KAKO SO MOJI PODATKI VAROVANI V DELOVNEM RAZMERJU?

Priročnik o varstvu osebnih podatkov

iDecide

Individuals decide - raising awareness about data protection rights

To publikacijo financira Evropska unija v okviru »Programa pravice, enakost in državljanstvo 2014-2020«.

Avtorji: Informacijski pooblaščenec RS (Maja Wondra Horvat, mag. Polonca Štrekelj, mag. Andrej Tomšič, dr. Jelena Burnik, mag. Vanja Zrimšek)

Oblikovanje: Informacijski pooblaščenec RS (Anže Novak)

Leto izdaje: 2020

INFORMACIJSKI POOBLAŠČENEC

REPUBLIKA SLOVENIJA

KAZALO

KAKO SO MOJI PODATKI VAROVANI V DELOVNEM RAZMERJU?

Zaposleni smo v delovnem razmerju podvrženi pogostim obdelavam zelo različnih osebnih podatkov. Z razvojem tehnologije se brišejo meje med službenim in zasebnim življenjem, njena uporaba za namen nadzora nad delavci pa povečujejo tveganja za nezakonito in nesorazmerno obdelavo osebnih podatkov in s tem kratenje pravice do zasebnosti.

Varstvo osebnih podatkov je temeljna človekova pravica. Namen varstva osebnih podatkov ni zgolj varovanje osebnih podatkov kot takih, temveč predstavlja širše varstvo posameznika, njegove zasebnosti, dostojanstva in svobode odločanja.

Ureditev

Področje je primarno urejeno s **Splošno uredbo o varstvu podatkov** (Splošna uredba),[1] ki je prinesla številne obveznosti, ki jih morajo zagotavljati delodajalci v EU in hkrati nove pravice, ki pripadajo delavcem. V določenih delih, kjer to Splošna uredba dopušča, ostaja v veljavi tudi **Zakon o varstvu osebnih podatkov** (ZVOP-1).[2]

Vsebina priročnika

Priročnik, ki je pred vami, na pregleden način pojasnjuje, kakšne so **vaše pravice** glede varstva osebnih podatkov v delovnem razmerju in kakšne so **dolžnosti delodajalca**. Našli boste številne primere, povezave do obrazcev, vzorcev, zahtev in pritožb, ki jih lahko uporabite za zaščito svojih pravic, ter do preostalih gradiv Informacijskega pooblaščenca, v katerih so določena vprašanja bolj podrobno razdelana.

1 Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter razveljavitvi Direktive 95/46/ES, UL EU L 119/1, 4. 5. 2016.

2 Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo).

ZAKONSKA UREDITEV VARSTVA OSEBNIH PODATKOV

OSNOVNI POJMI IN NAČELA

Obdelava osebnih podatkov

Je vse, kar delodajalec (ali delavec) z osebnimi podatki počne (njihovo zbiranje, vpisovanje, spreminjanje, vpogledovanje, posredovanje, uničenje ipd.). Tudi kadar delodajalec osebne podatke zgolj hrani, govorimo o obdelavi osebnih podatkov. Poleg osebnih podatkov delavcev delodajalec obdeluje tudi osebne podatke tretjih oseb (npr. kandidatov za zaposlitev, družinskih članov delavca, ki so pomembni zaradi določitve dopusta ipd.).

Da bi bila obdelava osebnih podatkov delavcev zakonita, mora delodajalec zagotavljati, da obdelava ves čas poteka v skladu s **splošnimi načeli** in **na ustrezni pravni podlagi.**

Načela varstva osebnih podatkov

- **Načelo zakonitosti, pravičnosti in preglednosti:**

Osebne podatke je treba obdelovati zakonito, pošteno in na pregleden način do delavca.

- **Načelo omejitve namena:**

Osebni podatki se lahko obdelujejo le za tisti namen, zaradi katerega so bili zbrani.

- **Načelo najmanjšega obsega podatkov:**

Delodajalec lahko zbira le tiste osebne podatke, ki jih potrebuje za dosego določenega namena.

Primer: *Če ste fotomodel, potem je upravičeno, da delodajalec od vas pričakuje foto portfelj, tega pa npr. delodajalec ne more zahtevati od*

računovodje ali informatika. Nabor potrebnih osebnih podatkov se glede na naravo dela zelo razlikuje od primera do primera. Osebni podatki se ne smejo zbirati »na zalogo« (npr. kandidat za zaposlitev ni dolžan delavcu sporočiti svoje davčne številke, če bo morda izbran, delodajalec pa tega nima pravice zahtevati). Kadar je mogoča izbira, je treba uporabiti manj občutljive podatke (npr. psevdonimi so boljši kot celotno osebno ime). Osebni podatki so na voljo le tistim osebam, ki jih dejansko potrebujejo (npr. TRR je na voljo računovodji, ki obračunava plače, ne pa tudi varnostniku podjetja).

- **Načelo točnosti:**

Delodajalec mora preveriti točnost podatkov in jih redno posodabljati. Zastareli, napačni ali nepopolni podatki imajo lahko za posameznika hude posledice.

- **Načelo omejitve shranjevanja:**

Delodajalec lahko osebne podatke hrani le toliko časa, kolikor je to potrebno za namen obdelave.

- **Načelo celovitosti in zaupnosti:**

Osebni podatki morajo biti zaščiteni pred zlorabami z ustreznimi tehničnimi in organizacijskimi ukrepi.

- **Načelo odgovornosti upravljavca:**

Delodajalec mora biti vsak trenutek sposoben izkazati, da z osebnimi podatki ravna v skladu s predpisi.

Področni predpisi

Delodajalci in delavci morajo poleg določb Splošne uredbe in ZVOP-1 upoštevati še druge predpise, ki podrobneje urejajo delovnopravna razmerja. Najpomembnejši so: Zakon o delovnih razmerjih (ZDR-1)[3], Zakon o evidencah na področju dela in socialne varnosti (ZEPDSV)[4], Zakon o varnosti in zdravju pri delu (ZVZD-1)[5], Zakon o javnih uslužbencih (ZJU-1)[6], Zakon

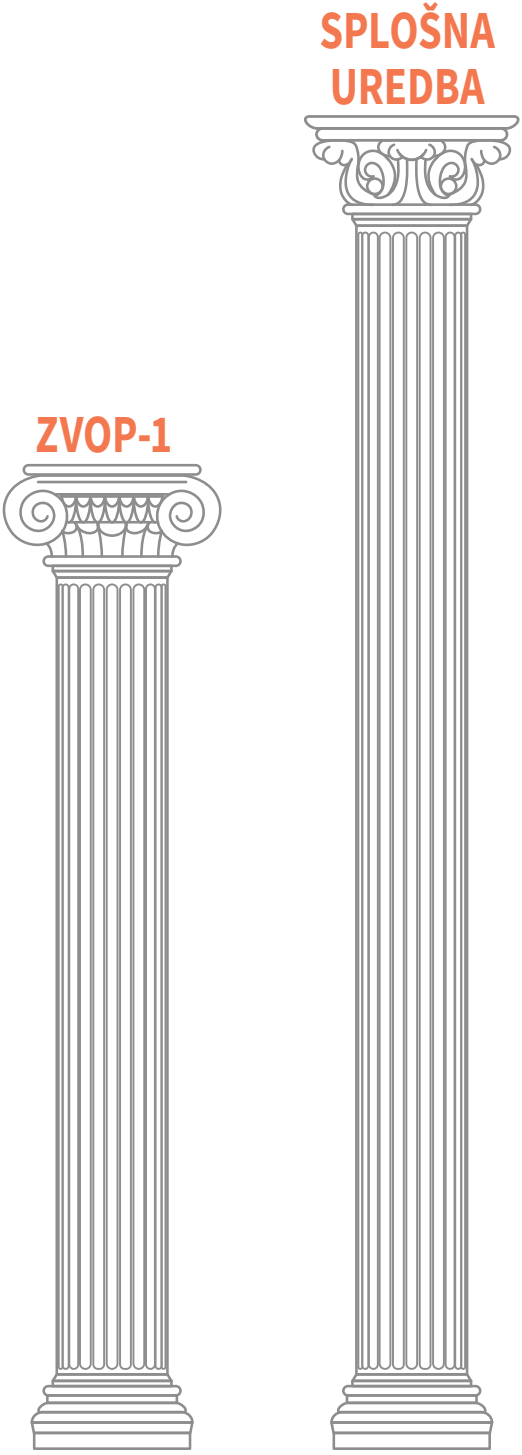
3 Uradni list RS, št. 21/13, 78/13 – popr., 47/15 – ZZSDT, 33/16 – PZ-F, 52/16, 15/17 – odl. US, 22/19 – ZPosS in 81/19.

4 Uradni list RS, št. 40/06.

5 Uradni list RS, št. 43/11.

6 Uradni list RS, št. 63/07 – uradno

o dostopu do informacij javnega značaja (ZDIJZ),[7] v delu, ki se nanaša na podatke javnih uslužbencev in javnih funkcionarjev v zvezi z njihovim delovnim razmerjem oziroma opravljanjem funkcije, oziroma na podatke o porabi javnih sredstev, Zakon o sistemu plač v javnem sektorju (ZSPJS).[8]



prečiščeno besedilo, 65/08, 69/08 – ZT-FI-A, 69/08 – ZZavar-E in 40/12 – ZUJF.

