznanitvi s kršitvijo, o njej uradno obvesti pristojni nadzorni organ v skladu s členom 55, razen če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov. Kadar uradno obvestilo nadzornemu organu ni podano v 72 urah, se mu priloži navedbo razlogov za zamudo.

### **Pripravite se na izvajanje načela odgovornosti**

Če so osebni podatki temelj vašega delovanja, ukrepajte pred obiskom inšpekcije in sami preverite, ali boste morali

- izvajati oceno učinka (čl. 35)
- imenovati odgovorno osebo za varstvo osebnih podatkov (»DPO«) (čl. 37)
- preveriti vaše postopke za minimizacijo (načelo vgrajenega in privzetega varstva osebnih podatkov (čl. 35); minimizirate lahko količino zbranih podatkov, obseg njihove obdelave, obdobje njihove hrambe in število oseb, ki jih obdelujejo.

Popišite tudi zbirke osebnih podatkov, ki nastajajo v vaši ustanovi.

## **Primeri iz prakse:**

- Če ste z nekom v stiku preko e-pošte (povpraševanje itd), ali jo lahko hranite in kontaktirate z njim kasneje?

Lahko, a le za informacije, ki jih je zahtevala stranka, ne pa za npr. pošiljanja obvestil itd.

- **Ali je za primer, da pošljem stranki tiskano pošto, potrebno pridobiti dovoljenje?**

Ne, ker to ureja druga zakonodaja (nalepka na poštnem nabiralniku).

- **Ali se sme obstoječi stranki poslati e-obvestilo o novi ponudbi?**

Sme, gre za neposredno trženje, vendar mora stranka imeti možnost zavrniti nadaljnje prejemanje takih sporočil. Bodite pozorni, da ni to možnost take uporabe svoje e-pošte zavrnila že na začetku.

- **Na seminarju udeleženci na evidenčnem listu označijo, da se strinjajo s sprejemanjem novic. Je to dovoljeno?**

Ob pridobivanju soglasja je potrebno posameznika seznaniti z vsebino 13., 14. in 15. člena GDPR. V omenjenem primeru navedite skrajšano verzijo splošnih pogojev na evidenčnem listu ali jih imejte na razpolago pri organizatorju dogodka.

- **Zbiranje podatkov za ureditev kakšne usluge udeležencu dogodka (rezervacija hotela, najem avtomobila itd). Smemo hraniti podatke, pridobljene za te namene?**

Ne, hranimo jih le tako dolgo, kot je potrebno za takšen namen, nato se morajo takoj izbrisati.

- **Je dovoljeno fotografiranje dogodkov in objavljanje fotografij na socialnih omrežjih?**

Je, če se stranka prijavi na dogodek, se mora strinjati s splošnimi pogoji. Stranki mora biti omogočeno, da javi svoje nestrinjanje s pojavljanjem na fotografijah z javnih dogodkov. Pri udeležbi otrok na dogodku morajo takšna strinjanja podati starši.

- **Ali lahko delodajalec zahteva telefonske številke zaposlenih?**

Delodajalci lahko zbirajo le tiste podatke, ki jih potrebujejo za izpolnjevanje zakonskih določil ali za potrebe nemotenega zaposlovanja. Zasebni telefon ali e-pošta nista praviloma potrebna za nemoteno poslovanje, delavec se lahko strinja, da delodajalec hrani njegovo številko, če je to v interesu obeh. Nekatere druge osebne podatke, ki so nujni za opravljanje dela, delodajalec sme hraniti (npr. podatki o konfekcijski številki za delovno obleko itd).

- **Kopiranje osebnih dokumentov za kadrovske evidence?**

Vpogled v dokumente je dovoljen pri vpisu osebnih podatkov v evidenco delodajalca. Tudi pridobitev kopij je dovoljena, vendar jih mora delodajalec uničiti takoj po prepisu podatkov.



### **Še zadnji novici:**

- Informacijski pooblaščenec bo vse do septembra 2020 izvajal evropski projekt RAPID.Si (Raising Awareness on Data Protection and the GDPR in Slovenia), ki je namenjen izobraževanju manjših in srednje velikih podjetij ter posameznikov o reformi zakonodaje s področja varstva osebnih podatkov.

(<https://www.ip-rs.si/novice/varstvo-osebnih-podatkov-pomoc-in-pojasnila-majhnim-podjetjem-in-posameznikom-1101/>)

- Priporočila Informacijskega pooblaščenca glede delovanja pooblaščene osebe za varstvo osebnih podatkov

([https://www.ip-rs.si/fileadmin/user\\_upload/Pdf/novice/Priporocila\\_IP\\_glede\\_delovanja\\_DPO\\_koncno.pdf](https://www.ip-rs.si/fileadmin/user_upload/Pdf/novice/Priporocila_IP_glede_delovanja_DPO_koncno.pdf))