Vodnik
po varstvu osebnih podatkov za posameznike

INFORMACIJSKI
POOBLAŠČENEC

Namen dokumenta:	Smernice so namenjene posameznikom in pojasnjujejo pravice posameznike in zahteve zakonodaje v različnih situacijah, v katerih se znajde posameznik – kot potrošnik, kot zaposleni, kot uporabnik storitev javnega sektorja.
Ciljne javnosti:	Posamezniki
Status:	Javno
Verzija:	1.1
Datum izdaje:	1. 2. 2021
Datum popravka	18. 5. 2022 (str. 21)
Avtorji:	Informacijski pooblaščenec, ilustracije vir: Freepik, Flaticon
Ključne besede:	Smernice, neposredno trženje, obdelava osebnih podatkov, pravice posameznika, informiranost posameznikov, varnost na spletu.

KAZALO

Uvod

Posamezniki nastopamo v različnih vlogah – kot potrošniki, državljani ali kot zaposleni. Z vsesplošnim trendom informatizacije in selitvijo mnogih storitev na splet nastajajo nove potrebe po zbiranju in obdelavi osebnih podatkov, kar prinaša tudi večja tveganja za pravice in svoboščine posameznikov. Da bi bili kot posamezniki bolj zaščiteni, ko organizacije zbirajo, hranijo, posredujejo in drugače obdelujejo naše osebne podatke, Splošna uredba o varstvu podatkov[1] (v nadaljevanju: Splošna uredba) tistim, ki zbirajo in uporabljajo naše osebne podatke - ‚upravljavcem' in ‚obdelovalcem' osebnih podatkov, nalaga številne obveznosti, da poskrbijo za zakonito, transparentno, pošteno, varno in odgovorno obdelavo osebnih podatkov. Na drugi strani pa Splošna uredba zagotavlja tudi posameznikom pravice, prek katerih imamo moč vplivati na obdelavo svojih podatkov. Na ta način se zagotavlja ravnovesje, ki je potrebno za uravnoteženje posega v pravico do varstva osebnih podatkov. Da bi lahko kot posamezniki učinkovito ščitili svojo pravico do varstva osebnih podatkov se moramo na prvem mestu sploh zavedati, da nekdo obdeluje naše podatke in za kakšen namen jih obdeluje...

[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 o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov).

Osnovni pojmi

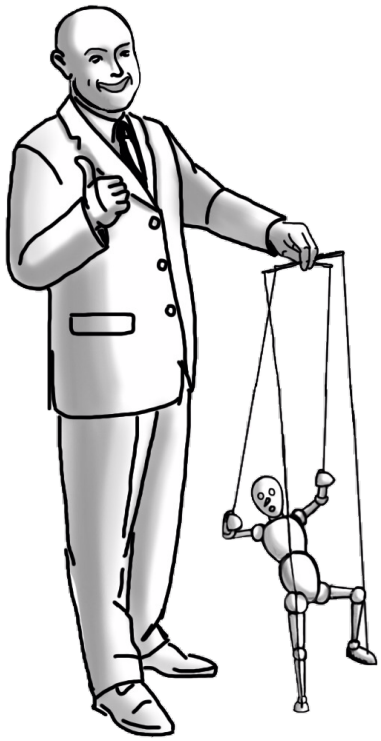
KJE IN KDO VSE ZBIRA IN OBDELUJE PODATKE O MENI?

◉ ‚Upravljavci‘

Osebne podatke o meni zbirajo, hranijo in drugače obdelujejo, npr.:

- **podjetja** (trgovci, oglaševalci, operaterji, banke, zavarovalnice,...) za izvajanje sklenjenih pogodb in za prodajo novih izdelkov ali storitev;
- **država v širšem pomenu besede**, ki zagotavlja različne javne storitve – od odločanja o pravicah iz javnih sredstev, do varnostnih (policija), zdravstvenih, izobraževalnih in drugih storitev, ki se financirajo iz javnih sredstev in so zato posebej regulirane;
- **delodajalci** za izvajanje obveznosti in pravic iz delovnega razmerja (obračun plače, službene poti, zagotavljanje varnosti in varstva zaposlenih, itd.).

Vsi navedeni subjekti iz javnega ali zasebnega sektorja lahko torej samostojno ali skupaj z drugimi določajo ‚namene in sredstva‘ obdelave osebnih podatkov. Drugače povedano, določajo zakaj in kako se bo osebne podatke obdelovalo. Ti subjekti torej upravljajo z našimi osebnimi podatki, zato jih imenujemo ‚upravljavci‘ osebnih podatkov.



◉ ‚Obdelovalci‘

Upravljavci lahko za določene obdelave osebnih podatkov najemajo ‚obdelovalce‘ osebnih podatkov, ki v njihovem imenu in za njihov namen izvajajo obdelave osebnih podatkov. Tako na primer podjetja:

*najemajo **računovodske servise,** da pripravijo obračun plač zaposlenih,*

*najemajo **spletne storitve**, kot je storitev oblačne hrambe podatkov, storitev za množično pošiljanje elektronskih sporočil več naslovnikom, ipd.,*

*najemajo **klicne centre** za ponujanje njihovih izdelkov ali storitev (klicni center pridobi seznam kontaktnih telefonskih številk na katere kliče), itd.*

Upravljavec mora z obdelovalcem skleniti **ustrezno pisno pogodbo o obdelavi osebnih podatkov**, v kateri bo opredeljeno pod katerimi pogoji in za kateri namen lahko podatke obdeluje.

Več o pogodbeni obdelavi:

➔ **Infografika**: Infografika o pogodbeni obdelavi[2]

➔ **Smernice IP**: Smernice o (pogodbeni) obdelavi osebnih podatkov po Splošni uredbi o varstvu podatkov[3]

[2] https://www.ip-rs.si/fileadmin/user_upload/Pdf/infografike/INFOGRAFIKA_Pogodbena_obdelava_1_.pdf

[3] https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_pogodbeni_obdelavi_web.pdf

KDAJ SE UPORABLJAJO PRAVILA ZA VARSTVO OSEBNIH PODATKOV?

Pravila varstva osebnih podatkov se uporabljajo za ‚obdelavo osebnih podatkov'. To pomeni, da mora biti
(1) podatek ‚*osebni podatek*' IN
(2) potekati ‚*obdelava*' osebnih podatkov.
Izpolnjena morata biti oba pogoja hkrati.

‚Osebni podatek'

‚Osebni podatek' je poenostavljeno povedano podatek, ki kaže na posameznika. Gre torej za katerikoli podatek (ne glede na obliko v kateri je izražen – črke, številke, znaki, slike, zvoki...), da sam ali v povezavi z drugimi omogoča določljivost posameznika. Osebni podatki so na primer poleg identifikacijskih in kontaktnih podatkov (ime in priimek, EMŠO, davčna številka, naslova prebivališča, datum rojstva), lahko tudi fotografija ali videoposnetki, na katerem je posameznik prepoznaven, podatek o lokaciji, podatki o nakupih, o stanju na računih, o lastništvu stanovanj in vozil, IP naslov, nameščen piškotek, zapis biometrično prebranega prstnega odtisa, zvočni posnetek, na katerem je posameznik prepoznaven, itd.

‚Obdelava osebnih podaktov'

Dalje, pravila varstva osebnih podatkov se uporabljajo, ko bo šlo za ‚obdelavo' osebnih podatkov. Obdelava osebnih podatkov je katerakoli dejavnost v zvezi z osebnimi podatki, ki je v

(1) zvezi z ‚zbirko osebnih podatkov' ALI

(2) kjer pride do ‚avtomatizirane obdelave' ne glede na obstoj zbirke.

Pogoja morata biti izpolnjena alternativno (ali eden ali drugi, pogosto pa sta izpolnjena oba hkrati).

‚Zbirka osebnih podatkov'

Za izpolnjevanje svojih nalog ali namenov upravljavci podatke hranijo v različnih ‚zbirkah osebnih podatkov', za katere so kot upravljavci tudi odgovorni.

Primeri zbirk: *državni registri osebnega statusa in prebivališča, davčni register, register lastništva in uporabe nepremičnin, vozil, vrednostnih papirjev, kapitalskega lastništva, zdravstvena dokumentacija, osebne mape učencev, bančni izpiski, osebna mapa zaposlenega pri delodajalcu, kazenska in prekrškovna evidenca, zbirka podatkov o nakupih s kartico zvestobe, zbirka podatkov preteklih nakupov v spletni trgovini, itd.*

Kakršnakoli dejavnost v zvezi z zbirko osebnih podatkov je obdelava osebnih podatkov (npr. vpogled v zbirko, kopiranje podatkov, posredovanje podatka iz zbirke (tudi javna objava), sestava nove zbirke na podlagi zbranih osebnih podatkov, itd.).

‚Obdelava osebnih podatkov z avtomatiziranimi sredstvi‘

Obdelava osebnih podatkov z ‚avtomatiziranimi sredstvi‘ je tesno povezana z razvojem informacijske tehnologije, ki nas obkroža. Slednja namreč ponuja zmogljivosti povezovanja in ustvarjanja novih zbirk podatkov v milisekundah, kot tudi obdelavo osebnih podatkov, brez nastanka zbirke osebnih podatkov, pri čemer pa rezultat kljub temu lahko vpliva na pravice in svoboščine posameznika. Pravila varstva osebnih podatkov se torej uporabljajo tudi v tovrstnih primerih, saj v postopku zbiranja podatkov pride do obdelave osebnih podatkov, ki so obdelani z ‚avtomatiziranimi sredstvi‘ – četudi pri tem ne pride do nastanka zbirke osebnih podatkov. Z uporabo umetne inteligence bo teh postopkov in rezultatov še mnogo več, saj nas obkrožajo naprave, ki merijo naše gibanje, zvoke in podobe, pri tem pa ni treba, da bi se vse zaznave teh naprav tudi zapisale v neko zbirko, da bi lahko upravljavec zaznane podatke »uporabil« za svoje namene.

KAKŠNA SO TEMELJNA PRAVILA ZA OBDELAVO OSEBNIH PODATKOV?

‚Temeljna človekova pravica‘

Varstvo osebnih podatkov sodi med ‚temeljne človekove pravice,‘ ki je varovano z Ustavo republike Slovenije. Splošna uredba okvirno določa pravila za varstvo osebnih podatkov. Namen varstva osebnih podatkov je varstvo posameznika, na katerega se podatki nanašajo. Da svojo pravico do varstva osebnih podatkov posameznik lahko uresničuje, morajo upravljavci in obdelovalci spoštovati nekatera pravila, ki določajo, kako je treba varno in ustrezno ravnati z osebnimi podatki, da ne pride do kršitve te človekove pravice.

‚Načela varstva osebnih podatkov‘

Načela varstva osebnih podatkov so osnovna vodila, ki jih morajo spoštovati upravljavci pri zbiranju in obdelavi osebnih podatkov. Ta so:

- da se podatki obdelujejo **POŠTENO, TRANSPARENTNO IN NA ZAKONITI PRAVNI PODLAGI**,
- da se podatke obdeluje le za **DOLOČENE, IZRECNE IN ZAKONITE NAMENE** in **NE ZA NAMENE, KI NISO ZDRUŽLJIVI Z NAMENOM ZBIRANJA**,
- da se zbira le tiste podatke, ki so **USTREZNI, RELEVANTNI IN OMEJENI NA NAMEN ZBIRANJA**, s čimer se prepreči zbiranje osebnih podatkov »na zalogo«,
- da so podatki **TOČNI** in **AŽURNI**,
- da se podatke **HRANI LE TOLIKO ČASA**, kot **NUJNO POTREBNO** glede na **NAMEN** obdelave,
- da je poskrbljeno za **VARNOST**; da do osebnih podatkov dostopajo le pooblačene osebe, da se prepreči izguba ali uničenje podatkov, itd,
- da upravljavci ravnajo **ODGOVORNO** tako, da v vsakem trenutku lahko zagotovijo in izkažejo, da osebne podatke obdelujejo skladno z zakonodajo (načelo odgovornosti; ang. ‚accountability principle‘).

‚Pravne podlage'

Iz NAČELA ZAKONITOSTI izhaja osnovno vprašanje – ali upravljavec sploh sme obdelovati osebne podatke? Z drugimi besedami ali obstaja ustrezna 'pravna podlaga' za obdelavo osebnih podatkov. Pravne podlage so lahko:

(a) **PRIVOLITEV** posameznika [4]

(b) izvajanje **POGODBE** in izvajanje **AKTIVNOSTI PRED SKLENITVIJO POGODBE**,

(c) izvajanje **ZAKONSKE OBVEZNOSTI**,

(d) zaščita **ŽIVLJENJSKIH INTERESOV**,

(e) izvajanje **JAVNE OBLASTI** ali **NALOGE V JAVNEM INTERESU** (v javnem sektorju),

(f) **ZAKONITI INTERESI** (v zasebnem sektorju).

‚Posebne vrste osebnih podatkov'

‚Posebne vrste osebnih podatkov,' so takšni podatki, ki razkrivajo:

- rasno ali etnično **POREKLO**;
- **POLITIČNO MNENJE**;
- versko ali filozofsko **PREPRIČANJE**;
- članstvo v **SINDIKATU**;
- obdelava **GENETSKIH PODATKOV**;
- **BIOMETRIČNIH PODATKOV** za namene edinstvene identifikacije posameznika;
- podatki v zvezi z **ZDRAVJEM**;
- podatki v zvezi s posameznikovim **SPOLNIM ŽIVLJENJEM** ali spolno usmerjenostjo.

Navedeni podatki so po svoji naravi bolj občutljivi, saj pri teh vrstah podatkov obstaja za posameznika večje tveganje, da bi bil zaradi razkritja podvržen diskriminaciji ali zlorabam. Zato so za obdelavo teh podatkov predpisani strožji pogoji kot pri običajnih vrstah osebnih podatkov.