7 Uradni list RS, št. 51/06 – uradno prečiščeno besedilo, 117/06 – ZDavP-2, 23/14, 50/14, 19/15 – odl. US, 102/15 in 7/1.

8 Uradni list RS, št. 108/09 – uradno prečiščeno besedilo, 13/10, 59/10, 85/10, 107/10, 35/11 – ORZSPJS49a, 27/12 – odl. US, 40/12 – ZUJF, 46/13, 25/14 – ZFU, 50/14, 95/14 – ZUPPJS15, 82/15, 23/17 – ZDOdv in 67/17.

PRAVICE DELAVCEV TER KJE IN KAKO JIH LAHKO UVELJAVLJATE

Kot delavec imam pravico:

◉ *Člen Splošne uredbe:*

… biti informiran ◉ *členi 12, 13, 14*

Primer: Delavec ima pravico vedeti, katere njegove osebne podatke vodi delodajalec (npr. evidenca prisotnosti v službi…).

… do seznanitve z lastnimi podatki ◉ *členi 11, 12, 15*

Primer: Delavec pri delodajalcu poda pisno zahtevo, naj mu pove, katere njegove osebne podatke obdeluje in zahteva kopijo osebne mape.

… do popravka mojih osebnih podatkov ◉ *člen 16*

Primer: Delavec opozori delodajalca, da ima o njem napačno davčno številko, da je spremenil stalno prebivališče, priimek ob poroki ipd.

… do izbrisa mojih osebnih podatkov (»pravica do pozabe«) ◉ *člen 17*

Primer: Delavec zahteva, da delodajalec odstrani njegovo fotografijo s spletne strani, če v objavo ni privolil ali je svojo privolitev umaknil.

… do omejitve obdelave mojih osebnih podatkov ◉ *člen 18*

Primer: Do ugotovitve o spremembi delavčevega priimka delavec zahteva, da delodajalec ne posreduje njegovih podatkov za potrebe izdelave potrdila o izobraževanju.

… do prenosljivosti mojih osebnih podatkov ◉ *člen 20*

Primer:Če želite svoje podatke prenesti k drugemu upravljavcu v strojno berljivi obliki, lahko uveljavljate pravico do prenosljivosti podatkov. Prenos lahko zahtevate, kadar vaše podatke delodajalec obdeluje z avtomatiziranimi sredstvi na podlagi vaše privolitve oziroma zaradi pogodbe.

… do ugovora obdelavi mojih osebnih podatkov ◉ *člen 21*

Primer: Delodjalec je objavil celoten življenjepis zaposlenega na spletni strani, delavec pa temu ugovarja, ker je v njem tudi njegov rojstni datum.

… do ugovora v primeru avtomatiziranih odločitev ◉ *člen 22*

Primer: Kandidat za zaposlitev lahko ugovarja avtomatizirani odločitvi delodajalca, če odločitev o izpolnjevanju pogojev (npr. glede št. let izkušenj in drugih formalnih pogojev) temelji zgolj na avtomatizirani odločitvi.

… do obveščenosti v primeru kršitve varstva osebnih podatkov. ◉ *člen 34 v povezavi s členom 33*

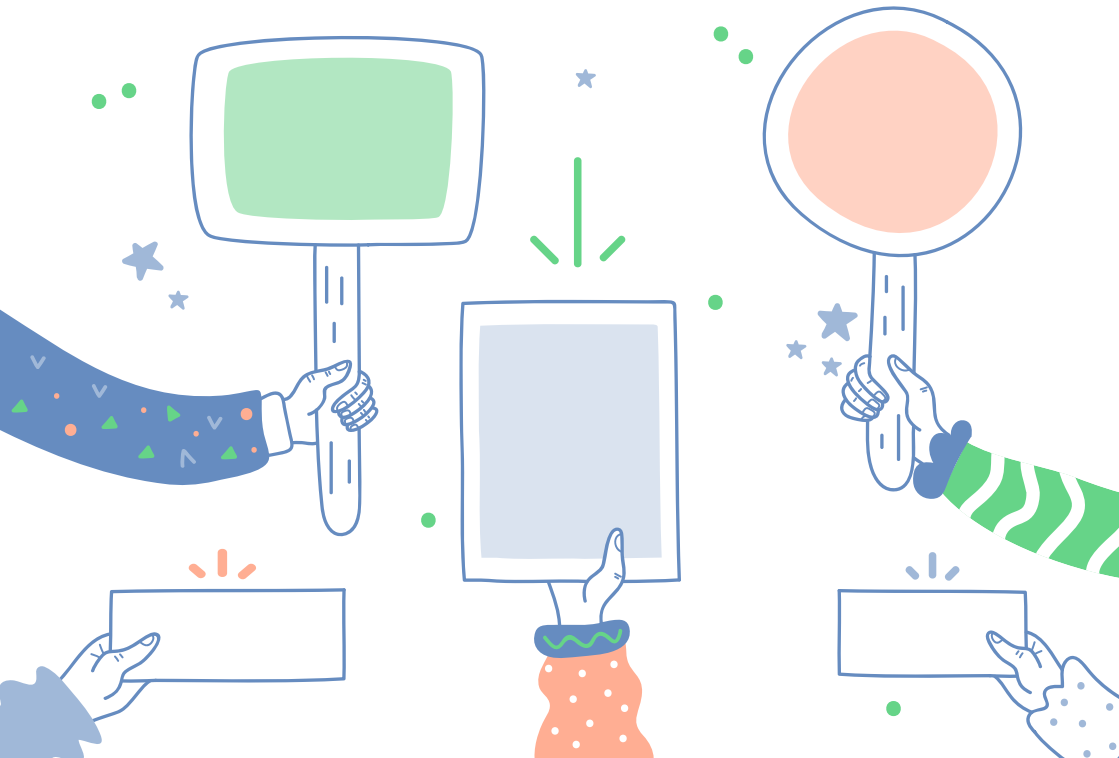
Primer: Delavec ima pravico vedeti, ali je prišlo do nepooblaščenega dostopa v elektronsko personalno mapo

KJE in KAKO lahko uveljavljam svoje pravice?

Zahtevo naslovim na svojega delodajalca, ki mora odločiti **v roku 1 meseca** od njenega prejema. Če ne dobim odgovora v enomesečnem roku ali če delodajalec zavrne mojo zahtevo, lahko pri Informacijskem pooblaščencu (v nadaljevanju IP) vložim **pritožbo**.

Obrazci:

- ➔ Zahteva za seznanitev z lastnimi osebnimi podatki
- ➔ Pritožba zaradi kršitve pravice do seznanitve z lastnimi osebnimi podatki



KATERE OBVEZNOSTI IMA DELODAJALEC?

Delodajalec je dolžan izvesti **ustrezne tehnične in organizacijske ukrepe,*** da **zagotovi** in da lahko **dokaže**, da **obdelava poteka v skladu s Splošno uredbo**. Ukrepe je dolžan redno pregledovati, dopolnjevati in posodobiti. Dolžnosti delodajalca so odvisne od narave, obsega, okoliščin in namenov obdelave, pa tudi od tveganj za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti.

Načelo odgovornosti

Splošna uredba je prinesla pomembno novost, in sicer **načelo odgovornosti**, ki pravi, da je **upravljavec odgovoren za skladnost z vsemi splošnimi načeli in je to skladnost zmožen tudi dokazati**. Načelo odgovornosti od delodajalca zahteva, da je ozaveščan o varstvu osebnih podatkov, da vsako odločitev o obdelavi osebnih podatkov tehtno in skrbno premisli, da vnaprej razmisli, kako bo osebne podatke varoval in na kakšen način bo omogočal izvrševanje pravic delavcem. Splošna uredba od delodajalca torej zahteva **proaktivnost in preventivno ravnanje**.

*** Tehnični in organizacijski ukrepi** lahko vključujejo izvajanje ustreznih politik (internih predpisov) za varstvo podatkov s strani delodajalca (npr. Politika o režimu gesel, Politika o upravljanju varnostnih incidentov, itd.), kadar je to sorazmerno glede na dejavnost obdelave (npr. večja podjetja, z velikim številom zaposlenih, kjer se obdelujejo večje količine podatkov).

Delodajalec ima naslednje obveznosti:

- zagotoviti ustrezno pravno podlago,
- o obdelavi na ustrezen način obvestiti zaposlenega,
- izvajati vgrajeno in privzeto varstvo osebnih podatkov,
- zagotoviti evidenco dejavnosti obdelav,
- zagotoviti varnost osebnih podatkov,
- zagotoviti ustrezno pogodbo, če obdelavo izvajo zunanji izvajalci,
- obvestiti IP in delavce v primeru kršitve varstva osebnih podatkov.

Nadzorni organ

Inšpekcijski nadzor nad določbami Splošne uredbe izvaja **Informacijski pooblaščenec**. Prijavo zaradi kršitev določb Splošne uredbe lahko podate na gp.ip@ip-rs.si, oz. po pošti. Pri tem lahko uporabite ustrezen obrazec IP. Več o prijavi kršitev si lahko preberete na spletni strani IP.

Ustrezna pravna podlaga

Delodajalec sme obdelovati osebne podatke delavcev le, če obstaja ena izmed spodaj naštetih pravnih podlag, sicer je obdelava nezakonita. Dopustne pravne podlage opredeljuje **člen 6(1) Splošne uredbe.**

Izvajanje pogodbe o zaposlitvi oz. o delu (oz. izvajanje ukrepov na zahtevo posameznika pred sklenitvijo pogodbe (npr. kandidata za zaposlitev)

6(1)(b)

Primer: Za izvajanje pogodbe o delu šoferja je delodajalec upravičen do podatkov iz njegovega vozniškega dovoljenja.

Obveznosti, ki izhajajo iz delovnopravne zakonodaje

6(1)(c)

Primer: Delodajalec je dolžan na podlagi ZDR-1 voditi evidenco delovnega časa delavca.

Primer: Za izvajanje pogodbe o delu delodajalec potrebuje št. bančnega računa delavca, na katerega mu bo nakazal plačilo za opravljeno delo.

Zaščita življenjskih interesov delavca ◉ *6(1)(d)*

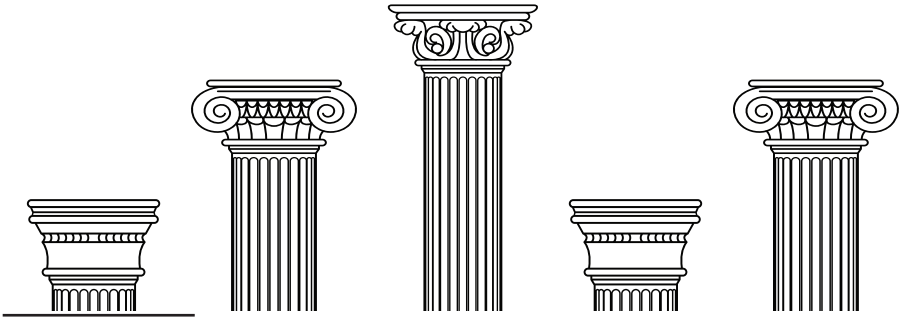
Primer: Ob izgubi zavesti zaposlenega na delovnem mestu zaradi nujnega ukrepanja delodajalec poizve pri sodelavcih o morebitnih pomembnih zdravstvenih težavah zaposlenega.

Opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti ◉ *6(1)(e)*

Primer: Delodajalec lahko zbira in obdeluje podatke udeležencev na dogodku v njegovi organizaciji, kjer so tudi zaposleni, sama vsebina dogodka pa sodi v področje dela, za katerega je pristojen.

Zakoniti interes, za katerega si prizadeva delodajalec ali tretja oseba (razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, ki zahtevajo varstvo osebnih podatkov)[9] ◉ *6(1)(f)*

Primer: Zaradi varovanja svojega omrežja delodajalec za omejen čas hrani podatke o dostopih do spletnih strani s službenih računalnikov.



9 Pravna podlaga zakonitega interesa, določena v členu 6(1)(f) se ne uporablja za obdelavo s strani javnih organov pri opravljanju njihovih nalog – te naloge morajo biti določene v zakonodaji – v tem primeru prideta v poštev pravni podlagi člena 6(1)(c) ali 6(1)(e).

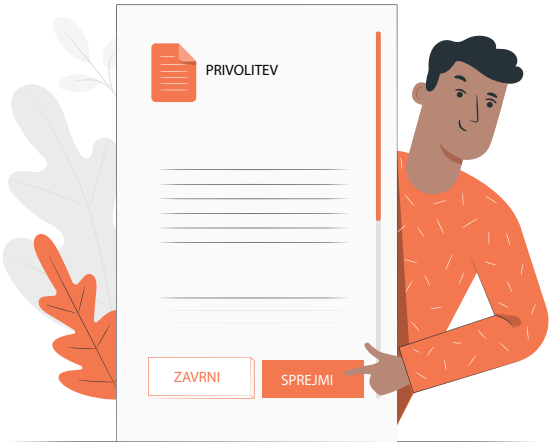
Privolitev zaposlenega – le izjemoma! Biti mora prostovoljna, neizsiljena, informirana in dokazljiva. Posameznik se lahko prostovoljno odloči, ali bo delodajalcu dovolil obdelavo ali ne in ne trpi negativnih posledic, če ne poda privolitve.

◉ *6(1)(a)*

POZOR! Privolitev za večino primerov obdelave ne more in ne sme biti pravna podlaga, in sicer zaradi posebnega odnosa med delodajalcem in delavcem, ki je praviloma šibkejša stran v tem razmerju. Če želi delodajalec zagotoviti, da bo privolitev zakonita, mora dokazati, da je ta prostovoljna, izrecna, informirana in nedvoumna izjava volje delavca, s katero je z izjavo ali jasnim pritrdilnim dejanjem izrazil strinjanje z obdelavo osebnih podatkov, ki se nanašajo nanj. To bo največkrat izjemno težko dokazati, saj se delavec običajno čuti dolžnega, da privoli v obdelavo, zaradi morebitnih neželenih ali neprijetnih posledic v zvezi z njegovim delovnim razmerjem.

Podrobnejše informacije:

- ➔ Smernice o privolitvi
- ➔ Smernice o privolitvi, dopolnjene s privolitvijo v primeru »piškotkov« (angl.)



O obdelavi obvestiti delavca na ustrezen način

◉ *člena 13 in 14 Splošne uredbe*

Delavcu morajo biti vse informacije, ki se nanašajo na obdelavo njegovih osebnih podatkov lahko dostopne, razumljive in izražene v jasnem in preprostem jeziku.

Obrazci:

➔ Vzorec obvestila posameznikom glede obdelave osebnih podatkov (člen 13 Splošne uredbe)

➔ Vzorec obvestila posameznikom glede obdelave osebnih podatkov (člen 14 Splošne uredbe)

Podrobnejše informacije:

➔ Smernice o preglednosti na podlagi Uredbe (EU) 2016/679

POZOR! Delodajalci pogosto neustrezno združujejo tri različne vrste dokumentov:

1. obvestilo delavcu glede obdelave njegovih osebnih podatkov,
2. izjavo delavca, da je seznanjen z obdelavo osebnih podatkov in politikami delodajalca, in
3. privolitev za obdelavo osebnih podatkov.

... v skupen dokument, ki ga delavec »mora podpisati«. Gre za tri različne dokumente, ki jih je treba razlikovati med seboj.

Izvajati vgrajeno in privzeto varstvo osebnih podatkov ves čas obdelave

◉ *člen 25 Splošne uredbe*

Vgrajeno varstvo osebnih podatkov od delodajalca zahteva, da že v najzgodnejše faze priprav na obdelavo (»vgrajeno«) vključi tehnične in organizacijske ukrepe, ki zagotavljajo učinkovito izvajanje načel varstva podatkov.

Primer: *Uporaba psevdonimizacije (nadomeščanje EMŠO, davčne številke z umetnimi identifikatorji) in šifriranja (kodiranja sporočil, da jih lahko preberejo samo pooblaščene osebe).*

Podrobnejše informacije:

➔ Smernice o členu 25 Splošne uredbe - vgrajeno in privzeto varstvo podatkov (angl.)

Zagotoviti evidenco dejavnosti obdelav

◉ *člen 30 Splošne uredbe*

Delodajalec mora svoje zbirke osebnih podatkov popisati (ustvariti katalog), z namenom, da se zaveda, katere osebne podatke sploh ima, na kakšni podlagi jih obdeluje, za katere namene, kje se nahajajo itd. Skrbno dokumentiranje procesov obdelav delodajalcu pomaga pri izkazovanju skladnosti s Splošno uredbo. S tem delavcu nudi boljšo obveščenost o tem, kaj o njem ve in zakaj.

Obrazci:

➔ Vzorca evidence dejavnosti obdelave za upravljavce in obdelovalce

Zagotoviti varnost osebnih podatkov

◉ *člen 32 Splošne uredbe, 24. in 25. člen ZVOP-1*

Delodajalec mora s tehničnimi in organizacijskimi postopki in ukrepi preprečiti, da bi osebni podatki prišli v roke nepooblaščenim osebam, se nepooblaščeno uporabljali, brisali, spreminjali ali izgubili.

Primer: *Delodajalec mora poskrbeti, da so npr. kadrovske mape zaposlenih varne, to pa zagotovi z zaklepanjem omar in prostorov, z uporabo primerne politike gesel za dostop v kadrovske aplikacije, z ozaveščanjem zaposlenih v kadrovski službi, z uporabo tehničnih ukrepov, kot so požarni zidovi, protivirusni programi ipd.*

Podrobnejše informacije:

➔ Smernice o zavarovanju osebnih podatkov

Zagotoviti ustrezno pogodbo, če obdelavo izvajajo zunanji izvajalci

◉ *člen 28 Splošne uredbe*

Kadar obdelavo osebnih podatkov v imenu upravljavca izvaja obdelovalec, mora za to obstajati pisna pogodba ali drug ustrezen akt. Pogodba je potrebna, da obe stranki poznata svoje obveznosti in odgovornosti, ki iz tega izhajajo.