4 Več informacij: spletna stran IP o privolitvi.

‚Varna obdelava osebnih podatkov'

Pri obdelavi osebnih podatkov je ključnega pomena, da se osebni podatki obdelujejo ‚varno'. Pojem varnosti moramo razlikovati od pojma varstva. Varstvo je širše in obsega tudi vprašanja, ali ima upravljavec pravno podlago za obdelavo osebnih podatkov, medtem ko se varnost nanaša le na tehnične in organizacijske ukrepe za zaščito osebnih podatkov pred nepooblaščenimi dostopi, izgubo podatkov, itd. Za ilustracijo si lahko predstavljamo varnost kot sef, kjer so podatki shranjeni – vendar noben še tako varen sef ne bo opravičil obdelave osebnih podatkov, če upravljavec podatkov sploh ne bi smel hraniti.

Več o varnosti (zavarovanju) osebnih podatkov:

➔ Spletna stran IP: Zavarovanje oz. varnost osebnih podatkov,[5]

➔ Smernice IP o zavarovanju osebnih podatkov.[6]

INŠPEKCIJSKI NADZOR

Vsakdo, ki zazna kršitev s področja varstva posebnih podatkov (ne glede na to ali se podatki nanašajo nanj ali ne), lahko poda ‚inšpekcijsko prijavo' nadzornemu organu za varstvo osebnih podatkov, to je Informacijski pooblaščenec RS (v nadaljevanju IP). Prijavo lahko poda na neobvezujočem obrazcu, ki ga je pripravil IP (glej spodaj – OBRAZEC).

Več o inšpekcijskem nadzoru:

➔ Sletna stran IP; varstvo osebnih podatkov/ inšpekcijski nadzor.

OBRAZEC:

➔ Prijava kršitve varstva osebnih podatkov (Obrazec ZIN PRIJAVA).

5 https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/zavarovanje-oz-varnost-osebnih-podatkov/

6 Smernice o IP zavarovanju osebnih podatkov, https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_zavarovanju_OP.pdf .

Informiranje posameznikov in pravice

INFORMIRANJE POSAMEZNIKOV

Da bi imeli kot posamezniki določeno mero nadzora nad obdelavo svojih osebnih podatkov, moramo biti najprej seznanjeni s tem, da nekdo sploh obdeluje naše osebne podatke in zakaj. To je še zlasti pomembno, ko se podatke zbira brez našega zavedanja. Zato Splošna uredba upravljavcem nalaga obveznost, da informirajo posameznike o vseh pomembnih vidikih obdelave osebnih podatkov (to izhaja iz načela ‚transparentnosti' pri obdelavi osebnih podatkov). Izjemoma informiranje posameznikov ni potrebno, npr. če posameznik informacije že ima ali pa ko to zahtevajo posebni nameni zbiranja osebnih podatkov (npr. za preiskovanje kaznivih dejanj).

Upravljavec, mora posameznika seznaniti s tem:

- **Kdo je upravljavec? (naziv, sedež, kontaktni podatki)**
- **Zakaj obdeluje osebne podatke? (namen, pravna podlaga)**
- **Komu bo podatke posredoval? (morebitni obdelovalci, drugi upravljavci ali uporabniki in če bo podatke posredoval v tretje države)**
- **Katere so posameznikove pravice?**

Velja posebej poudariti, da Splošna uredba zahteva več kot to, da so navedene informacije pri upravljavcu nekje zapisane (pogosto »skrite v splošnih pogojih poslovanja«). Te informacije morajo biti jasno in razvidno dostopne, hkrati pa morajo biti podane v jeziku in obliki, ki je primeren glede na starost, izobrazbo in druge osebne okoliščine ciljne skupine posameznikov od katerih upravljavec zbira osebne podatke (npr. v posamezniku razumljivi izjavi o zasebnosti na spletnih straneh).

Več o pregledni obdelavi osebnih podatkov:

- ➔ Spletna stran tiodlocas.si,[7]
- ➔ Smernice IP: Smernice za oblikovanje izjave o varstvu osebnih podatkov na spletnih straneh[8]

7 Transparentna obdelava osebnih podatkov, https://tiodlocas.si/moram-biti-obvescen/.

8 Smernice za oblikovanje izjave o varstvu osebnih podatkov na spletnih straneh https://www.ip-rs.si/publikacije/prirocniki-in-smernice/smernice-informacijskega-pooblascenca-za-oblikovanje-izjave-o-varstvu-osebnih-podatkov-na-spletnih-straneh/.

PRAVICE POSAMEZNIKA PO SPLOŠNI UREDBI

Posameznikom Splošna uredba ponuja možnost nadzora nad njihovimi osebnimi podatki prek uveljavljanja pravic po Splošni uredbi. Ker je Splošna uredba evropski splošni pravni akt, ki velja neposredno v vseh državah članicah EU, lahko posamezniki uveljavljajo svoje pravice po tej uredbi pred vsakim upravljavcem iz EU.

Več o pravicah posameznika po Splošni uredbi:

➔ Spletna stran IP: Pravice posameznika

Pravice, ki so zapisane v členih 15 -22 Splošne uredbe so naslednje:

§15 PRAVICA DO DOSTOPA ALI DO SEZNANITVE Z LASTNIMI OSEBNIMI PODATKI

Pravica dostopa omogoča posamezniku, da mu upravljavec pojasni oziroma poda informacije:

- Ali ima njegove osebne podatke?
- Katere vrste podatkov obdeluje?
- Za katere namen(e) obdelave?
- Komu se podatki posredujejo (uporabnike)?
- Kako dolgo se hranijo?

Hkrati pa ta pravica omogoča tudi vpogled oziroma pridobitev kopije posameznikovih osebnih podatkov. Tako na primer lahko posameznik pridobi fotokopijo svojih podatkov, izpis podatkov o svojih nakupih ali transakcijah, video-nadzorni posnetek, na katerem je prepoznaven itd.

Več o pravici dostopa:

➔ Spletna stran tiodlocas.si: Želim vedeti, kaj počnejo z mojimi podatki [9]

➔ Spletna stran IP: Seznanitev z lastnimi osebnimi podatki ali pravica do dostopa do osebnih podatkov [10]

OBRAZCI:

➔ Zahteva za seznanitev z lastnimi osebnimi podatki (obrazec SLOP)[11]

➔ Pritožba zaradi kršitve pravice do seznanitve z lastnimi osebnimi podatki (obrazec P-SLOP)[12]

§16 PRAVICA DO POPRAVKA

‚Pravica do popravka' ponuja možnost, da posameznik od upravljavca zahteva, da popravi netočne ali neažurne podatke v zvezi z njim in dopolni nepopolne osebne podatke. Tako lahko na primer posameznik zahteva uskladitev svojih podatkov pri svojem operaterju, po tem ko je spremenil svoj priimek ali podatek o prebivališču, če se je preselil, ipd. Upravljavec je dolžan netočne ali nepopolne podatke izbrisati.

Več o pravici do popravka:

➔ Spletna stran tiodlocas.si: Želim popraviti netočne podatke[13]

9 https://tiodlocas.si/?page_id=106_

10 https://www.ip-rs.si/varstvo-osebnih-podatkov/pravice-posameznika/seznanitev-z-lastnimi-osebnimi-podatki/

11 https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/Zahteva_za_seznanitev_z_lastnimi_osebnimi_podatki__Obrazec_SLOP_.doc

12 https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/Pritozba_zaradi_krsitve_pravice_do_seznanitve_z_lastnimi_osebnimi_podatki__Obrazec_P-SLOP.doc

13 https://tiodlocas.si/zelim-popraviti-netocne-podatke/

§17 PRAVICA DO IZBRISA (pravica do POZABE)

‚Pravica do izbrisa (pravica do pozabe, ang. right to be forgotten)' omogoča posamezniku, da zahteva izbris osebnih podatkov, kadar so za to izpolnjeni pogoji. Kadar na primer upravljavec podatke vodi zaradi zakonske obveznosti (npr. državni registri in evidence), pravica do izbrisa ne bo prišla v poštev. V poštev pa bo prišla na primer, ko upravljavec vodi podatke o posamezniku na podlagi njegove privolitve, pa posameznik privolitev umakne (npr. prijava na e-novice na podlagi privolitve).

Posamezniki pogosto zahtevajo izbris medijskih objav, ki jih javnosti izpostavljajo in jih zato motijo (lahko tudi kvarijo ugled, ipd.). Pojasniti je treba, da Splošna uredba izrecno onemogoča uresničevanje pravice do izbrisa, kadar se z objavo uresničuje pravica do svobode izražanja in obveščanja (kar je najbolj očitno pri objavah s strani medijev, ki po Zakonu o medijih uživajo poseben status ravno zaradi uresničevanja svobode izražanja). Slednje sicer ne pomeni, da se za nobeno medijsko objavo in pod nobenim pogojem ne da doseči izbrisa, ne glede na naravo in vrsto podatkov, ki so objavljeni. Kljub temu pa se mora poseg v pravico do varstva osebnih podatkov v konkretnem primeru uravnotežiti z drugimi konkurirajočimi človekovimi pravicami in svoboščinami. Takšno tehtanje se lahko izvede le ob upoštevanju vseh okoliščin primera v konkretnem pravnem postopku.

Pravica do izbrisa pa se s Splošno uredbo razteza tudi na možnost umika spletnih povezav do člankov ali vsebin, za katere je utemeljeno, da se izbrišejo. Slednje je posledica sodbe v zadevi Google Spain,[14] ko je Sodišče EU ugotovilo, da mora upravljavec spletnega iskalnika, če so pogoji izpolnjeni, s seznama zadetkov, ki se prikaže po iskanju, opravljenem na podlagi imena osebe, odstraniti povezave na spletne strani, ki jih objavijo tretje osebe in ki vsebujejo informacije, ki se nanašajo na to osebo.[15]

Več o pravici do izbrisa (pravici do pozabe):

- ➔ Spletna stran tiodlocas.si: Želim izbrisati svoje podatke[16]
- ➔ Spletna stran tiodlocas.si: Izbris osebnih podatkov in pravica do pozabe[17]

§18 PRAVICA DO OMEJITVE OBDELAVE

- Pravica do omejitve obdelave lahko pride v poštev na primer, ko bi bil posameznik sicer upravičen zahtevati izbris, pa vseeno želi, da upravljavec podatke hrani zaradi morebitnih kasnejših dokazovanj pred pristojnimi organi ali drugimi deležniki. Prav tako lahko pravica pride v poštev, če posameznik zahteva, da upravljavec podatkov ne zbriše, ko bi jih glede na predviden rok hrambe sicer zbrisal, zaradi uveljavljanja svojih pravnih zahtevkov (npr. videonadzorni posnetek kraja, kjer se je zgodila prometna nesreča, zaradi uveljavljanje škode pri zavarovalnici). Omejitev obdelave je mogoče zahtevati tudi v povezavi s pravico do popravka (dokler upravljavec ne odloči o popravku) in pravico do ugovora (dokler ne odloči o ugovoru).

Več o pravici do omejitve obdelave:

- ➔ Spletna stran tiodlocas.si: Želim omejiti obdelavo svojih podatkov[18]

14 Sodba (C-131/12 z dne 13.5.2014),), povzetek v objavi za javnost na spletni strani IP: https://www.ip-rs.si/novice/upravljavec-spletnega-iskalnika-je-upravljavec-osebnih-podatkov-in-zato-zavezan-k-spostova-890/.

15 Prav tam.

16 https://tiodlocas.si/zelim-izbrisati-svoje-podatke/

17 https://tiodlocas.si/top-nasveti/izbris-osebnih-podatkov-in-pravica-do-pozabe/

18 https://tiodlocas.si/zelim-zacasno-zamrzniti-svoje-podatke/

§20 PRAVICA DO PRENOSLJIVOSTI

Pravica do prenosljivosti omogoča posamezniku, da zahteva od upravljavca, da posreduje drugemu upravljavcu (ali posamezniku) osebne podatke, ki jih vodi o tem posamezniku v strojno berljivi obliki. Pogoji so, da upravljavec podatke obdeluje z avtomatiziranimi sredstvi in na podlagi privolitve oziroma zaradi pogodbe.

Pravica do prenosljivosti pride v poštev, npr.:

Posameznik od ponudnika pretočne glasbe ali spletne videoteke, ki mu plačuje mesečno uporabnino, zahteva, da prenese njegove podatke o preteklih poslušanjih in ogledih drugemu ponudniku pretočne glasbe/video vsebin.

Posameznik od trgovca, pri kateremu imate kartico zvestobe, zahteva posredovanje podatkov o svojih preteklih nakupih drugemu trgovcu.

Posameznik od svoje banke zahteva prenos podatkov o svojih transakcijah drugi banki.

OBRAZEC:

➔ Zahteva za prenosljivost (obrazec ZPP)[19]

Več o pravici do prenosljivosti:

➔ Spletna stran tiodlocas.si: Želim prenesti svoje podatke k sebi ali k drugim upravljavcem[20]

§21 PRAVICA DO UGOVORA

Pravica do ugovora pride v poštev, ko gre za obdelavo osebnih na podlagi zakonitih interesov (za zasebni sektor) ali zaradi izvajanja naloge v javnem interesu ali javne oblasti (za javni sektor).

Kakšni to ti primeri? Na omenjenih podlagah se na primer pogosto izvaja:

- *poslovna komunikacija prek javno objavljenih kontaktnih oseb pri podjetju,*
- *analitika avtocestnega prometa zaradi merjenja gostote prometa,*
- *zagotavljanje varnosti informacijskih sistemov, pri čemer prihaja do obdelave osebnih podatkov (npr. zaposlenih),*
- *snemanje cest in ulic za vzpostavitev virtualnega zemljevida, itd.*

Primeri obdelave na teh pravnih podlagah so v praksi pogosti, izvajajo pa se brez privolitve – zato posameznik te obdelave nima možnosti »predhodno odobriti« kot pri privolitvi. Posledično je zelo pomembno, da so posamezniki o obdelavi na primeren način tudi obveščeni. Pravica do ugovora skupaj z obvestilom daje posamezniku vsaj določeno mero vpliva nad tem, kaj se dogaja z njegovimi osebnimi podatki. Informacija o pravici do ugovora mora biti posamezniku podana istočasno, kot vse ostale informacije – mora pa biti jasno razločna od drugih informacij. Posameznik pa mora biti jasno in razločno informiran tudi o razlogih zakonitega interesa, ki utemeljuje obdelavo osebnih podatkov.