Podrobnejše informacije:

➔ Smernice Informacijskega pooblaščenca o (pogodbeni) obdelavi osebnih podatkov

Obvestiti IP in delavce v primeru kršitve varstva osebnih podatkov

◉ *člen 33 in 34 Splošne uredbe*

Delodajalec mora obvestiti IP o zaznanih kršitvah varnosti osebnih podatkov, če je verjetno, da bi bile s kršitvijo ogrožene pravice in svoboščine posameznikov. Obvestilo je treba podati takoj po zaznani kršitvi, najkasneje pa v 72 urah. Kadar je verjetno, da kršitev varnosti osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, mora upravljavec kršitev sporočiti tudi posamezniku, na katerega se nanašajo osebni podatki.

Podrobnejše informacije:

➔ Smernice v zvezi z uradnim obvestilom o kršitvi varnosti osebnih podatkov

➔ Infografika: Prijava kršitve varnosti

Primer: *Če delodajalec izgubi delavčeve osebne podatke (npr. na USB ključu), pride do kršitve varnosti osebnih podatkov. Če oceni, da bi bile lahko ogrožene pravice in svoboščine delavcev (npr. na USB so podatki o imenu, priimku in nazivu delovnega mesta delavcev), mora o kršitvi najkasneje v 72 urah obvestiti IP. Če kršitev predstavlja veliko tveganje za pravice in svoboščine delavcev (npr. na USB ključu so podatki delavcev, ki se uporabljajo za izplačilo plač), mora o kršitvi obvestiti tudi njih.*

Imenovati pooblaščeno osebo za varstvo osebnih podatkov (»DPO«)

◉ *členi 37, 38, 39 Splošne uredbe*

DPO deluje kot notranji revizor za varstvo osebnih podatkov, njegove glavne naloge pa so: spremljanje skladnosti s Splošno uredbo, svetovanje delodajalcu o njegovih obveznostih, izobraževanje in ozaveščanje delavcev.

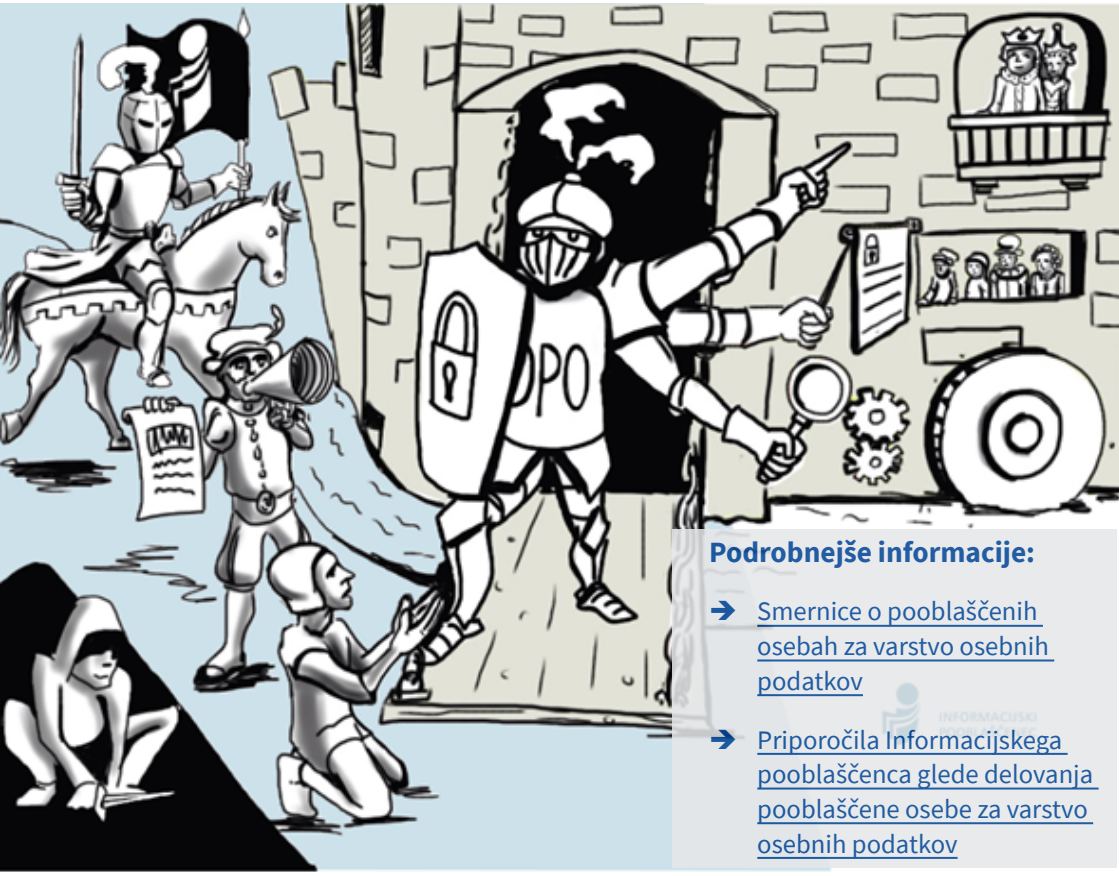
Obrazec:

➔ Obvestilo o imenovanju pooblaščene osebe za varstvo osebnih podatkov

POZOR! Kdaj se lahko kot zaposleni obrnem na pooblaščeno osebo za varstvo podatkov v našem podjetju? Na primer:

1. ko menim, da določeno ravnanje ali postopek ni skladen z zakonodajo o varstvu podatkov (npr. interna politika podjetja, obrazec za zbiranje osebnih podatkov ipd.);
2. če je prišlo do kršitve mojih osebnih podatkov v okviru delodajalca;
3. če bi rad več izvedel o pravilih glede varstva osebnih podatkov.

DPO ima dolžnost varovati informacije kot zaupne.



Podrobnejše informacije:

- Smernice o pooblaščenih osebah za varstvo osebnih podatkov
- Priporočila Informacijskega pooblaščenca glede delovanja pooblaščene osebe za varstvo osebnih podatkov

OBDELAVA OSEBNIH PODATKOV S SODOBNIMI TEHNOLOGIJAMI

S pomočjo sodobnih tehnologij lahko delodajalci nadzirajo zaposlene tako na delovnem mestu kot tudi pri delu od doma. Tehnologije, kot so npr. GPS, videonadzor, biometrija, aplikacije za pomoč za delo od doma, odpirajo vrsto vprašanj glede zasebnosti na delovnem mestu. Za razliko od klasičnih načinov nadzora se tak nadzor namreč lahko izvaja prikrito.

Z izjemo videonadzora in biometrije ter nadzora nad porabo na službenih telefonih navedena področja še niso zakonsko urejena. Pri ugotavljanju, ali je takšen nadzor upravičen, je zato treba izhajati iz splošnih načel sorazmernosti in zakonitosti.

Delodajalec je pred uvedbo tovrstnega nadzora dolžan:

- **razmisliti o namenu, ki ga želi doseči (kaj želi z nadzorom urediti oz. katero težavo želi rešiti),**
- **razmisliti, ali je ukrep potreben (ali se da isti cilj doseči na manj invaziven način) in sorazmeren glede na namen,**
- **izbrati najustreznejšo pravno podlago.**

OBDELAVE OSEBNIH PODATKOV PRED ZAPOSLITVIJO

Katere podatke lahko delodajalec zbira od kandidata za zaposlitev?

Delodajalec lahko od kandidata za zaposlitev zahteva le tiste osebne podatke, ki mu pomagajo ugotoviti, ali kandidat izpolnjuje **pogoje** za delovno mesto in ali ima zahtevana **znanja in izkušnje**.

Delodajalec pri sklepanju pogodbe o zaposlitvi od kandidata ne sme zahtevati podatkov o družinskem oziroma zakonskem stanu, o nosečnosti, o načrtovanju družine oziroma drugih podatkov, če niso neposredno povezani z delovnim razmerjem. Pri obdelavi osebnih podatkov kandidatov mora delodajalec prav tako upoštevati načelo najmanjšega obsega podatkov (to pomeni, da v fazi razgovora še ne potrebuje kandidatove davčne številke, EMŠO ali podatka o številu otrok).

Podrobnejše informacije:

➔ Smernice IP: Varstvo osebnih podatkov v delovnih razmerjih (z vključenimi primeri obdelave osebnih podatkov kandidatov pred zaposlitvijo)

Ali lahko zbira osebne podatke kandidatov z družabnih omrežij (Facebook, Twitter, Youtube itd.)?

Delodajalec sme obdelovati le tiste osebne podatke z družabnih omrežij, ki jih potrebuje za presojo, ali kandidat izpolnjuje pogoje za zasedbo delovnega mesta.

Podatki, ki jih objavimo na družabnih omrežjih, so naši osebni podatki. Njihova uporaba lahko pomeni poseg v našo zasebnost. Ali gre za poseg ali ne, je odvisno tudi od naših nastavitev zasebnosti.

Če je naš **profil »javen«** (in lahko naše fotografije, komentarje in sezname prijateljev vidi vsakdo),

potem kandidat ne more pričakovati popolne zasebnosti. Če si delodajalec pred razgovorom ogleda naše fotografije ali komentarje, je težko trditi, da gre za neupravičen poseg v našo zasebnost, saj bi si jih lahko ogledal kdorkoli. **Vpogled in pridobitev fotografij z javnega profila zato praviloma ne pomeni kršitve osebnih podatkov**. Kljub temu pa delodajalec naših podatkov ne sme uporabiti za kakršen koli namen (npr. za vzpostavitev nove zbirke osebnih podatkov).

Kaj pa v primeru "zaprtega profila"?

Položaj je seveda drugačen, kadar ima kandidat **t. i. zaprti profil**. Če bi delodajalec pod krinko izmišljenega profila (ali preko katerega od naših prijateljev) prišel do naših fotografij ali všečkanih strani, bi to lahko predstavljalo kršitev naše zasebnosti. Vendar pa, če smo delodajalca sami (z njegovo pravo identiteto) dodali med svoje prijatelje in mu omogočili dostop do podatkov na našem (sicer zaprtem) profilu, uporaba teh podatkov največkrat ne pomeni kršitve zasebnosti. Dobro je vedeti, da lahko npr. na Facebooku osebi omejimo dostop do svojih objav tudi takrat, ko gre za našega prijatelja. Delodajalca lahko torej dodate med prijatelje, vendar mu hkrati omejite dostop do svojih objav. Na ta način bo videl le tisto, kar je označeno kot »javno«.

OBDELAVE OSEBNIH PODATKOV NA DELOVNEM MESTU

Za vse v tem poglavju navedene vrste obdelav velja, da je zakonodaja zelo ohlapna ali je sploh ni, zato mora delodajalec skrbno presojati, ali obdelava podatkov morebiti že posega v pravico do zasebnosti delavca in je tako lahko nezakonita. Krhko ravnovesje bo delodajalec lahko ujel s pomočjo naslednjih **skupnih priporočil:**

◉ delodajalec naj izvede oceno učinka

V okviru ocene učinka naj delodajalec natančno **opredeli namen**, za katerega bi bilo treba posegati v e-pošto delavca, spremlja obiskanost spletnih strani, izvaja videonadzor nad zaposlenimi itd., **izvede oceno potrebnosti in sorazmernosti** dejanj obdelave glede na opredeljeni namen, **oceno tveganj** za posameznike (delavce) in določi **ukrepe za obravnavanje tveganj**);

◉ vnaprej določi pravno podlago

Za vsako vrsto obdelave osebnih podatkov (npr. poseg v e-pošto, izvajanje nadzora nad tiskalniki itd.) je treba **določiti najustreznejšo pravno podlago**, določeno v členu 6(1) Splošne uredbe in upoštevati morebitno podlago, določeno v ZVOP-1 (videonadzor, biometrija) ali drugi področni zakonodaji;

◉ zagotovi predvidljivost za primere nadzora

Primere obdelav, ki lahko pomenijo nadzor nad zaposlenimi in s tem poseg v zasebnost delavcev, bi moral delodajalec **navesti v internem aktu in z njim seznaniti vse zaposlene**;

◉ raje vnaprej omeji kot nadzira

Delodajalec lahko **s tehničnimi sredstvi omeji** uporabo npr. e-pošte ali interneta na način, da bo zadostil namenu, ki ga zasleduje (npr. omejitev pošiljanja priponk nad določeno velikostjo, omejitev velikosti samega poštnega predala itd.).

Elektronska pošta in internet

Nerazumno je pričakovati, da bo delavec službeno e-pošto in internet uporabljal zgolj za službene namene, zato je treba mejo med posegi v pravico do zasebnosti delavca in pravico nad delovnimi sredstvi delodajalca določiti z ustreznimi organizacijskimi in tehničnimi ukrepi. Tudi podatek o tem, katere spletne strani si je delavec ogledal, je osebni podatek delavca, zato mora biti obdelava takšnih podatkov sorazmerna in zakonita.

Pri uporabi e-pošte ločimo **varstvo osebnih podatkov** (to so prometni podatki, kot npr. elektronski naslovi, datum in čas sporočila, prejemnik, zadeva, velikost priponke) in **širšo pravico do zasebnosti**, tajnosti občil in osebnostnih pravic. Varstvo osebnih podatkov tako varuje podatek o tem, kdo je poslal elektronsko sporočilo in kdaj, vsebino samega sporočila pa lahko posameznik varuje v kazenskih in civilnih postopkih pred sodiščem.

Podrobnejše informacije:

➔ Varstvo osebnih podatkov v delovnih razmerjih

Telefon

Delodajalci smejo z namenom nadzora nad porabo na službenem telefonu spremljati porabo s strani delavca, lahko pa spremljajo tudi vsebino telefonskega pogovora s stranko (z namenom zagotavljanja kakovosti storitve, nudene po telefonu).

Zakon o elektronskih komunikacijah (ZEKom-1),[10] ki določa pravico delodajalca do pridobivanja razčlenjenih telefonskih računov in seznama klicanih številk, ureja tudi zaupnost komunikacij in dopustnost snemanja telefonskih klicev.

Podrobnejše informacije:

➔ Smernice o snemanju telefonskih klicev

10 Zakon o elektronskih komunikacijah (Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17)

Tiskalniki in podobne naprave (npr. skenerji)

Večina tiskalnikov, skenerjev in multifunkcijskih naprav samodejno shranjuje nekatere podatke o tiskanju in skeniranju (tiskalnik lahko shrani vaše uporabniško ime, ime natisnjene datoteke, status tiskanja, število natisnjenih strani), ki predstavljajo zbirko osebnih podatkov. Če delavec natisne svoj zdravniški izvid, lahko iz imena datoteke delodajalec sklepa o zdravstvenem stanju delavca.

Podrobnejše informacije:

➔ Varstvo osebnih podatkov v delovnih razmerjih

Videonadzor

Videonadzor pomeni enega najhujših posegov v zasebnost, saj močno vpliva na vedenje posameznikov in ima lahko dolgoročne posledice na spremembo njihovega obnašanja.

Delodajalec mora o videonadzoru obvestiti posameznike in sistem zavarovati pred dostopom nepooblaščenih oseb. Obvestilo o videonadzoru mora biti na vidnem mestu, kjer se izvaja videonadzor. Videonadzor dostopa v službene ali poslovne prostore (npr. vhodna avla) se lahko izvaja zaradi varnosti ljudi ali premoženja, za nadzor vstopa ali izstopa v prostore oz. če zaradi narave dela obstaja možnost ogrožanja zaposlenih. Izvajanje videonadzora znotraj delovnih prostorov (npr. v pisarnah ali v obratu) je dovoljeno le v izjemnih primerih (če je nujno treba zaradi varnosti ljudi ali premoženja).

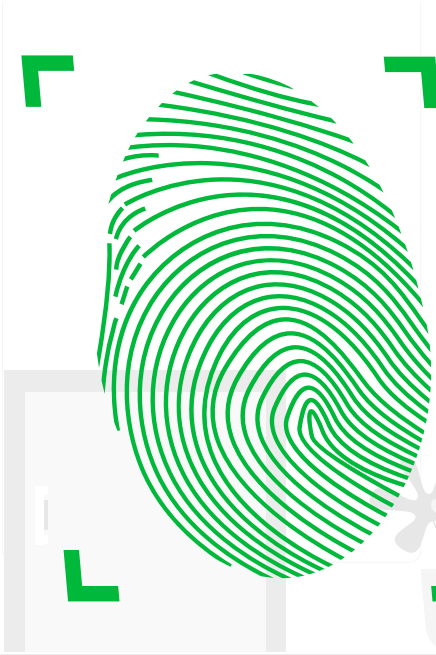
Podrobnejše informacije:

➔ Smernice Informacijskega pooblaščenca glede izvajanja videonadzora.

Biometrija

Nevarnosti

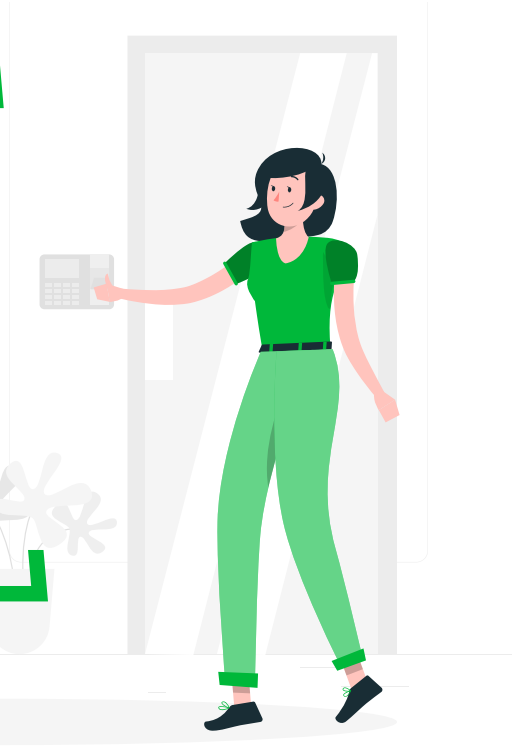
Uporaba sredstev za biometrično identifikacijo posameznika predstavlja zelo velik poseg v informacijsko zasebnost posameznika (delavca), saj se z biometrijo obdelujejo tiste značilnosti posameznika, ki so edinstvene in stalne za vsakega posameznika posebej. Njihova zloraba ima lahko za posameznika hude, daljnosežne in nepopravljive posledice. Za razliko od »običajnih« načinov avtentikacije oziroma identifikacije, kjer je možna relativno enostavna menjava in pridobitev novega znaka (geslo, PIN-koda), je menjava biometrijskih značilnosti (obraz, prstni odtis, mrežnica, šarenica) praktično nemogoča. Zato je zakonodajalec uvedbo biometrijskih ukrepov strogo omejil na tiste okoliščine, kjer je njihova uporaba nujno potrebna in kjer istih ciljev ni mogoče doseči z drugimi sredstvi, ki manj posegajo v informacijsko zasebnost posameznika. Splošna uredba določa biometrične podatke kot osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki. Sodijo med posebne vrste osebnih podatkov, za obdelavo katerih so predvideni posebni pogoji obdelave.