Pravica do ugovora torej daje posamezniku možnost, da ugovarja obdelavi, upravljavec pa mora takoj prenehati izvajati obdelavo, razen če dokaže, da obstajajo ‚nujni legitimni razlogi za obdelavo'. Kdaj bo torej nujno, da se obdelavo izvaja, bo odvisno od konkretnih primerov, pri tem pa je treba poudariti, da mora upravljavec dokazati, da obstajajo takšni razlogi, zaradi katerih lahko utemeljeno zavrne ugovor. Obrazložitev upravljavca mora biti konkretna in ustrezno upoštevati razloge, ki jih navaja posameznik v svojem ugovoru.

Poseben režim je predviden za neposredno trženje - v tem primeru mora upravljavec takoj prenehati z obdelavo in ugovora ne more zavrniti. Več o tem v poglavju o neposrednem trženju.

Poseben režim velja tudi za obdelave z znanstveno- ali zgodovinskoraziskovalnim ali statističnim namenom. V tem primeru posameznik z ugovorom ne more uspeti, če se ta namen izpolnjuje zaradi opravljanja naloge, ki je v javnem interesu (npr. državna statistika, raziskave po zakonu o raziskovalni dejavnosti, ipd.).

Več o pravici do ugovora:

➔ Spletna stran tiodlocas.si: Želim ugovarjati obdelavi mojih podatkov[21]

19 Zahteva za prenosljivost (obrazec ZPP), https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/Zahteva_za_prenosljivost_podatkov_Obrazec_ZPP.docx.

20 https://tiodlocas.si/zelim-prenesti-svoje-podatke/

21 https://tiodlocas.si/zelim-ugovarjati-obdelavi-mojih-podatkov/

§22 PRAVICA, DA ZA POSAMEZNIKA NE VELJA AVTOMATIZIRANA ODLOČITEV VKLJUČNO S PROFILIRANJEM

Avtomatizirane odločitve so odločitve, ki jih na podlagi podatkov izdajo stroji, brez človeškega posredovanja. Lahko gre za odločanje v zasebnem ali javnem sektorju.

Primera iz javnega sektorja:

***izdaja informativnega izračuna dohodnine s strani finančne uprave**. Ta se izda na podlagi podatkov iz davčnega registra, brez človeškega posredovanja in šele v primeru morebitnega ugovora zoper informativni izračun, pravilnost izračuna preveri človek (oseba zaposlena pri FURS).*

***odločanje Centrov za socialno delo** o nekaterih socialnih transferjih.*

Primera v zasebnem sektorju:

sklepanje kreditnih posojil kar na bankomatu, brez človeškega posredovanja. Pri odobravanju kreditov banka na podlagi kreditne ocene in drugih kriterijev oceni tveganje ter donos in sprejme odločitev glede posojila. Ko gre za avtomatizirano odločanje, odločitev sprejme informacijski sistem, brez človekovega posredovanja (v Sloveniji takšno za odobravanje kreditov ni dopustno zaradi veljavnih določb Zakona o centralnem kreditnem registru, ki posebej zahteva človekovo posredovanje).

Nekatera večja zasebna podjetja, ki se soočajo tudi z več deset tisoč prošnjami za eno delovno mesto, da zožajo izbor kandidatov, uporabijo sisteme za avtomatizirano odločanje o ustreznem naboru kandidatov.

Primerov je v praksi še veliko več, z razvojem umetne inteligence pa se predvideva, da jih bo v prihodnosti še mnogo več. Ker se avtomatizirane odločitve o posamezniku sprejemajo zlasti z obdelavo osebnih podatkov (in profiliranjem kot delom tega postopka), gre torej primarno za vprašanje varstva osebnih podatkov in posega v zasebnost. Splošna uredba pa ne velja za vse avtomatizirane odločitve, temveč le tiste, ki imajo za posameznika neko pomembno posledico. Uredba pravi, da velja to za obdelave, ki imajo pravne učinke ali podobne učinke, ki na posameznika znatno vplivajo'. Največkrat gre za odločitve, ki za posameznika pomeni neko finančno posledico (odobritev/zavrnitev posojila, odpoved pogodbe, dostop do delovnega mesta, ipd.).

Avtomatizirano odločanje, vključno z oblikovanjem profilov je po Splošni uredbi praviloma prepovedano. Obstajajo pa pomembne izjeme v okviru katerih je to odločanje dopustno. Avtomatizirano odločanje je tako dopustno, če je odločitev:

- (a) nujna za sklenitev ali izvajanje pogodbe med posameznikom in upravljavcem
- (b) dovoljena po pravu Unije ali pravu države članice, ki velja za upravljavca in določa tudi ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki, (beri: določena z zakonom), ali
- (c) je posameznik vanjo izrecno privolil.

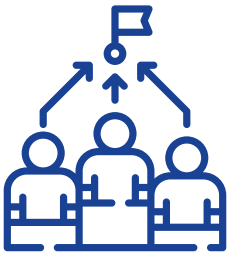
Kadar upravljavec izpolnjuje eno od zgoraj navedenih podlag, potem sme sprejemati tudi avtomatizirane odločitve, vključno z oblikovanjem profilov.

Posameznik pa ima možnost nasprotovati avtomatiziranemu odločanju:

- kadar gre za odločanje na podlagi zakona (v skladu zgoraj navedeno (b) točko – zlasti velja za javni sektor), se uporablja postopek, ki je predpisan v nacionalni ali evropski ureditvi,
- kadar bo šlo za odločanje na podlagi sklenjene pogodbe ali izrecne privolitve (v skladu zgoraj navedenima točkama (a) in (c) – zlasti velja za zasebni sektor), potem ima že po Splošni uredbi posameznik: »pravico do osebnega posredovanja upravljavca, do izražanja lastnega stališča in izpodbijanja odločitve«.

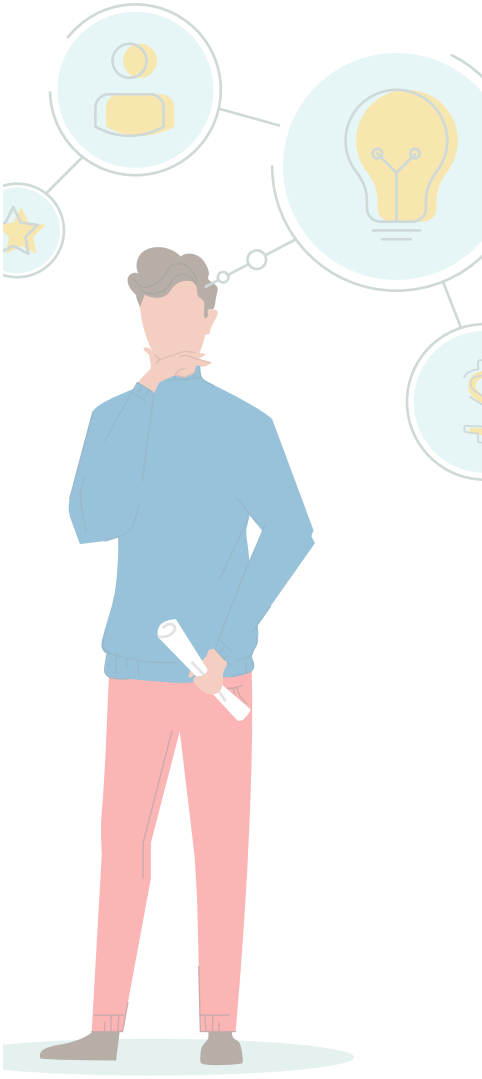
Da bi lahko posameznik učinkovito nasprotoval avtomatizirani odločitvi, mora seveda vedeti, zakaj je bila sprejeta takšna odločitev – poznati mora torej ‚smiselne informacije o razlogih, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki'. Te informacije bi moral upravljavec zagotoviti že sam "proaktivno" v okviru svoje obveznosti informiranja, posameznik pa ima te informacije pravico izvedeti tudi na zahtevo z uveljavljanem svoje ‚pravice do dostopa'.

UVELJAVLJANE PRAVIC PO SPLOŠNI UREDBI



Pri komu se uveljavljajo pravice?

Zgoraj omenjene pravice – do dostopa ali seznanitve, popravka, izbrisa, omejitve, ugovora in prenosljivosti – lahko posameznik uveljavlja pri upravljavcu. Upravljavec mora svoje kontaktne podatke sporočiti posamezniku.



Kdo lahko uveljavlja pravice po Splošni uredbi?

Pravice po Splošni uredbi lahko uveljavlja vsak posameznik v zvezi s podatki, ki se nanašajo nanj.

Za osebe mlajše od 15 let lahko uveljavljajo pravice v njihovem imenu zakoniti zastopniki (npr. starši, skrbniki, rejniki). Mladoletniki starejši od petnajst let, praviloma lahko uveljavljajo pravice po Splošni uredbi sami, razen kadar na primer sami niso upravičeni podati privolitve za obdelavo njihovih osebnih podatkov, ker bi zakon določal, da lahko podatke upravljavec zbira le s soglasjem zakonitih zastopnikov (primer: določene zbirke v šolski dokumentaciji).

Svojo pravico lahko posamezniki s pooblastilom prenesejo tudi na pooblaščenca, ki v njihovem imenu lahko uveljavlja pravice po Splošni uredbi (pogost primer je zbiranje dokazov za namen pravdnih ali drugih postopkov oziroma pravna pomoč pri uveljavljanju določenih pravic pri upravljavcih zbirk).

V kakšni obliki naj vložim zahtevo?

Čeprav ni izrecno predpisano, IP predlaga, da svoj zahtevek na upravljavce posamezniki naslovijo pisno in se izogibajo vlaganju ustnih zahtev. Pisna oblika namreč omogoča kasnejše dokazovanje, da je bil zahtevek dejansko vložen, kdaj je bil vložen in kaj je posameznik zahteval. Pri tem ni pomembno, ali je zahtevek vložen po elektronski poti ali v fizični obliki. Zlasti je pomembno, da se zahtevek vloži v obliki, ki omogoča kasnejše dokazovanje datuma, dejstva vložitve zahteve in njene vsebine.

Za vlaganje zahtev v zvezi s pravicami posameznikov niso predpisani posebni obrazci. IP zgolj za pomoč prosilcem pripravlja tudi posebne obrazce, ki so objavljeni na spletni strani IP.

OBRAZEC:

Spletna stran IP: Obrazci s področja varstva osebnih podatkov[22]

22 https://www.ip-rs.si/obrazci/varstvo-osebnih-podatkov/

V kakšni obliki lahko posameznik pričakuje odgovor?

Posameznik lahko sam izbira, v kakšni obliki želi prejeti odgovor (pisni ali elektronski). Kadar v svoji zahtevi tega ne navede, potem se domneva, da če je vložil zahtevo v elektronski obliki, da želi odgovor prejeti tudi v elektronski obliki.

V kolikšnem času mora upravljavec odgovoriti na zahtevo?

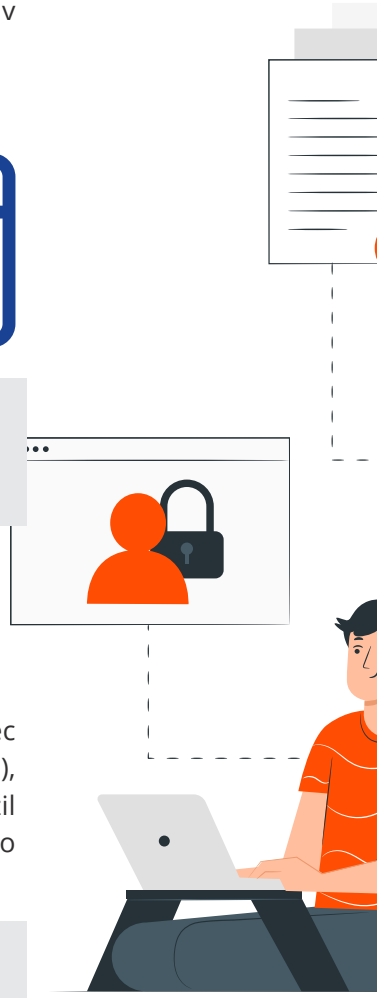
Rok za odgovor na zahtevo posameznika po Splošni uredbi je ‚brez nepotrebnega odlašanja' in v vsakem primeru ‚v enem mesecu po prejemu zahteve'. Ta rok lahko upravljavec izjemoma podaljša za največ dva dodatna meseca ob upoštevanju kompleksnosti in števila zahtev. Upravljavec mora obvestiti posameznika o vsakem takem podaljšanju v enem mesecu po prejemu zahteve skupaj z razlogi za zamudo.

Kaj pa, če upravljavec ne odgovori v roku?

Upravljavec je dolžan odgovoriti na zahtevo v predpisanem roku, sicer nastopi molk. V tem primeru se ima posameznik možnost obrniti na IP. Če je posameznik vložil zahtevo za seznanitev z lastnimi osebnimi podatki, lahko svojo pritožbo vloži tudi na obrazcu IP.

OBRAZEC:

➔ Pritožba zaradi kršitve pravice do seznanitve z lastnimi osebnimi podatki (obrazec P-SLOP).[23]



Kaj pa, če posameznik z odgovorom ni zadovoljen?

Posameznik, ki ni zadovoljen z odgovorom (npr. meni, da je upravljavec neupravičeno zahtevo zavrnil, ali pa ni izpolnil, kar je posameznik zahteval), se lahko obrne na IP. Enako kot v primeru molka, če je posameznik vložil zahtevo za seznanitev z lastnimi osebnimi podatki, lahko svojo pritožbo vloži tudi na neobveznem obrazcu, ki ga je pripravil IP.