ZVOP-1 dovoljuje uporabo biometrije le v naslednjih primerih:

javni sektor:

le kadar tako določa zakon (npr. Zakon o potnih listinah), če je to nujno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi, izjemoma na podlagi posebnih zakonskih določil tudi za vstop v stavbo ali dele stavb in evidentiranje zaposlenih pri delu;



zasebni sektor:

sme izvajati biometrijske ukrepe le nad svojimi zaposlenimi, če jih o tem predhodno obvesti in če je za izvajanje teh ukrepov predhodno pridobil odločbo Informacijskega pooblaščenca (če ni določeno z zakonom).

Podrobnejše informacije:

➔ Smernice glede uvedbe biometrijskih ukrepov (smernice IP)

OBDELAVE OSEBNIH PODATKOV IZVEN DELOVNEGA MESTA

Delo na daljavo, delo od doma

Delo na daljavo in delo od doma je v zadnjih nekaj letih postalo vse bolj priljubljena možnost za delodajalce, saj zaposlenim omogoča, da ostanejo povezani in učinkoviti tudi, ko niso v pisarni. Ta oblika dela po eni strani predstavlja pozitiven razvoj z vidika učinkovitosti in ekonomičnosti poslovanja, pomeni pa tudi področje dodatnega tveganja za delodajalca. Zaposleni, ki imajo dostop do informacijske infrastrukture delodajalca z daljave ali od doma, namreč niso podvrženi fizičnim varnostnim ukrepom (senzorska vrata, videonadzorne kamere itd.), poveča pa se tudi možnost nepooblaščenega dostopa do podatkov na napravi (prenosni računalnik, tablica, službeni telefon), ki se ne nahaja v prostorih delodajalca. V takih okoliščinah je torej pomembno **zagotavljati ustrezno varnost osebnih podatkov**.

Brez izvajanja ustreznih tehničnih in organizacijskih ukrepov se tveganje za kršitev varnosti osebnih podatkov poveča, poveča pa se tudi možnost, da delodajalec prekorači svoje pristojnosti in poseže v zasebnost delavca. **Ključno je, da se tveganja obravnavajo sorazmerno in zakonito**.

Informacijski pooblaščenec priporoča, da delodajalci vnaprej predvidijo vsa morebitna tveganja, ustrezne organizacijske in tehnične ukrepe navedejo **v svojih internih aktih** in z njimi seznanijo svoje zaposlene.

V vsakem primeru morajo delodajalci:

- **vpeljati in posodabljati vse varnostne mehanizme** na napravah, ki jih delavec uporablja (antivirusni program, šifrirana naprava, požarni zidovi, filtriranje internetnega prometa, sistem za prevencijo in zaznavanje nepooblaščenega dostopa);

- **zavarovati prenosnike** in **mobilne telefone** z ustrezno **avtentikacijo** (gesla, SecureID kartice ...);
- **opozarjati** delavce na pazljivost pred **nepooblaščenim dostopom** (zaklepanje ekrana po določenem času neuporabe ...);
- **vpeljati** in **izvajati politiko močnih gesel**;
- ustrezno **šifrirati** vso **komunikacijo** (e-pošta, internet, telefon ...) in informirati zaposlene, da uporaba zasebne e-pošte ni priporočljiva;
- **pred uporabo pregledati vse odstranljive naprave** (USB ključki, zunanji diski ...), da ne vsebujejo **škodljivih ali zlonamernih programov** (črvi, virusi, trojanski konji ...);
- **pri uporabi avdio in video klicev** (namesto fizičnih sestankov) **preveriti varnost** posamezne **aplikacije** in priporočiti delavcem uporabo **preverjenih programov**;
- **zagotavljati varnost tudi na klasičnih medijih** (npr. papirju).

GPS sledilne naprave

Številna podjetja in institucije uporabljajo GPS za različne namene, kot je sledenje tovornjakom, delovnim strojem, taksijem in drugim službenihm vozilom, za optimizacijo voznih parkov, obračun službenih poti idr. Lociranje vozil in ljudi pomeni obdelavo osebnih podatkov. Zakonodaja z vidika obdelave osebnih podatkov uporabe GPS sledilnih naprav posebej ne ureja, zato je treba pri uporabi GPS naprav spoštovati temeljna načela varstva osebnih podatkov – presoditi, pod kakšnimi pogoji bi bila uporaba sledilnih naprav sorazmerna ter zakonita in upoštevati ostala načela (poštenost, transparentnost, zavarovanje, namenskost, pravice posameznika itd.).

Podrobnejše informacije:

➔ Smernice Informacijskega pooblaščenca o uporabi GPS sledilnih naprav in varstvu osebnih podatkov

Uporaba zasebnih naprav v službene namene (BYOD)

Prednosti in slabosti

Množična uporaba moderne tehnologije, težnja delodajalcev k večji produktivnosti in želja delavcev po delu izven delovnega mesta in izven delovnega časa, so pripeljali do tega, da zaposleni čedalje pogosteje uporabljajo tudi svoje zasebne naprave (prenosnike, pametne telefone, tablice) v službene namene (t. i. koncept »Bring Your Own Device«, BYOD). Takšno delo prinaša delodajalcem (in predvsem njihovim IT delavcem) velik izziv na področju zagotavljanja varnosti v informacijskem sistemu, do katerega dostopajo zaposleni preko svojih naprav. Hkrati takšno delo predstavlja tudi izziv z vidika zasebnosti delavca, saj njegove naprave vsebujejo številne osebne podatke. Pri uporabi zasebnih naprav v službene namene je treba upoštevati določbe Splošne uredbe glede pravnih podlag in temeljnih načel obdelave osebnih podatkov.

Delodajalec je dolžan ves čas nadzirati podatke, vendar je to skoraj nemogoče, če nima v lasti naprave, s katero delavec dostopa do podatkov ali jih shranjuje.

Priporočili:

1. da delavec pri uporabi mobilnih telefonov in drugih informacijskih sredstev **ločuje poslovni (službeni) način delovanja od zasebnega**,

2. da so **varnostni postopki in ukrepi vnaprej opredeljeni** v internih aktih delodajalca.

Pravna podlaga za obdelavo osebnih podatkov

Ker **neposredna zakonska podlaga** za uporabo BYOD v nacionalni zakonodaji **ne obstaja**, je treba to izpeljati iz naslednjih podlag:

- **zakon**

  Možnost dela od doma ureja ZDR-1. Delavec in delodajalec morata pravice, obveznosti in pogoje dela od doma urediti s pogodbo o zaposlitvi. Morata se dogovoriti za nadomestilo za uporabo lastnih sredstev v službene namene, lahko se pa dogovorita, da bo delavec preusmeril službene klice na svoj mobilni telefon (v tem

primeru ima delodajalec pravico obdelovati zasebno telefonsko številko delavca);

- **javni interes ali izvajanje javne oblasti**

V primeru naravnih ali drugih nesreč oz. v drugih izjemnih okoliščinah, ko je ogroženo življenje in zdravje ljudi ali premoženje delodajalca, se lahko vrsta ali kraj opravljanja dela, določenega s pogodbo o zaposlitvi, začasno spremenita tudi brez soglasja delavca. Sprememba lahko traja le, dokler trajajo take okoliščine.

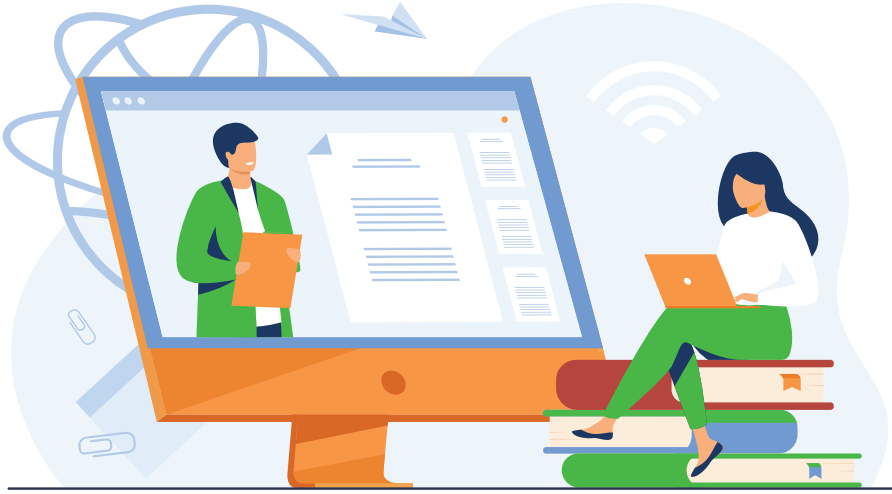
- **privolitev zaposlenega**

Privolitev zaposlenega mora biti popolnoma prostovoljna, informirana, dokazljiva – delodajalec ga ne sme prisiliti v uporabo zasebnih sredstev v službene namene. Zaposleni lahko brez posledic zavrne takšno delo.

Zaradi obdelave osebnih podatkov pri delu na lastnih napravah delavca mora delodajalec **prilagoditi svoje interne akte.**

Podrobnejše informacije:

➔ Smernice o uporabi zasebnih naprav v službene namene



VARSTVO OSEBNIH PODATKOV V ČASU IZREDNIH RAZMER ZARADI EPIDEMIJE KORONAVIRUSA COVID-19

Širjenje epidemije koronavirusa (COVID-19) je večino delodajalcev prisililo v spremembo delovnega procesa, predvsem z izvajanjem različnih oblik dela na daljavo. Uporaba različnih storitev in sistemov, kot so oddaljeni dostop zaposlenih do različnih strežnikov (poštni, datotečni ipd.), aplikacij (npr. spletni klepetalniki) in sistemov (npr. videokonference), prinaša številna vprašanja z vidika pravnih podlag obdelave osebnih podatkov in njihove varnosti.

Podrobnejše informacije:

➔ Vsa aktualna stališča in mnenja v zvezi z varstvom osebnih podatkov v času izrednih razmer zaradi koronavirusa COVID-19.

Ker je v času širjenja okužb s COVID-19 ogroženo tako zdravje posameznika kot javno zdravje, posebne okoliščine lahko terjajo ukrepe, ki posegajo tudi na področje obdelave posebnih vrst osebnih podatkov (npr. podatkov o zdravstvenem stanju). Ukrepi, ki sicer pomenijo obdelavo zdravstvenih osebnih podatkov delavcev, so hkrati lahko namenjeni tudi zaščiti življenjskih interesov zaposlenih, zakonitih interesov podjetij in tudi v javnem interesu. Vendar pa gre za vprašanje, na katero mora primarno podati odgovor zdravstvena stroka, zlasti pooblaščena oseba za medicino dela, s katero naj se delodajalec posvetuje pred uvajanjem konkretnega ukrepa obdelave zdravstvenih podatkov zaposlenih in drugih oseb.

Ali lahko delodajalec meri in spremlja telesno temperaturo zaposlenih ob prihodu na delo preko IR sistema ali termo kamer?

Za delodajalce, ki razmišljajo o uvedbi merjenja ali spremljanja temperature zaposlenih, **je priporočljivo:**

- da **se posvetujejo s predstavniki medicinske stroke,** ali je tovrstno merjenje nujno in upravičeno, v kakšnem obsegu naj se izvaja in v kakšnem obsegu se podatki lahko hranijo;
- da **izvedejo oceno učinkov** glede varstva osebnih podatkov;
- če se bo to izvajalo, je **treba zaposlene o tem ustrezno obvestiti**, prav tako pa je treba upoštevati vsa **temeljna načela varstva osebnih podatkov** in zagotoviti vse ostale potrebne in ustrezne varovalke, kot so minimizacija in sorazmernost obsega obdelave osebnih podatkov in rokov hrambe, varnost podatkov, skrb za točnost in ažurnost podatkov.

Ko gre (ob merjenju telesne temperature zaposlenim) **hkrati tudi za uporabo biometrijskih ukrepov** (npr. IR kamera, ki meri telesno temperaturo iz daljave, za svoje delovanje pa uporablja tehnologijo prepoznave obraza ter vseskozi spremlja lokacijo

zaposlenega), je treba upoštevati določbe ZVOP-1 glede biometričnih ukrepov. Če se delodajalec odloči za takšno izvajanje merjenja temperature, mora tudi pojasniti (v sklopu ocene učinka), zakaj ne bi zadoščalo že izvajanje merjenja, ki omogoča zgolj »zaznavo« obraza (ko torej ne gre za izvajanje biometrijskih ukrepov).

Ali je v času epidemije dopustno zahtevati od delavca, da delodajalcu sporoči, da se je okužil s koronavirusom?

Praviloma ne. Delavci niso dolžni avtomatično in v vsakem primeru delodajalca obvestiti o okužbi. **Lahko** pa takšno obveznost zaposlenega posamezno podjetje ali organizacija odredi **po presoji pristojnih institucij in pooblaščene osebe za medicino dela** (glede na posebno naravo in organizacijo dela). Če je treba, glede na oceno pooblaščene osebe za medicino dela ali po navodilu pristojnih oblasti (NIJZ), lahko delodajalec zahteva od zaposlenih tudi obveščanje o okužbi.

Če takšna obveznost obstaja, delavcem ni treba podati privolitve, saj pravna podlaga za obdelavo izhaja iz delovnopravne zakonodaje. Kljub temu je treba upoštevati **načelo najmanjšega obsega podatkov** in obdelovati zgolj tiste podatke, ki so nujni za dosego namena. Ta podatek pa mora delodajalec **ustrezno varovati** in ga brez ustrezne pravne podlage ni upravičen posredovati naprej. Načeloma za nadaljnje obveščanje zadoščajo statistični podatki (npr. zgolj podatek o pojavu okužbe v določenem podjetju, razredu, nadstropju ipd.) brez drugih podatkov, ki omogočajo določljivost posameznika.

Ali lahko delodajalec od delavca zahteva, da poda izjavo o nezmožnosti za delo ker pripada rizični skupini delavcev in zahteva od njega, da za to priloži dokazila?

V času epidemije je delodajalec **upravičen od zaposlenega pridobiti izjavo o tem, ali ta (glede na svoje osebno zdravstveno stanje ali zdravstveno stanje članov svojega gospodinjstva) spada v rizično skupino delavcev**, zaradi česar ne more izvajati svojih pogodbenih obveznosti. Vendar pa delodajalec **ni upravičen, da bi od delavca zahteval predložitev dokazil** oz. zdravstvene dokumentacije, iz katere bi bili razvidni konkretni razlogi za delavčevo ogroženost. Le zdravstvena stroka je tista, ki lahko presoja, kateri delavci spadajo v rizično skupino. Delodajalci nimajo znanj, da bi lahko presojali zdravstvene podatke zaposlenih (npr. diagnoza, znaki bolezni ipd.), zato do njih niso upravičeni.

Delodajalec lahko od delavca, ki poda takšno izjavo, kot dokaz zahteva le **običajno zdravniško potrdilo** (ki zgolj potrjuje dejstvo, da delavec spada v rizično skupino) in ga praviloma izda izbrani osebni zdravnik; ali drugo dokazilo, iz katerega niso razvidni konkretni zdravstveni razlogi za uvrstitev v rizično skupino.

Ali delodajalec novinarju (javnosti) lahko razkrije informacije, ali so z virusom okuženi delavci?

Odgovor na to vprašanje ni enoznačen in je odvisen od tega, katere podatke novinar zahteva, od katerega delodajalca (javni ali zasebni sektor), ne nazadnje tudi od velikosti organizacije oziroma podjetja. Sama informacija, da je določeno število zaposlenih okuženih (brez drugih podatkov), ne pomeni obdelave osebnih podatkov, saj posameznik na tak način ni določljiv. Obdelave osebnih podatkov torej ne predstavlja posredovanje statističnih podatkov (za določeno širše območje, za šolo, za posamezen organ ali organizacijo), na podlagi katerih posameznika ni mogoče določiti (torej brez razkrivanja podatka o spolu, starosti, naslovu, ulici, delovnem mestu ipd.)

V primerih, kjer bi bil posameznik na podlagi odgovora novinarju določljiv, praviloma **ni dopustno razkrivati osebnih podatkov posameznikov javnosti**. Izjemoma bi lahko podatek posredovali na podlagi ZDIJZ, če bi bila informacija v interesu javnosti (npr. če bi šlo za absolutno javno osebnost). Te primere je treba presojati posamično, upoštevajoč vse okoliščine konkretnega primera. Izven tega okvira pa delodajalec javnosti ne sme razkriti podatkov (imena, priimka in drugih osebnih podatkov) iz katerih bi bilo mogoče sklepati na določljivega zaposlenega, ki je okužen.

Ali lahko delodajalec v podjetju pove, kdo od sodelavcev je okužen?

Kadar delodajalec meni, da je **obdelava nujna za zaščito življenjskih interesov posameznika, lahko osebni podatek** posreduje sodelavcem neposredno na podlagi Splošne uredbe. Posebna privolitev posameznika se v tovrstnih položajih ne zahteva.

Delodajalec mora glede na navodila prejeta od zdravstvene stroke (NIJZ) in glede na lastno oceno nevarnosti **od primera do primera** presojati in ugotavljati, kateri podatki so potrebni za zaščito življenjskih interesov ljudi, oz. so v zvezi z zagotavljanjem zdravja in varstva pri delu.