OBRAZEC:

➔ Pritožba zaradi kršitve pravice do seznanitve z lastnimi osebnimi podatki (obrazec P-SLOP).[24]

23 https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/Pritozba_zaradi_krsitve_pravice_do_seznanitve_z_lastnimi_osebnimi_podatki__Obrazec_P-SLOP.doc

24 Prav tam.

Kako posameznik obdrži nadzor, če njegovi podatki potujejo v ZDA, Indijo ali na Kitajsko?

Pri izmenjavi podatkov po elektronskih omrežjih zelo hitro pride do ‚prenosa osebnih podatkov v tretje države ali mednarodne organizacije'. To je na primer pogosto pri uporabi različnih spletnih storitev ponudnikov iz tretjih držav (ali pa ko na primer podjetja iz EU svoje spletne storitve gostujejo na strežnikih pri podjetjih v tretjih državah). Za tretje države se štejejo katerekoli države, ki niso članice EU in evropskega gospodarskega prostora (sem sodijo poleg EU članic še Norveška, Islandija ter Lihtenštajn). Do prenosa pride, ko osebni podatek prestopi meje omenjenih držav (npr. se hrani na strežnikih v Indiji). Za tovrstne prenose Splošna uredba predpisuje dodatne pogoje, ki bi zagotovili primerljivo raven varstva osebnih podatkov, kot ga zagotavlja posameznikom Splošna uredba.

Na kakšen način lahko posamezniki uresničujejo svoje pravice v primeru tovrstnega prenosa, je odvisno od konkretnih pogojev, pod katerimi so bili osebni podatki posredovani. O teh pogojih pa vas mora obvestiti upravljavec, ki podatke prenaša.

Več o prenosih osebnih podatkov v tretje države:

- Infografika IP: Prenos osebnih podatkov po Splošni uredbi v tretje države in mednarodne organizacije v dveh korakih[25]
- Smernice IP: Smernice glede prenosa osebnih podatkov v tretje države in mednarodne organizacije [26]
- Smernice IP: Računalništvo v oblaku [27]

25 https://www.ip-rs.si/fileadmin/user_upload/Pdf/infografike/Prenos_osebnih_podatkov_po_Uredbi_v_dveh_korakih.pdf

26 https://www.ip-rs.si/publikacije/prirocniki-in-smernice/smernice-glede-prenosa-osebnih-podatkov-v-tretje-drzave-in-mednarodne-organizacije-po-splosni-uredbi-o-varstvu-podatkov/

27 https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_Varstvo_osebnih_podatkov_in_racunalnistvo_v_oblaku_2016.pdf

Posameznik kot potrošnik

OGLAŠEVANJE

SPLOŠNO

Oglaševanje je temeljna dejavnost domala vsakega podjetja in tista podjetja, kjer so končni kupci posamezniki (potrošniki) je posebej občutljivo z vidika varstva osebnih podatkov. Zaradi vedno strožjih pogojev konkurence si podjetja izmišljajo najrazličnejše načine kako doseči svoje potencialne kupce. Zakonodaja posebej ureja obdelavo osebnih podatkov, ko gre za neposredno trženje in ko gre za uporabo določenih sledilnih tehnologij uporabnikov spleta (npr. piškotkov). V osnovi pa je treba pri tem še vedno spoštovati splošna pravila varstva osebnih podatkov (načelo obdelave v skladu z namenom zbiranja, načelo najmanjšega obsega podatkov, načelo omejitve shranjevanja itd.), ki jih določa Splošna uredba. Uporabo različnih oblik sledenja uporabnikov spleta in neposredno trženje prek elektronskih komunikacij, bo na novo uredila ePrivacy uredba, ki pa do izdaje teh smernic še ni bila sprejeta.

NEPOSREDNO TRŽENJE

Neposredno trženje je urejeno drugače, ko gre za neposredno trženje po navadni pošti in ko gre za neposredno trženje po različnih poteh elektronske komunikacije (telefonija, sms, e-maili, itd.). Nad neposrednim trženjem po poteh elektronske komunikacije izvaja nadzor Agencija za komunikacijska omrežja in storitve (AKOS).[28]

Kaj lahko naredite, če vas moti neposredno trženje?

Prvič, praviloma morajo podjetja za uporabo kontaktov za namen neposrednega trženja **pridobiti predhodno privolitev**, ki posamezniku zagotavlja najvišjo stopnjo obveščenosti in vpliva na obdelavo njegovih osebnih podatkov – posameznik mora biti **vnaprej seznanjen** in če se ne strinja, se obdelave ne sme izvesti. **Izjemoma**, ko so izpolnjeni določeni pogoji, ki jih predpisuje zakonodaja, je izvajanje neposrednega trženja dopustno **tudi brez predhodnega soglasja** ali privolitve. Tako je na primer neposredno trženje **po naslovljeni navadni pošti** dopustno brez predhodne privolitve na naslove, ki jih je upravljavec **pridobil iz javno dostopnih virov (npr. v telefonskem imeniku) ali v okviru zakonitega opravljanja dejavnosti**. Po **elektronski pošti** pa je brez vnaprejšnje privolitve dovoljeno trženje **podobnih izdelkov ali storitev** na **e-naslov kupcev** (torej oseb, ki so pri izvajalcu neposrednega trženja že kupili izdelek ali storitev in mu pri tem zaupali svoj e-naslov). Za neposredno trženje po drugih elektronskih komunikacijskih poteh (telefon, SMS, itd.) je **praviloma treba pridobiti predhodno soglasje**.

Drugič, zahteva se **visok nivo obveščenosti** posameznika. Posameznik mora biti seznanjen z **namenom** zbiranja njegovih podatkov za namen neposrednega trženja, **že v trenutku, ko podatke posreduje**. Informacije o tem morajo biti posamezniku predstavljene **jasno** in **pregledno** in to, da so bile informacije posredovane mora biti upravljavec sposoben dokazati.

Tretjič, če **posameznik ne želi (več) obveščanja**, **vedno lahko zahteva prenehanje** uporabe njegovega osebnega podatka za namen neposrednega trženja. **Vse preklice zahtev po prenehanju obveščanja morajo podjetja spoštovati**. Če upravljavec ne upošteva preklica ima posameznik možnost **vložiti prijavo, če gre za oglaševanje**:

- ➔ po navadni pošti **na IP** (gp.ip@ip-rs.si);
- ➔ po elektronski poti **na AKOS** (info.box@akos-rs.si).

28 http://www.akos-rs.si/

Če pa posameznik želi izvedeti, kje je upravljavec pridobil njegove osebne podatke, lahko nanj vedno naslovi tudi zahtevo za dostop do lastnih osebnih podatkov in zahteva želene informacije ali kopije osebnih podatkov, ki jih o njem upravljavec vodi (glej zgoraj - PRAVICA DO DOSTOPA ALI DO SEZNANITVE Z LASTNIMI OSEBNIMI PODATKI (člen 15).

OBRAZEC:

- Zahteva za prenehanje uporabe osebnih podatkov za namen neposrednega trženja[29]

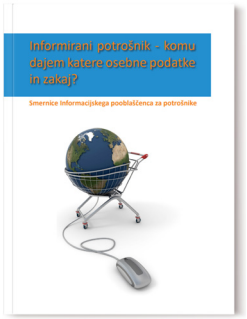
Več o tem:

- Spletna stran IP: Neposredno trženje[30]
- Spletna stran IP: Nezaželena elektronska sporočila (angl. spam) in slovenska zakonodaja[31]
- Smernice IP: Informirani potrošniki - komu dajemo katere osebne podatke in zakaj?[32]

DRUGE RAZLIČNE OBLIKE OGLAŠEVANJA (SMS OGLAŠEVANJE, VIRUSNI MARKETING, ITD.)

Obstajajo tudi druge različne oblike oglaševanja. Nekatere je IP opisal v že omenjenih smernicah: Informirani potrošniki - komu dajemo katere osebne podatke in zakaj? V omenjenih smernicah boste našli opise naslednjih oblik oglaševanja:

- klubi imetnikov kartic zvestobe,
- SMS klubi,
- bluetooth oglaševanje,
- virusni marketing.



29 https://www.ip-rs.si/fileadmin/user_upload/Pdf/obrazci/obrazec_za_zahtevo_Varuhu_pravic_Scit_zasebnosti.pdf

30 https://www.ip-rs.si/varstvo-osebnih-podatkov/inspekcijski-nadzor/najbolj-pogoste-krsitve/neposredno-trzenje/_

31 https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/#c410

32 https://www.ip-rs.si/publikacije/prirocniki-in-smernice/informirani-potrosniki-komu-dajemo-katere-osebne-podatke-in-zakaj/

NAGRADNE IGRE

Nagradne igre so pogost način pridobivanja osebnih podatkov za širitev baze potencialnih strank, ki jim podjetja lahko ponujajo svoje produkte. Pri tem je treba razumeti, da podjetja pri nagradnih igrah pogosto pogojujejo sodelovanje v nagradni igri s privolitvijo v neposredno trženje. V takšnem primeru, mora biti posameznik ustrezno seznanjen in aktivno izjaviti, da privoli v neposredno trženje - s čimer posledično pridobi možnost sodelovanja v nagradni igri. Ob tem je zelo pomembno, da so izpolnjeni pogoji za privolitev skladno s Splošno uredbo.

Več o tem:

- Spletna stran tiodlocas.si: Sodelovanje v nagradnih igrah[33]
- Smernice IP: Informirani potrošniki - komu dajemo katere osebne podatke in zakaj?[34]

33 https://tiodlocas.si/top-nasveti/sodelovanje-v-nagradni-igri/

34 https://www.ip-rs.si/publikacije/prirocniki-in-smernice/informirani-potrosniki-komu-dajemo-katere-osebne-podatke-in-zakaj/

KAJ SO ‘PIŠKOTKI’ O KATERIH ME SPLETNE STRANI NENEHNO OBVEŠČAJO?

‚Piškotki‘ so kratke besedilne datoteke, ki se naložijo na strojno opremo uporabnika spletne storitve in tako uporabnika »označijo«, da ga ciljna spletna stran ali aplikacija lahko »prepozna«. Nameni zakaj se ta tehnologija uporablja so lahko različni – od predizpolnjenih spletnih obrazcev do analize obiska spletne strani ali za namen oglaševanja različnih izdelkov ali storitev (zaradi prepoznave posameznika je lahko oglaševanje prilagojeno). V vseh primerih velja, da s tem, ko je uporabnik »označen« to omogoča, da se mu »sledi«. Ker gre za sledenje določljivemu posamezniku, gre za obdelavo osebnih podatkov, kjer je treba spoštovati pravila varstva osebnih podatkov. Tehnologija na področju »sledenja« uporabnikov spleta se bliskovito razvija in namestitev piškotkov je zgolj ena od možnih oblik sledenja. Opredelitev v zakonodaji je tehnološko nevtralna, kar vzpostavlja regulacijo nad več oblikami »sledilnih tehnologij«. Piškotki so zgolj ena od možnih tehnologij, ki pa je zelo razširjena in tudi zakonsko regulirana. Zaradi enostavnejšega razumevanja bomo v nadaljevanju razlage uporabljali pojem piškotek za vse oblike sledilnih tehnologij.

Zakonodaja za namestitev piškotkov praviloma zahteva prehodno privolitev posameznika, ki je skladna s splošnimi pravili varstva osebnih podatkov. Izjemoma v določenih primerih privolitev ni potrebna. V teh primerih je poseg v zasebnost manj invaziven.[35] V vsakem primeru – ne glede na to ali je za namestitev piškotkov potrebna predhodna privolitev – je treba posameznika o namestitvi piškotkov oziroma pred njo jasno in razločno obvestiti z obvestilom na spletni strani. Pogoji privolitve in obveznosti informiranja so po Splošni uredbi strožji kot prej in jih je treba upoštevati. Glede na smernice Evropskega odbora za varstvo podatkov v zvezi s privolitvijo, skladno z novo zakonodajo, pogojev ne zadovolji več zgolj obisk spletne strani oz. njena nadaljnja raba (npr. s pomikanjem navzdol ali podrsavanjem po spletišču oz t. i. »scrolling down«).

Več o tem:

- Spletna stran IP: Piškotki - odgovori na pogosta vprašanja[36]
- Spletna stran IP, obvestilo z javnost: Informacijski pooblaščenec se pridružuje tistim nadzornim organom, ki najavljajo posodobitev svojih smernic o uporabi piškotkov in podobnih tehnologij [37]

35 Aktualna ureditev po 157. členu ZEKom-1 ne zahteva predhodne privolitve, ko je to potrebno izključno zaradi prenosa sporočila po elektronskem komunikacijskem omrežju, ali če je to nujno potrebno za zagotovitev storitve informacijske družbe, ki jo naročnik ali uporabnik izrecno zahtevata.

36 https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/piskotki-odgovori-na-pogosta-vprasanja/

37 https://www.ip-rs.si/novice/informacijski-pooblascenec-se-pridruzuje-tistim-nadzornim-organom-ki-najavljajo-posodobit-1135/

POSAMEZNIK KOT UPORABNIK BANČNIH STORITEV

KDAJ BANKE ZBIRAJO OSEBNE PODATKE?

Banke zbirajo veliko osebnih podatkov od svojih strank in uporabnikov njihovih storitev. Že ob odpiranju bančnega računa posamezniki običajno izpolnjujejo različne obrazce, prek katerih se zbira več podatkov o njih. Vsakokrat, ko stranka želi na bančnem okencu opraviti storitev (npr. dvig gotovine), banka zahteva identifikacijo z osebnim dokumentom in bančno kartico. Za varno in zanesljivo poslovanje je seveda bistveno, da je banka prepričana o identiteti osebe, ki zahteva storitev, preden to storitev izvede. K takšnemu poslovanju pa jo zavezuje tudi zakonodaja, zato smejo finančne institucije kopirati in hraniti kopije osebnih izkaznic ali potnih listov svojih strank že na podlagi zakona.