Ali je dopustno podpisovanje izjave s strani delavcev glede njihovega zdravstvenega stanja?

Odgovor na vprašanje je odvisen od narave same izjave. Z vidika varstva osebnih podatkov je dopustno, da delavec pisno potrdi, da je prejel določene informacije in navodila, ki so v zvezi s pravicami in dolžnostmi iz delovnega razmerja (v konkretnem primeru v zvezi s preprečevanjem in obvladovanjem epidemije COVID-19).

Če ne gre za anamnestično anketo, ki bi jo delavec ob vsakokratnem prihodu na delo moral izpolniti in predložiti delodajalcu, zdravstvena vprašanja v takem dokumentu niso sporna z vidika varstva osebnih podatkov.

Ni pa dopustno predložiti v podpis delavcu izjave, ki vsebuje njegovo obveznost obveščanja delodajalca o konkretnih znakih bolezni in o konkretnih navodilih, ki bi jih delavcu dal osebni zdravnik, če ta navodila presegajo informacije o splošnem režimu zdravljenja (predviden čas bolniške odsotnosti, s strani zdravnika določen režim gibanja, podatke, ki so redoma navedeni na bolniškem listu, kot so izolacija, nega, poškodba...), do katerih je delodajalec sicer upravičen. Drugih **informacij**, ki presegajo informacije o režimu gibanja in informacije na bolniškem listu, pa delodajalec z vidika varstva osebnih podatkov delavca, **ni upravičen zahteva**ti.

Pošiljanje elektronskih bolniških listov po e-pošti (znotraj delodajalca)

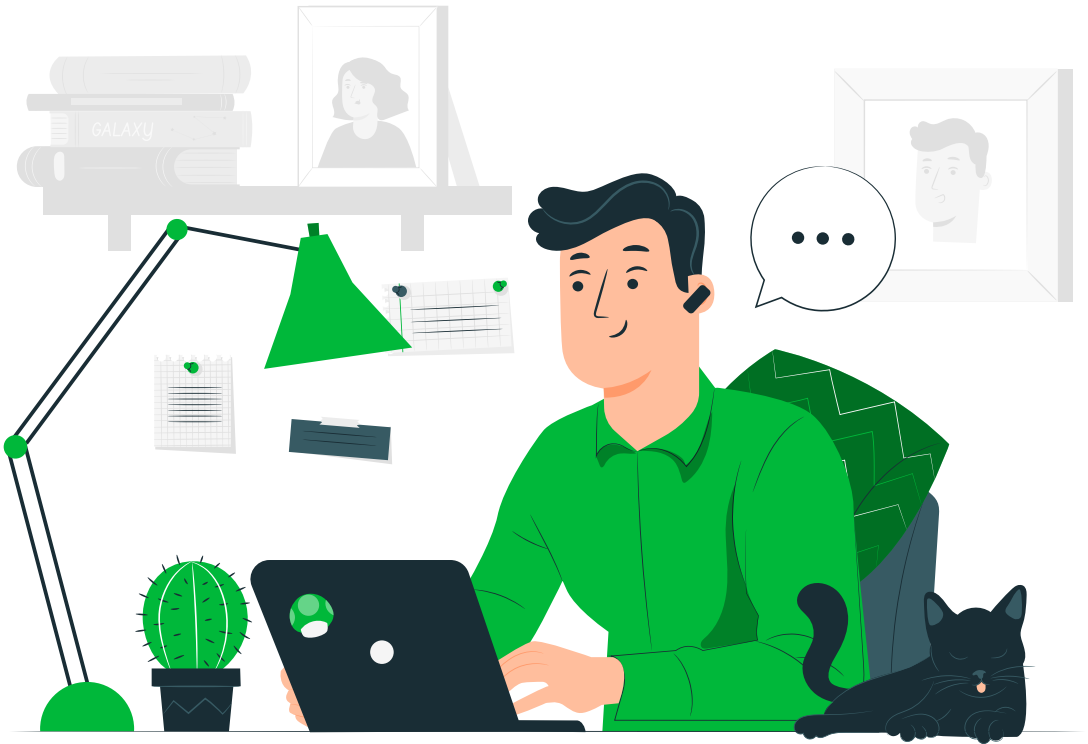
Organizacija dela (npr. v obliki dela na domu) v času epidemije lahko povzroči, da sicer ustaljeno posredovanje e-bolniških listov med pristojnimi osebami znotraj organizacijskih enot delodajalca ni možno.

Ker gre v primeru bolniških listov za posebne vrste osebnih podatkov, je treba glede njihovega zavarovanja upoštevati še veljavne določbe 14. člen ZVOP-1 glede prenosa občutljivih osebnih podatkov preko telekomunikacijskih omrežij. V teh primerih je nujno, da so občutljivi osebni podatki med prenosom **ustrezno šifrirani. Pri konkretnih rešitvah oz. programski opremi** je bistveno, da izpolnjuje **naslednja priporočila:**

- uporabljeni šifrirni mehanizmi morajo biti takšni, da se v času uporabe štejejo kot varni (tj. da niso bile ugotovljene posebne ranljivosti). Izogibati se je treba uporabi »lastniških« šifrirnih rešitev, katerih trdnost ni bila javno preverjena. Šifriranja osebnih podatkov ne smemo enačiti z anonimizacijo podatkov (!) – ustrezno šifriranje preprečuje nepooblaščenim osebam seznanitev z vsebino, ne pomeni pa, da so podatki razosebljeni in da identifikacija oseb ni več možna. Šifrirani osebni podatki so psevdonimizirani osebni podatki in veljajo za osebne podatke.
- nujno je, da se geslo za odpiranje datotek posreduje po drugam kanalu (če se šifrirana datoteka pošlje po e-pošti, se geslo sporoči po telefonu, prek SMS ali na drug ustrezen način in ne po e-pošti).
- gesla morajo ustrezati uveljavljenim standardom za varno izbiro gesel (nekaj koristnih priporočil najdete na spletni strani Varninainternetu.si: Zavarujte svoje geslo).

Ali lahko delodajalec telefonske klice (notranje klice, klice zunanjih institucij in klice strank) v času ukrepov preveže na zasebne telefone zaposlenih na podlagi njihove pisne privolitve za obdelavo podatka o zasebni telefonski številki?

Če se delodajalec glede na izredne razmere odloči, da je dosegljivost določenega delavca preko telefona nujna zaradi opravljanja njegovih nalog (npr. zaradi dela s strankami), bi mu moral zagotoviti temu primerna delovna sredstva (npr. službeni telefon). Lahko pa delavec da na voljo tudi svoja delovna sredstva (preusmeritev na zasebni mobilni telefon), če v to **privoli**. Delavčeva **zasebna telefonska številka se lahko uporablja zgolj v obsegu, ki je nujen za opravljanje nalog dela na domu**.



SKLEPNO

Pri obdelavi osebnih podatkov v delovnih razmerjih je treba upoštevati neenakopraven položaj delavca v primerjavi z delodajalcem. Zaradi tega je obdelava osebnih podatkov delavca mogoča le, če temelji na zakoniti pravni podlagi in temeljnih načelih obdelave osebnih podatkov, kot jih določa Splošna uredba.

Delodajalca pri obdelavi osebnih podatkov zavezuje načelo odgovornosti, ki je v Splošni uredbi poudarjeno kot izhodiščno načelo. Pred vsakokratno odločitvijo o obdelavi osebnih podatkov delavcev je delodajalcu v pomoč ustrezno izvedena ocena učinkov na varstvo osebnih podatkov. Splošna uredba delavcem daje številne pravice, ki jih lahko uveljavijo glede obdelave njihovih osebnih podatkov s strani delodajalca.

Le z doslednim upoštevanjem standardov varstva osebnih podatkov delavcev in s hkratnim omogočanjem izvrševanja pravic, ki jih imajo v zvezi s svojimi osebnimi podatki delavci, je mogoče zgraditi sistem zaupanja med delavci in delodajalci, ki dolgoročno krepi pripadnost delavcev delovnemu okolju in povečuje delovno uspešnost podjetja oz. organizacije.

Informacijski pooblaščenec RS

Dunajska cesta 22

1000 Ljubljana, Slovenija

T: 01 230 97 30

F: 01 230 97 78

gp.ip(at)ip-rs.si

Uradne ure:

PON – PET

10.00 - 12.00 in 14.00 - 15.00

V okviru projekta iDecide nudimo v času uradnih ur strokovno podporo z **brezplačnim telefonskim svetovanjem na številki 01 230 97 30**. Vsakodnevno strokovno podporo nudimo tudi s **pisnim svetovanjem** (vprašanje lahko posredujete na e-naslov gp.ip@ip-rs.si) in **objavami informacij in izobraževalnih gradiv na spletnih straneh IP**.

Če zaznate kršitev oziroma se vam je zgodila kršitev vaših pravic po Splošni uredbi, lahko svojo prijavo ali pritožbo posredujete IP po elektronski ali navadni pošti. Uporabite lahko tudi ustrezen obrazec, objavljen med Obrazci na spletni strani IP.