Dodaten izziv v zvezi z identifikacijo predstavlja poslovanje na daljavo, npr. prek elektronske banke z mobilno napravo ali računalnikom. Da bi banka omogočila varno in zanesljivo poslovanje na daljavo, mora za identifikacijo prej zakonito pridobiti določene osebne podatke, ki jih lahko v fazi identifikacije primerja s podatki osebe, ki želi (oddaljeno) uporabljati njihovo storitev.

Kar največ podatkov pa banke zbirajo pri odobravanju posojil (kreditov), saj se morajo pred odobritvijo prepričati, da bo posojilojemalec sposoben vrniti odobreni znesek posojila. Tudi k temu jih zavezuje zakonodaja, hkrati pa je v tem tudi bistven poslovni interes banke, da zagotovi svoje delovanje. Večje kot je tveganje posojila, več informacij o posojilojemalcu zahteva banka. Tako na primer lahko banka zakonito pridobiva tudi podatke o preteklih izdatkih fizične osebe, kar sicer kaže na življenjski slog in lahko pove veliko o posamezniku.

Banke so pri opravljanju bančnih storitev podvržene številnim zakonskim zahtevam, tako za zagotavljanje varnega poslovanja in lastne stabilnosti (kot omenjeno zgoraj), kot tudi za druge javne interese, na primer preprečevanje pranja denarja in financiranja terorizma. Podatki v zvezi z bančnim poslovanjem so nedvomno bogat vir informacij za pristojne organe, ki preprečujejo kazniva ravnanja. Da lahko država zakonito in transparentno pride do kvalitetnih informacij, pa z zakonodajo nalaga določene obveznosti bankam in drugim finančnim institucijam, ki terjajo dodatno zbiranje (osebnih) podatkov od njihovih strank. Banke morajo za zadostitev tem obveznostim sprejeti interna pravila, ki omogočajo učinkovito zaznavanje sumljivih poslov – pri tem pa zbirajo tudi osebne podatke.

V zvezi z zakonitostjo zbiranja osebnih podatkov od svojih strank je IP odgovoril na mnoga vprašanja, med drugim:

- **Ali sme banka ob odpiranju osebnega računa za potrebe depozita, zahtevati podatke o statusu (poročeni ali ne), zaposlitvi, dolžini delovne dobe, številu članov gospodinjstva, izvršbah in dolgovih?** (mnenje št. 0712-1/2019/2504, z dne 5. 11. 2019)
- **Ali sme banka pregledati osebno izkaznico oziroma na drug način ugotavljati istovetnost?** (mnenje št. 07121-1/2020/198)
- **Ali sme banka po telefonu zahtevati davčno številko in EMŠO, da lahko pridobite izpisek?** (Mnenje št. 0712-1/2019/840, z dne 26.04.2019)
- **Ali lahko banka za odobritev kredita zahteva tudi podatke o življenjskih stroških?** (Mnenje št. 0712-3/2018/2671, z dne 31.12.2018)
- **Ali je banka upravičena do številke mobilnega telefona, za namen bančnega poslovanja v spletnem programu za dostop in uporabo mobilne in spletne banke?** (Mnenje št. 0712-1/2019/1841, z dne 07.08.2019)
- **Katere podatke banka zbira zaradi preprečevanja pranja denarja in financiranja terorizma?** (Mnenje št. 0712-1/2018/582, z dne 13.03.2018)
- **Ali lahko banka oz. hranilnica zahteva določene poslovne listine za preverjanje zakonitosti izvora denarja pred izplačilom gotovine?** (Mnenje št. 0712-1/2019/2609, z dne 18.11.2019)
- **Ali sme banka kopirati osebno izkaznico ali drug osebni dokument?** (Mnenje št. 07121-1/2020/48, z dne 16.01.2020)
- **Ali sme banka hraniti elektronsko kopijo osebne izkaznice?** (Mnenje št. 07121-1/2020/377, z dne 18.03.2020)
- **Ali sme banka zahtevati kopijo plačilnega lista?** (Mnenje št. 07121-1/2020/360, z dne 17.03.2020 IN mnenje št. 07121-1/2020/48, 16.01.2020)
- **Stranka želi urediti plačevanje prek »trajnika«. Katere podatke lahko zahteva banka in katere ponudnik (upnik, ki je upravičen do izplačil)?** (Mnenje št. 0712-3/2018/2707, z dne 07.01.2019)
- **Ali lahko zaposleni pri banki A, ki je povezana družba z banko B, dostopajo do osebnih podatkov strank banke B?** (Mnenje št. 0712-1/2019/2636, z dne 19.11.2019)
- **Ali sme banka pridobivati podatek o številu otrok v družini in to upoštevati pri kreditni sposobnosti?** (Mnenje št. 0712-1/2019/2530, z dne 7.11.2019)

KATERE SO OBVEZNOSTI BANK V ZVEZI Z INFORMIRANJEM POSAMEZNIKOV IN UVELJAVLJANJEM PRAVIC

Ker banke zbirajo mnoge osebne podatke za različne namene – tako lastne kot tudi v javnem interesu – je za posameznika ključno, da je jasno in razumljivo seznanjen s tem zakaj banka zbira določene njegove podatke in komu jih posreduje. V praksi so še vedno pogoste situacije, ko bančni uslužbenci preprosto ne vedo zakaj zbirajo konkretne podatke od posameznikov in zato odgovorijo: »Ker so nam tako naročili«. Splošna uredba pa nalaga obveznost bankam (in drugim upravljavcem), da zagotovijo te informacije posameznikom. Informacije morajo biti jasne in ne »skrite v pogojih poslovanja«. Informacije morajo biti tudi razumljive posamezniku, torej prilagojene glede na to kdo je naslovnik teh informacij. Informacije morajo banke zagotoviti proaktivno – torej same, hkrati pa ima posameznik možnost informacije pridobiti tudi na zahtevo.

Posameznik lahko pri banki, kot upravljavcu osebnih podatkov uveljavlja vse zgoraj opisane pravice po Splošni uredbi (pravico dostopa, popravka, izbrisa, omejitve, prenosljivosti, ugovora-kjer bo ustrezno). Če bi posameznik želel popravek ali izbris njegovih podatkov iz centralnega kreditnega registra (ker npr. netočni ali zastareli podatki vplivajo na njihovo kreditno oceno in s tem sposobnost za pridobitev bančnega posojila) lahko posameznik uveljavlja te svoje pravice pri Banki Slovenije na podlagi Zakona o centralnem kreditnem registru.

Pomembna vprašanja se nanašajo tudi na dostopanje do podatkov o transakcijah za dediče pokojnega zapustnika. Na tem področju velja, da so dediči (prvega dednega reda) upravičeni dostopati do osebnih podatkov zapustnika, če ta ni izrecno prepovedal dostopa do njegovih podatkov v času svojega življenja. Dediči pa morajo izkazati pravni interes. Na to temo je bilo izdanih tudi nekaj mnenj in nekatere omenjamo spodaj.

V zvezi z uveljavljanjem pravic na področju varstva osebnih podatkov je IP izdal tudi več mnenj, v katerih je odgovoril tudi na spodnja vprašanja:

- Ali lahko posameznik po zaprtju svojega tekočega računa zahteva izbris njegovih podatkov o transakcijah pri banki? (Mnenje št. 0712-1/2018/575, z dne 13.03.2018)
- Ali lahko posameznik pridobi podatek o tem, kdo pri banki je vpogledal v njegov tekoči račun? (Mnenje št. 0712-1/2019/2330, z dne 15.10.2019)
- Ali sme banka klicati posameznike za preverjanje zadovoljstva svojih strank? (Mnenje št. 0712-1/2019/1695, z dne 17.07.2019)
- Kako lahko posameznik zahteva izbris ali popravek svojih podatkov v centralnem kreditnem registru? (Mnenje št. 0712-1/2019/1583, z dne 02.07.2019)
- Kakšna so pravila glede avtomatiziranega odločanja za banke? (Mnenje št. 0712-1/2019/83, z dne 20.02.2019)
- Ali lahko posameznik zahteva od banke, da se izključi prikaz stanja na bankomatu po opravljeni transakciji? (Mnenje št. 0712-3/2018/2575, z dne 14.12.2018)
- Pod katerimi pogoji lahko hči vpogleda v bančne podatke svojega pokojnega očeta? (Mnenje št. 0712-1/2019/2814, z dne 06.12.2019)
- Ali lahko posameznik za časa življenja prepove dostop do njegovih osebnih podatkov tudi dedičem? (Mnenje št. 0712-1/2019/934, z dne 24.04.2019)

IZBRIS IZ SPLETA

Kako dosežem odstranitev vsebine iz spleta?

Izbris vsebine iz spletnega mesta lahko posameznik zahteva, kadar so izpolnjeni pogoji za izbris podatkov skladno s členom 17 Splošne uredbe. Izbris je treba zahtevati od upravljavca – kar je v primeru objav na spletu, ponudnik vsebin (npr. lastnik spletne strani, spletnega foruma, družabnega omrežja). Če upravljavec zavrne izbris, se lahko posameznik obrne na IP.

Pod določenimi pogoji lahko izbris zahtevate tudi od ponudnika gostovanja, torej tistega pri katerem spletna stran gostuje. Gre za posebno pravico po določbah Zakona o elektronskem poslovanju na trgu. V primeru zavrnitve se lahko posameznik obrne na sodišče.

Več o tem:

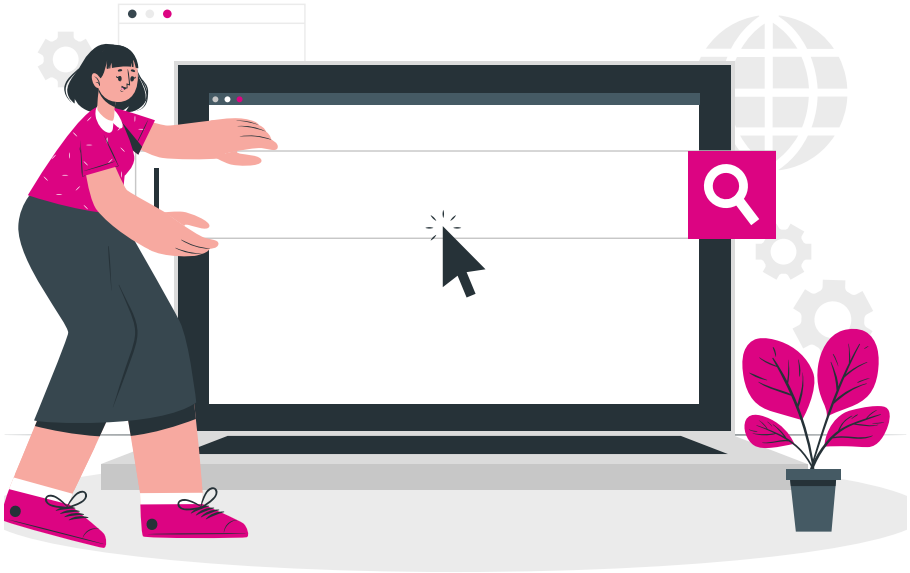
- Spletna stran IP: Želim izbrisati svoje podatke[38]
- Spletna stran IP: Kako dosežem, da se s spletne strani umaknejo moji protipravno objavljeni osebni podatki?[39]
- Spletna stran IP: Kako odstranim zadetke spletnega iskalnika, če izvirne strani ni več na internetu?[40]

Ali lahko dosežem izbris povezav do spletnih objav IN kako?

Pri ponudnikih storitev spletnih iskalnikov (npr. Google, Bing, Yahoo, itd.) je možno je doseči izbris povezav do objavljenih vsebin na spletu pod pogojem, da je posameznik upravičen do izbrisa njegovih osebnih podatkov. V praksi ponudniki spletnih iskalnikov, ki so uskladili svoje poslovanje s pogoji Splošne uredbe, ponujajo možnost vložitve spletnega zahtevka za izbris povezav. Praktičen opis, kako zahtevati izbris povezav pri Google iskalniku najdete v smernicah O orodjih za zaščito zasebnosti na internetu,[41] str. 15.

Več o tem:

- Smernice IP: O orodjih za zaščito zasebnosti na internetu[42]



38 https://tiodlocas.si/zelim-izbrisati-svoje-podatke/

39 https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/#c1098

40 https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/#c793

41 https://www.ip-rs.si/index.php?id=886

42 https://www.ip-rs.si/index.php?id=886

SNEMANJE TELEFONSKIH KLICEV

»Vaš klic se snema zaradi višje kakovosti storitev«. Ali je snemanje dopustno?

Snemanje telefonskih klicev za namen »izboljšanja kakovosti storitev« praviloma ne bo zadostovalo za zakonitost snemanja. To je dovoljeno, če je telefonski pogovor edini dokaz o sklenitvi, spremembi ali prekinitev posla (npr. nakupa blaga prek telefona), ni pa dovoljeno snemati splošnih klicev za informacije (o ponudbi, zalogah ipd.).

Vse oblike nadzora oziroma prestrezanja komunikacij, kot so poslušanje, prestrezanje, snemanje, shranjevanje in posredovanje komunikacij, ki jih izvajajo tretje osebe in te niso uporabniki, so načeloma prepovedane, dopustne pa le izjemoma pod zakonsko določenimi pogoji. Snemanje je na primer lahko dopustno za klice na:

- na urgentno telefonsko linijo policije,
- na urgentno telefonsko linijo za nujno zdravniško pomoč,
- na urgentno telefonsko linijo gasilske ali druge organizacije za zaščito in reševanje,
- telefonsko številko pri teleoperaterju, namenjeno sklepanju ali spreminjanju naročniških razmerij preko telefona,
- telefonsko številko pri banki, namenjeno odpiranju ali spreminjanju tekočega računa,
- itd.

Zakon o elektronskih komunikacijah (ZEKom-1) za javni sektor določa, da lahko snemanje izvajajo organizacije in državni organi, ki so pristojni za izvajanje obveščevalnih in varnostnih nalog, nalog policije, obrambe in zaščite, reševanja in pomoči pod pogojem, da so kličoči uporabniki predhodno obveščeni o snemanju, njegovem namenu in trajanju hranjenja posnetka (npr. avtomatski odzivniki). Za zasebni sektor ZEKom-1 določa, da se lahko telefonske klice snema, kadar je za izvajanje zakonite poslovne prakse treba zagotoviti dokaz o tržni transakciji ali kateri koli drugi poslovni komunikaciji, ki se nanaša na sklenitev, spremembo ali prekinitev posla. Ni pa nujno, da se telefonski pogovor začne snemati na začetku in da se snema ves čas.

Posebej pomembno je, da so kličoči uporabniki predhodno obveščeni o snemanju, njegovem namenu in trajanju hranjenja posnetka (npr. avtomatski odzivniki).

Ali obstajajo primeri, ko predhodno obvestilo ni potrebno?

ZEKom-1 načeloma glede obveznosti obveščanja o snemanju ne določa nobenih izjem, vendar - kot izhaja iz Smernic o snemanju telefonskih klicev,[43] ki jih je IP pripravil skupaj z AKOS, ki pokriva tudi področje snemanja telefonskih klicev – IP meni, da je v izjemnih primerih lahko utemeljeno, da se o snemanju klicev posameznikov ne obvešča. Primeri morajo biti skrbno pretehtani in utemeljeno mora biti, da je snemanje dejansko potrebno oziroma dejansko pomaga pri uresničevanju ciljev. Primeri, ko je to lahko dopustno so: telefonske linije za urgentno zdravniško pomoč, policijo ali reševanje, ker bi se s tem pridobilo čas za ukrepanje; telefonska linija za pomoč ljudem, ki so v hudih duševnih stiskah, so depresivni ali celo nameravajo storiti samomor, da jih obvestilo, ne bi odvrnilo od iskanja pomoči. Seznam ni izčrpen, vendar mora biti vsaka tovrstna odločitev posebej utemeljena in pretehtana v konkretnem primeru.

Kako se v praksi zagotavlja, da so posneti samo tisti klici, kjer gre za dokazovanje posla?

Ena od možnosti so v praksi pogosto uporabljani avtomatski odzivniki, ki posameznika preusmerijo glede na naravo klica, npr. »Pritisnite 1, če želite splošne informacije.« in »Pritisnite 2, če želite opraviti nakup.« ali »Pritisnite 3, če želite podati reklamacijo«. V navedenem primeru se lahko snemajo tisti klici, ki se nadaljujejo s pritiskom na 2 ali 3, seveda pa mora biti klicatelj v teh primerih obveščen o dejstvu snemanja, namenu snemanja in trajanju hrambe posnetka.

Kaj pa, če posameznik pokliče na splošno telefonsko številko, med pogovorom pa se ugotovi, da je snemanje potrebno zaradi sklenitve posla? V tem primeru bi bila ustrezna praksa, da se posameznika po tem, ko izrazi namero za sklenitev posla, obvesti, da bo od takrat naprej klic posnet (zaradi dokazovanja o sklepanju

43 Str. 13, https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_snemanju_telefonskih_klicev.pdf,

pogodbe), ter da se ga obvesti o namenu snemanja in trajanju hrambe posnetka. Ni pa dopustno snemati klicev, če posamezniki iščejo zgolj splošne informacije.

»Vaš klic se ‚lahko' snema« – kaj pa če se ne?

V praksi se pojavljajo tudi primeri, ko upravljavci predvajajo obvestilo, da se klici »lahko« snemajo, ker to po njihovih izkušnjah zmanjša število žaljivih, neprimernih in včasih tudi grozilnih klicev. Ali je takšna praksa sporna, če se v resnici klicev sploh ne snema?

IP poudarja, da namen predhodnega obvestila o snemanju telefonskih klicev ni »zastraševanje« kličočih, temveč transparentno delovanje upravljavca do posameznika. Nepošteno je namreč zlorabljati institut transparentnega informiranja, z zavajanjem vseh kličočih s tem, da se klice snema (čeprav se ne) – tudi če je namen v ozadju, da se odvrne osebe, ki bi bile žaljive ali bi se drugače neprimerno sporazumevale. Praktično vse organizacije se v večji ali manjši meri soočajo s klici, ki so (subjektivno ali objektivno) žaljivi, neprimerni in včasih tudi grozilne narave. Kljub temu pa ni sprejemljivo, da se zgolj zaradi možnosti, da bo prišlo do neprimernega klica, zavaja vse klicatelje. Po drugi strani pa je lahko dopustno, da se osebo, ki se vede žaljivo ali grozilno, opozori, da se bo od tistega trenutka naprej, če bo oseba nadaljevala z žalitvami ali grožnjami, pogovor posnel – in se to tudi izvrši. Ni pa primerno, če se opozorilo za snemanje uporablja z namenom zastraševanja klicateljev na splošno, temveč le takrat, kot gre v konkretnem primeru za objektivno žaljiv ali grozilen pogovor.

Ali lahko kot kličoči izveste, ČE se pogovor snema?

Posamezniki imajo v okviru pravice dostopa skladno s Splošno uredbo (glej zgoraj) možnost od upravljavca med drugim pridobiti tudi informacije o tem, ali v zvezi z njimi obdeluje osebne podatke. Snemanje telefonskih klicev praviloma štejemo za obdelavo osebnih podatkov, zato imajo posamezniki od upravljavca pravico pošteno in transparentno izvedeti, če se pogovor snema.

Več o snemanju telefonskih klicev:

➔ Smernice IP: Smernice o snemanju telefonskih klicev[44]

44 https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_snemanju_telefonskih_klicev.pdf

DIGITALNA TELEVIZIJA

Digitalna televizija predstavlja enega od več zaslonov, ki jih vsakodnevno uporabljamo in omogoča upravljavcem zbiranje množice osebnih podatkov od svojih gledalcev/poslušalcev. Njena bistvena kvaliteta z vidika varstva osebnih podatkov je njena interaktivnost, saj mogoča spremljanje kaj uporabniki gledajo, v katerem času, itd. Pametne televizije se po svojih funkcionalnostih skoraj ne razlikujejo več od osebnega računalnika, tablice ali pametnega telefona saj omogočajo dostop do spleta in brskanje po njem, predvajanje video in avdio vsebin in uporabo različnih spletnih aplikacij, ki ponujajo zlasti pretočne video in avdio vsebine. Vse navedeno korenito spreminja našo uporabo televizije in hkrati tehnološko omogoča širokemu spektru upravljavcev dostop do naših osebnih podatkov, ki lahko definirajo naše interese, želje, hotenja ali pričakovanja.

Varstvo osebnih podatkov se pri tem kaže kot ključna točka, ki na zakonodajni in izvršilni ravni zagotavlja posameznikom določeno mero nadzora in vpliva nad tem, kako bodo upravljavci zbirali osebne podatke in jih nadalje obdelovali. Prvi problem je v transparentnosti obdelave osebnih podatkov. Zaradi množice upravljavcev – od tistih, ki zagotavljajo televizijski program (izdajatelji TV programov, operaterji), do ponudnikov pretočne video in avdio vsebine in drugih aplikacij, ki imajo tehnično sposobnost spremljati posameznikove aktivnosti v zvezi s TV napravo – je za posameznika težko ugotoviti že to, kdo vse o njih vodi osebne podatke, ki se zbirajo prek njegove TV naprave. Še težje pa je ugotoviti zakaj. Če smo kot uporabniki naklonjeni zlasti k hitremu dostopu do želenih vsebin in se ne »obremenjujemo z drobnim tiskom«, lahko relativno hitro podamo privolitev za obdelavo naših osebnih podatkov, ki je sicer zavestno ne bi podali. Ob tem velja poudariti, da Splošna uredba zahteva od upravljavcev, da jasno in razumljivo predstavijo posamezniku kaj bodo počeli z njegovimi osebnimi podatki. To od upravljavcev terja visoko stopnjo aganžmaja. Kljub temu, pa tudi stroga zakonodaja ne more preprečiti ignorance ljudi, ki slepo delijo svoje podatke, brez kančka zanimanja za to – kdo zbira, katere podatke, za katere namene, s kom jih deli, itd.

V zvezi z uporabo digitalne televizije velja izpostaviti še pravico posameznika do prenosljivosti osebnih podatkov (več o tej pravici, glej odsek: Pravica do prenosljivosti).

Primer: *uporabnik pretočnih video in avdio vsebin želi zamenjati ponudnika (npr. iz Netflix na HBO). Nov ponudnik posamezniku ponuja naročnino po znižani ceni, če bi posameznik prenesel na novega ponudnika tudi svoje osebne podatke, ki jih je o njem zbral sedanji izbrani ponudnik. Pravica do prenosljivosti omogoča, da posameznik od (starega) ponudnika zahteva, da (novemu) ponudniku omogoči prevzem posameznikovih osebnih podatkov v strojno berljivi obliki.*

OBRAZEC:

➔ Zahteva za prenosljivost (obrazec ZPP).[45]

Več o obdelavi osebnih podatkov pri uporabi digitalne televizije:

➔ Smernice IP: Smernice glede varstva zasebnosti pri digitalni televiziji[46]

45 Zahteva za prenosljivost (obrazec ZPP), https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/Zahteva_za_prenosljivost_podatkov_Obrazec_ZPP.docx.

46 https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice__DTV.pdf

Posameznik kot zaposleni ali iskalec zaposlitve

KATERE VSE PODATKE ZBIRAJO DELODAJALCI?

Posameznik v razmerju do delodajalca lahko nastopa kot zaposleni ali iskalec zaposlitve. Poleg »klasičnih« osebnih podatkov, kot so EMŠO in davčna ter podatki o plačah ter evidence delovnega časa, sodobni trendi izvajanja delovnih obveznosti povečujejo uporabo interneta, elektronske pošte, mrežnih tiskalnikov, različnih vozil, stacionarne in mobilne telefonije, magnetnih/RFID kartic za odpiranje vrat ali druge elektronske opreme ali storitve. Pri uporabi navedenih storitev praviloma nastajajo razne zbirke podatkov ali pa se podatke zgolj avtomatizirano obdeluje, te podatke pa je tehnično izvedljivo spremljati ali analizirati. Ko je na podlagi zbranih podatkov možna določljivost zaposlenih (kar praviloma je) – podatki predstavljajo osebne podatke, njihova obdelava pa mora biti skladna s pravili varstva osebnih podatkov, kot jih določa Splošna uredba in področna zakonodaja. Ker je zaposleni v razmerju do delodajalca vselej v podrejenem položaju, je treba biti pri obdelavi osebnih podatkov še posebej pazljiv in skrben, da se z obdelavo sorazmerno in upravičeno posega v posameznikuzagotovljene pravice ali svoboščine. Število in obseg zbirk, ki nastaja pri delodajalcu je praviloma občutno večji od zgolj tistih, ki jih delodajalci vodijo zaradi svojih zakonskih obveznosti (na primer po Zakonu o evidencah na področju dela in socialne varnosti).[47]

Več o obdelavi osebnih podatkov v delovnih razmerjih:

- ➔ Priročnik IP: Kako so moji podatki varovani v delovnem razmerju (Priročnik o varstvu osebnih podatkov)
- ➔ Smernice IP: Varstvo osebnih podatkov v delovnih razmerjih[48]

PRAVICE POSAMEZNIKOV V DELOVNIH RAZMERJIH

Posamezniki imajo na voljo različne pravice na področju varstva osebnih podatkov s pomočjo katerih lahko izvedo, kako obdeluje njihove osebne podatke njihov delodajalec, na primer:

- **Ali podjetje izvaja videonadzor in za kakšen namen?**
- **Ali je v službenih vozilih vstavljen GPS in kakšni so pogoji uporabe (kdo pregleduje, zakaj, itd.)?**
- **Ali delodajalec spremlja aktivnosti zaposlenih na spletu prek službenih naprav in katere podatke spremlja?**
- **Ali ima delodajalec zagotovljeno elektronsko evidenco vpogledov v sistem beleženja prihodov in odhodov?**
- **Ali ima sprejete interne akte, ki opredeljujejo pogoje uporabe posameznih sledilnih tehnologij?**

Zaposleni, ki je v dvomu, se lahko glede posameznih vprašanj obrne tudi na pooblaščeno osebo za varstvo osebnih podatkov pri podjetju (če je imenovana) in ta mu mora zagotavljati zaupnost.

Več o pravicah posameznikov v zvezi z varstvom osebnih podatkov v delovnih razmerjih:

- ➔ Priročnik IP: Kako so moji podatki varovani v delovnem razmerju? (Priročnik o varstvu osebnih podatkov)

47 Zakon o evidencah na področju dela in socialne varnosti (Uradni list RS, št. 40/06).

48 https://www.ip-rs.si/publikacije/prirocniki-in-smernice/varstvo-osebnih-podatkov-v-delovnih-razmerjih/

PRAKSE OBDELAV OSEBNIH PODATKOV V DELOVNIH RAZMERJIH

Ali sme delodajalec izvajati videonadzor nad svojimi zaposlenimi?

Videonadzor je znatnejši poseg v zasebnost, zato je videonadzor delovnih prostorov (kjer zaposleni opravljajo delo) dopusten le izjemoma, ko:

- **(1) ne obstaja milejši ukrep za dosego istega cilja IN**
- **(2) le zaradi varnosti ljudi ali premoženja, ali pa, če je treba varovati tajne podatke stopenj tajnosti tajno ali strogo tajno ter poslovno skrivnost.**

Delodajalec, ki izvaja videonadzor delovnih prostorov se mora še pred uvedbo posvetovati z reprezentativnim sindikatom o nujnosti uvedbe takšnega videonadzora, če tak sindikat pri njem obstaja. Če delodajalec konkretno ne izkaže, da je videonadzor nujen zaradi varnosti ljudi ali premoženja, varovanja tajnih podatkov ali poslovnih skrivnosti, potem takšnega videonadzora ne sme uvesti. Manj strogo pa velja za snemanje vhodov v poslovne stavbe, ki niso »delovni prostor«.

Pravice zaposlenih v zvezi z videonadzorom

Pri videonadzoru je zelo pomembno, da so zaposleni o tem obveščeni. Zaposleni morajo biti obveščeni o njegovem izvajanju pisno, še pred začetkom izvajanja videonadzora. Na vidnem mestu v prostoru, kjer se izvaja videonadzor mora biti izpostavljeno tudi obvestilo. Obveznost informiranja, ki mora biti skladno s Splošno uredbo zagotovljena posameznikom v zvezi z videonadzorom je širša, kot jo zahteva ZVOP-1.

Delodajalec je zasposlene in druge, ki se nahajajo na posnetkih dolžan obvestiti o tem:

- **Za kateri namen izvaja videonadzor?**
- **Kdaj in pod kakšnimi pogoji bo lahko pregledoval videonadzorne posnetke in kako bo zagotovil sledljivost vpogledov (opredelitev organizacijskih in tehničnih ukrepov za varnost)?**
- **Kakšen je rok hrambe posnetkov?**
- **Komu bo podatke posredoval in za kakšen namen?**
- **Katere so pravice zaposlenih v zvezi z izvajanjem videonadzora?**

Čeprav Splošna uredba videonadzora posebej ne ureja, pa s svojimi zahtevami po transparentni obdelavi osebnih podatkov in zagotavljanjem pravic posameznikom pomembno vpliva na izvajanje videonadzora prav v zvezi z uveljavljanem pravic posameznikov.

Primer: *v velikem podjetju pride do nesreče na delovnem mestu. Delovno mesto je pod videonadzorom. Zaposleni želi dobiti odškodnino od svojega delodajalca zaradi neustreznih varnostnih ukrepov. Delodajalec mu ne želi izročiti videonadzornega posnetka v okviru njegove pravice do dostopa, zato delavec zahteva omejitev obdelave do rešitve spora na sodišču.*

V praksi bo prišla v poštev tudi pravica do ugovora

Primer: *Podjetje na območju svojega parkirišča uvede videonadzor zaradi suma na neupravičeno uporabo parkirnih mest v lasti podjetja za zasebne namene zaposlenih in njihovih bližnjih. Kot pravno podlago delodajalec navede svoj zakoniti interes (člen 6(1)(f) Splošne uredbe). Sindikat, ki deluje pri podjetju, takšnemu videonadzoru nasprotuje, zato v po pooblastilu v imenu zaposlenih vloži ugovor skladno členom 21 Splošne uredbe.*

Kdaj sme delodajalec uvesti GPS za sledenje zaposlenim?

GPS sodi med najbolj uveljavljene tehnologije za pozicioniranje, sledenje in nadzor oseb, predmetov in vozil. Gre za satelitski navigacijski sistem, ki se uporablja za določanje natančnega položaja in časa kjerkoli na Zemlji. Zaradi odsotnosti posebne zakonske ureditve uporabe GPS sistemov je **pri GPS sledenju najpomembnejša predhodna ocena - ali in pod kakšnimi pogoji bi bila uporaba GPS naprav poštena, zakonita, transparentna, sorazmerna in varna**. Uvedba GPS sledenja v delovnih razmerjih je dopustna le izjemoma in se priporoča predhodna izvedba t.i. ocene učinkov,[49] ki omogoča predhodni premislek o bistvenih vprašanjih s področja varstva osebnih podatkov.

Več o oceni učinkov:

➔ Spletna stran IP: Ocena učinka v zvezi z varstvom podatkov[50]

➔ Smernice IP: Smernice o ocenah učinkov na varstvo podatkov[51]

Uporaba sledilnih naprav za nadzor nad zaposlenimi – bodisi da gre za naprave v vozilih, paketih ali celo na telesih zaposlenih - je lahko sporna predvsem zaradi posega v pravice zaposlenih in možnosti neupravičenega in nesorazmernega sledenja s strani delodajalca, in sicer na podlagi osebnih podatkov o njihovih lokacijah. Takšno sledenje je zato lahko dopustno le takrat, »kadar istega namena, zaradi katerega se uvede sledenje, ni mogoče doseči z milejšimi sredstvi, ki v manjši meri posegajo v varstvo osebnih podatkov in zasebnost zaposlenih«.

Primer: *Podjetje želi v vsa službena vozila, tudi v tista, ki se uporabljajo za zasebne namene kot boniteta, vgraditi GPS sistem za sledenje vozilu. Opredeljeni nameni so: varnost in zaščita opreme ter dokumentov delodajalca, ki se nahajajo v navedenih vozilih; preprečevanje protipravnega odvzema vozila; varnost zaposlenih; določitev lokacije v primeru prometne nesreče.*

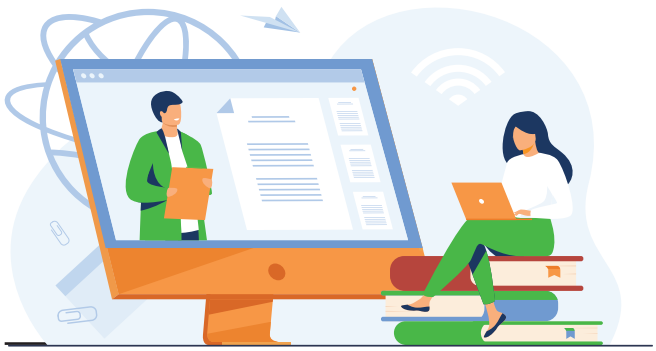
Primer opisuje sledenje vsem službenim vozilom, na splošno, kar ni dopustno. Uporaba GPS sledilne naprave bi lahko bila dopustna, če bi obstajali na primer posebej utemeljeni razlogi za uvedbo GPS(npr. prevoz nevarnih snovi, premoženja visoke vrednosti ipd.). Tudi v takšnih primerih, pa bi moral upravljavec uvesti ustrezne ukrepe za zmanjševanje tveganj za neupravičen poseg v pravice in svoboščine posameznikov, kot npr.:

- da se sistem sledenja vklopi zgolj ob vnaprej predvidenih tveganih vožnjah,
- da je tovrstna službena pot določena vnaprej;
- pri vozilih, ki se uporabljajo tudi za zasebne namene, mora imeti zaposleni med zasebnimi vožnjami možnost izklopiti sistem z uporabo posebnega stikala v vozilu, tudi če bi sicer šlo za vožnjo, pri kateri bi bila uporaba GPS dopustna;
- da so z internim aktom, natančno predpisani pogoji uvedbe GPS tehnologij in pogoji pregledovanja ter obdelav podatkov v zbirkah nastalih z zbiranjem GPS signalov.

Kot že večkrat poudarjeno v pričujočih smernicah, je transparentnost do posameznikov ključnega pomena za skladno obdelavo osebnih podatkov. Zaposleni morajo biti seznanjeni z vsemi vidiki pomembnimi vidiki varstva osebnih podatkov, ki jih določa Splošna uredba (glej zgoraj: Transparentna obdelava osebnih podatkov). V zvezi z uvedbo GPS sledenja je torej ključnega pomena, da so posamezniki seznanjeni z nameni uvedbe GPS tehnologij, pogoji pregledovanja zbirk nastalih z zbiranjem GPS signalov ter drugimi pomembnimi informacijami v zvezi z obdelavo osebnih podatkov zaposlenih.

Več o uvedbi GPS tehnologije z vidika varstva osebnih podatkov:

➔ Smernice IP: Uporaba GPS sledilnih naprav in varstvo osebnih podatkov Smernice Informacijskega pooblaščenca[52]



49 Več o oceni učinkov: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/ocena-ucinka-v-zvezi-z-varstvom-podatkov/

50 Prav tam.

51 https://www.ip-rs.si/publikacije/prirocniki-in-smernice/ocene-ucinkov-na-varstvo-podatkov/

52 https://www.ip-rs.si/publikacije/prirocniki-in-smernice/uporaba-gps-sledilnih-naprav-in-varstvo-osebnih-podatkov/

Na kaj je treba paziti, ko zaposleni uporablja lastno napravo (BYOD)?

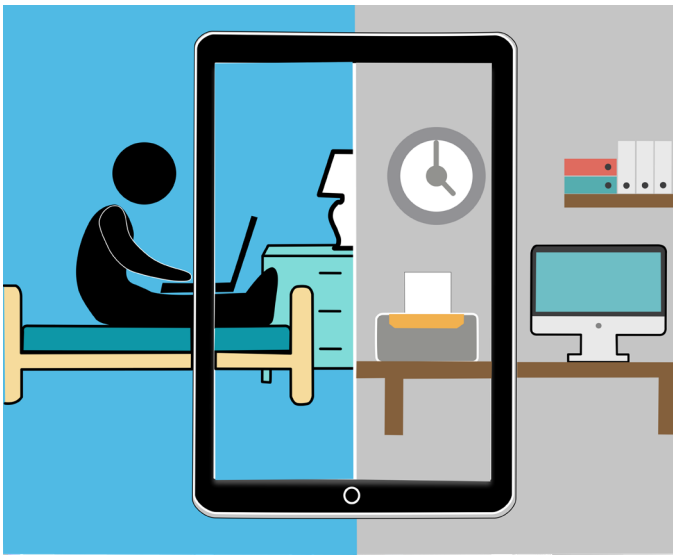
»*Bring Your Own Device*« **(BYOD)** je praksa, **ko zaposleni v službena okolja prinašajo svoje zasebne naprave (prenosnike, tablice, pametne telefone)**, prek katerih potem dostopajo do poslovnih, osebnih in drugih podatkov v informacijskem sistemu organizacije. Posledično so možnosti organizacije za nadzor nad varnostjo določene naprave in podatkov, ki so dostopni prek nje, pomembno omejene. Pravil, ki sicer veljajo za službeno opremo, namreč ni dopustno nediskriminatorno uveljaviti tudi za zasebno opremo. Velik del vprašanj glede BYOD je tako povezan z vidiki informacijske varnosti. Ker so BYOD naprave praviloma manj varne, je tudi zaposleni izpostavljen večjemu tveganju, da delodajalec zoper njega uvede različne disciplinske ali druge ukrepe oziroma se prek njega želi razbremeniti odgovornosti ko pride do varnostnega incidenta na njegovi napravi (na primer nepooblaščen dostop ali izguba podatkov zaradi izgube oziroma kraje naprave, hekerski vdor,itd.). Vse navedeno predstavlja povečano tveganje tako za delodajalca kot tudi za zaposlenega, zato je zelo pomembno, da se oba zavedata tveganj in da so jasna pravila glede uporabe BYOD naprave vnaprej opredeljena v internih aktih – s katerimi je zaposleni tudi dobro seznanjen.

Drugi del vprašanj pa se nanaša na spoštovanje delavčeve zasebnosti in varstva osebnih podatkov. Za zagotovitev varstva osebnih podatkov in zasebnosti zaposlenega mora biti jasno opredeljena ločnica med: (1) osebnimi podatki uporabnika naprave in drugih oseb, ki lahko uporabljajo napravo (npr. družinski člani); in (2) osebnimi podatki, s katerimi upravlja organizacija in do katerih ima uporabnik dostop preko BYOD naprave. Če ta ločnica ni jasno zarisana, z ustreznimi tehničnimi in organizacijskimi ukrepi (npr. internimi pravilniki o uporabi – kdaj, kako, katere podatke, za katere namene; ločevanje poslovnega in zasebnega načina delovanja, itd.), potem v praksi lahko prihaja še do večjih težav.

Primer: *Delavec ima na svoji BYOD napravi pomemben poslovni imenik kontaktov poslovnih partnerjev in strank, vendar zaradi daljše odsotnosti iz zdravstvenih razlogov ni dosegljiv. Ali bi delodajalec lahko oddaljeno dostopil do njegove naprave in posledično pridobil želene podatke? Odgovor na vprašanje ni enostaven in vselej odvisen od konkretnih okoliščin, kot je npr. stopnja nujnosti pridobitve kontaktov, vnaprej opredeljenih postopkov s katerimi mora biti zaposleni praviloma seznanjen, itd. Pri tem velja vodilo, da se mora pri uporabi BYOD delodajalec izogibati vsakršnemu dostopu do zasebnega dela ali zasebnega načina delovanja naprave, kot na primer podatkov kdo je kdaj koga klical, katere spletne strani je obiskoval, s kom, kdaj in kaj je komuniciral, kje in kdaj se je gibal, zasebni korespondenci, datotekam in aplikacijam zasebne narave.*

Več o varstvu osebnih podatkov v zvezi z BYOD:

- Smernice IP: Smernice o uporabi zasebnih naprav v službene namene (BYOD) [53]
- Spletna stran z informacijami o delu na daljavo v čas epidemije COVID-19[54]



53 https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_BYODweb.pdf

54 https://www.ip-rs.si/index.php?id=897

Posameznik v javnem sektorju

POSEBNOSTI V ZVEZI Z OBDELAVO OSEBNIH PODATKOV, KI JO IZVAJA JAVNI SEKTOR

Država v širšem pomenu besede deluje prek mnogih služb, ki odločajo o pravicah iz javnih sredstev, zagotavljajo varnost in mir, nudijo zdravstveno oskrbo, izobraževalne storitve, socialno pomoč in podporo, idr. Skupno vsem tem službam je, da so njihove javne naloge posebej regulirane z zakonodajo in da so financirane iz javnih sredstev. Narava obdelav osebnih podatkov v javnem sektorju je tudi, da je posledica oblastnega delovanja. Posameznik na primer ne more policistu zavrniti vpogleda v osebne podatke na vozniškem dovoljenju, ko policist to zahteva pri izvajanju svojih nalog. Gre torej za obdelave, ki jih predpisuje zakon in na katere posameznik praviloma nima vpliva oziroma so njegove pravice v teh primerih lahko tudi omejene. Omejitve pravic pa morajo biti predpisane z zakonom in zgolj iz določenih razlogov, ki jih opredeljuje Splošna uredba (npr. državne varnosti; obrambe; javne varnosti; preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem, itd.). Tako na primer osebe, ki ji tajno prisluškuje policija zaradi odkrivanja kaznivega dejanja, policija ni dolžna predhodno obvestiti o zbiranju podatkov niti ta oseba nima pravice dostopa do podatka o tem, da se tajno prisluškovanje izvaja, saj bi to škodilo izvedbi policijskega postopka. Omejitve pravic so torej odvisne od narave in potreb posameznih postopkov oziroma obdelav, ki se izvajajo v javnem sektorju. Posebnosti po posameznih področjih (zdravstvo, šolstvo, socialno delo, policija, itd.) so opisane v nadaljevanju.

Vsesplošni trend informatizacije vpliva tudi na storitve javnega sektorja, ki za učinkovitejše izvajanje svojih nalog vpeljuje različne informacijske sisteme, ki omogočajo ‚povezovanje zbirk podatkov', ‚oddaljen dostop', ‚avtomatizirano odločanje v posamičnih zadevah', itd. Vse navedeno vsekakor pripomore k učinkovitosti delovanja javnega sektorja, hkrati pa prinaša tudi pomembna tveganja, ki jih morajo upravljavci in obdelovalci ustrezno nasloviti pred vpeljavo novih rešitev. Za varstvo osebnih podatkov je namreč bolje, da »preveč napredna« tehnologija ne nadomesti človeka pri odločanju in da niso »na enem mestu« dostopni vsi podatki o posamezniku. Takšne rešitve je kljub tehnološki zmogljivosti treba implementirati previdno in ob upoštevanju pravic in svoboščin posameznikovi, ki so jim navsezadnje vsi ti postopki tudi namenjeni – informatizacija procesov, ki jih uporablja država pri svojem delovanju namreč ni namenjena temu, da bi država lažje delovala, temveč, da bi bilo njeno delovanje v največjo korist ljudi, ki na njenem ozemlju živijo.

Več o povezovanju zbirk v javni upravi:

➔ Smernice IP: Varstvo osebnih podatkov pri povezovanju zbirk osebnih podatkov v javni upravi[55]

55 https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Varstvo_osebnih_podatkov_pri_povezovanju_zbirk_osebnih_podatkov_v_javni_upravi.pdf

OBDELAVE OSEBNIH PODATKOV V ZDRAVSTVU

Posebnosti obdelave osebnih podatkov v zdravstvu

Zdravstveni domovi, bolnišnice in drugi izvajalci zdravstvene dejavnosti o posameznikih zbirajo in hranijo velike količine osebnih podatkov, ki spadajo med ‚posebne vrste osebnih podatkov.' Uvodoma je bilo navedeno, da za posebne vrste osebnih podatkov Splošna uredba predpisuje posebej visoke kriterije glede obdelave, saj so lahko posledice izgub, pomot, nepooblaščenega dostopa ali posredovanja brez pravne podlage za pacienta zelo resne. Lahko si je predstavljati resnost posledic, če se na recept po pomoti navede napačen podatek glede odmerka zdravila ali pa se v evidence vnese napačna krvna skupina ali pa če se izgubi zdravstvena kartoteka, kjer so navedene ključne ugotovitve za pacientovo nadaljnjo obravnavo. Varstvo osebnih podatkov v zdravstvu je torej še kako pomembno in prav je, da se tega zavedamo.

Pravice posameznikov po Splošni uredbi (popravek, omejitev, izbris,...) veljajo sicer tudi v zvezi z dostopom do podatkov iz zbirk pri izvajalcih zdravstvene dejavnosti, vendar v praksi redko pridejo v poštev, razen pogosto uporabljene pravice ‚dostopa do lastne zdravstvene dokumentacije'. Ta po vsebini pokriva pravico do seznanitve z lastnimi osebnimi podatki, ki jo na splošno ureja člen 15 Splošne uredbe. Ker pa je pravica dostopa do lastne zdravstvene dokumentacije urejena v specialnem predpisu – to je v Zakonu o pacientovih pravicah (ZPacP), ki je prilagojen glede na naravo obdelav podatkov, ki se izvaja v zdravstvu – se za dostop do lastnih osebnih podatkov v zvezi z zdravstveno dokumentacijo uporablja ZPacP.

Dostop do lastne zdravstvene dokumentacije

Posebnosti pri ureditvi pravice do lastne zdravstvene dokumentacije po ZPacP v primerjavi s pravico dostopa do lastnih osebnih podatkov po Splošni uredbi so:

- zahtevo lahko uveljavlja pacient pri izvajalcu zdravstvene dejavnosti,
- rok za odločanje je 5 delovnih dni,
- pacient ima možnost, da k zapisom v svoji zdravstveni dokumentaciji doda svoje pripombe.
- upravičene osebe lahko zahtevajo tudi seznanitev s podatki umrlih oseb.

Pacient, ki ni prejel zahtevane dokumentacije v roku ali pa z odločitvijo izvajalca zdravstvene dejavnosti ni bil zadovoljen, lahko vloži pritožbo pri IP.

Upravičena oseba, ki je zahtevala dostop do zdravstvene dokumentacije umrle osebe, lahko zoper molk ali odločitev izvajalca zdravstvene dejavnosti vloži pritožbo pri IP.

Več o varstvu osebnih podatkov v zdravstvu:

- ➔ Spletna stran IP, podstran: Pravice pacientov [56]
- ➔ Smernice IP: Smernice za izvajalce zdravstvenih storitev[57]
- ➔ Smernice IP: Evropske smernice za zdravstvene delavce o zaupnosti in zasebnosti v zdravstvu

OBRAZCI:

- ➔ Zahteva za seznanitev z lastno zdravstveno dokumentacijo (Obrazec ZPacP 41-3).[58]
- ➔ Pritožba v zadevi seznanitve z lastno zdravstveno dokumentacijo (Obrazec ZPacP 41).[59]
- ➔ Pritožba v zadevi seznanitve z_zdravstveno dokumentacijo umrlega pacienta (Obrazec ZPacP 42.doc).[60]

56 Spletna stran IP, Pravice pacientov https://www.ip-rs.si/varstvo-osebnih-podatkov/pravice-posameznika/pravice-pacientov/

57 https://www.ip-rs.si/fileadmin/user_upload/Pdf/brosure/Smernice_za_izvajalce_zdr._storitev_net.pdf

58 https://www.ip-rs.si/obrazci/pravice-pacientov/.

59 Prav tam.

60 Prav tam.

OBDELAVE OSEBNIH PODATKOV, KI JIH IZVAJAJO CENTRI ZA SOCIALNO DELO (CSD)

CSD-ji na prvi stopnji odločajo o mnogih pravicah, ki omogočajo socialne transferje (npr. otroški dodatek, dodatek za nego in varstvo otroka, socialna pomoč, vdovska in starševska pokojnina, itd.) ali drugih pravicah in obveznostih, s katerimi država izvaja socialno skrb prebivalstva. V svojih postopkih uporabljajo mnoge baze podatkov za ugotavljanje relevantnih okoliščin pomembnih za odločanje v konkretnem postopku. Za vsako zbiranje osebnih podatkov mora obstajati ustrezna pravna podlaga po zakonu.

IP je izdal smernice za Centre za socialno delo[61], ki opisujejo za kakšen namen in na kateri podlagi smejo CSD-ji zbirati osebne podatke:

- **o premoženjskem stanju,**
- **iz družabnih omrežij,**
- **od patronažne službe,**
- **zdravstvene dokumentacije od zdravnika,**
- **od nevladnih organizacij,**
- **od zavoda za prestajanje kazni zapora,**
- **od oseb pod skrbništvom,**
- **od šole,**
- **od oseb na prestajanju zaporne kazni,**
- **v primerih nasilja v družini.**

IP je v navedenih smernicah zbral tudi odgovore na pogosta vprašanja s področja dela CSD in sicer glede:

- **vpogleda v lastne osebne podatke v spisu CSD,**
- **pravice staršev do seznanitve z osebnimi podatki otroka,**
- **vpogleda v osebne podatke rejenca,**
- **obdelave osebnih podatkov pri delu v multidisciplinarnih timih,**
- **obdelave osebnih podatkov prijavitelja,**
- **osebnih podatkih na odločbi CSD,**
- **obdelave osebnih podatkov v primeru posvojitve,**
- **obdelave osebnih podatkov z uporabo telekomunikacijskih sredstev.**

V zvezi s smernicami se je treba zavedati, da so pravice posameznikov po Splošni uredbi urejene nekoliko drugače, kot je veljalo po ZVOP-1 in da navedene smernice (še) niso prilagojene na novo ureditev. Kljub temu so še vedno uporabne, ker vsebujejo sklice na slovensko področno zakonodajo, ki velja tudi še po pričetku uporabe Splošne uredbe.

Več o tem:

➔ Smernice IP: smernice za Centre za socialno delo[62]

61 https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_za_CSD_julij2017.pdf

62 https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_za_CSD_julij2017.pdf

VPOGLED V CENTRALNI REGISTER PREBIVALSTVA

Centralni register prebivalstva (CRP) je osrednja zbirka podatkov o državljanih Republike Slovenije in tujcih, ki imajo dovoljenje za stalno ali začasno prebivanje v Republiki Sloveniji ali določene pravice ali obveznosti na področju pokojninskega in invalidskega zavarovanja, davkov, iz humanitarnih razlogov ali na drugem področju, če je tako določeno z zakonom. Upravljavec CRP je ministrstvo, pristojno za notranje zadeve.

Vpogled v lastne osebne podatke iz CRP je možen preko spleta z uporabo kvalificiranega digitalnega potrdila na spletnem portalu eUprave - Modul Moja eUprava.[63]

Več o obdelavah osebnih podatkov v zvezi s CRP:

➔ Smernice IP: Obdelava osebnih podatkov iz centralnega registra prebivalstva [64]

VARSTVO OSEBNIH PODATKOV PRI POLICIJI

Narava dela policije in drugih organov pristojnih za preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj je pomembno drugačna od drugih služb, prek katerih deluje država. V ta segment spadajo tudi organi pristojni za izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem. Kadar navedeni organi obdelujejo osebne podatke za te namene, potem se Splošna uredba ne uporablja. Posameznikom, ki se želijo seznaniti s tem, kaj o njih vodi policija ali uveljavljati druge pravice v zvezi z varstvom osebnih podatkov, so na voljo podobne pravice, kot jih nudi Splošna uredba za obdelave osebnih podatkov. Kljub temu, pa obstajajo pomembne omejitve (na primer glede dostopanja do podatkov, če je posameznik osumljenec storitve kaznivega dejanja in zoper njega poteka preiskava v predkazenskem postopku). Pravila varstva osebnih podatkov (vključno s pravicami posameznikov) v navedenih primerih ureja Policijska direktiva (Direktiva (EU) 2016/680). EU direktiva je bila prenesena v slovenski pravni red z Zakonom o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD).[65]

Ker policija deluje kot represivni organ, mora varstvu človekovih pravic nameniti posebno pozornost tudi v preventivnem smislu in ravno pri varstvu osebnih podatkov je to ključno za zagotavljanje ustreznega varstva. IP je že pred sprejemom Splošne uredbe in Policijske direktive podal priporočila za izvedbo ocene vpliva na zasebnost in varstvo osebnih podatkov pri uvajanju novih policijskih pooblastil. Brezpilotni letalniki (droni), biometrijska prepoznava obrazov, bralniki registrskih tablic in podobni sodobni nadzorovalni sistemi morajo prestati predhodne teste nujnosti, sorazmernosti in primernosti. Glede tega je IP izdal tudi posebne smernice.[66]

Več o tem:

➔ Smernice IP: Presoje vplivov na zasebnost pri uvajanju novih policijskih pooblastil [67]

63 https://e-uprava.gov.si/pomoc-kontakt/pomoc-pri-uporabi/uporaba-modula-moja-euprava.html

64 https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_CRP_web.pdf

65 Uradni list RS, št. 177/20

66 https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Presoje_vplivov_na_zasebnost_pri_uvajanju_novih_policijskih_pooblastil_Smernice_IP.pdf

67 Prav tam.

MEDNARODNE EVIDENCE

Podatki v zvezi s prepovedjo vstopa v Schengensko območje in s tem povezanimi kaznivimi dejanji

Schengenski informacijski sistem (SIS II) je zbirka podatkov o osebah, ki jim je vstop v schengensko območje prepovedan ali ki se iščejo zaradi odvzema prostosti ali izročitve, ter podatkov o pogrešanih osebah, kot tudi podatkov o ukradenih vozilih, plovilih, zrakoplovih, dokumentih, orožju, označenem denarju, ki izvira iz kaznivih dejanj, itd. Zbirka se vodi za potrebe policijskih postopkov.

Posamezniki lahko svojo pravico do seznanitve lastnimi osebnimi podatki uveljavljajo pri Policiji.

Več o tem:

- pojasnila na spletni strani IP: podstran Schengenski informacijski sistem[68]
- Spletna stran Policije.[69]

OBRAZEC

- Zahteva za seznanitev s podatki v Schengenskem informacijskem sistemu v Sloveniji (SIS II).[70]

Podatki pri Europolu

Europol – Evropski policijski urad je kot agencija Evropske unije pristojen za organizirani kriminal, terorizem in druge hujše oblike kriminala, ki prizadenejo dve ali več držav članic tako, da je zaradi obsega, pomena in posledic kaznivih dejanj potreben skupen pristop držav članic. Temeljna naloga Europola je izboljšati učinkovitost in sodelovanje med pristojnimi organi držav članic pri preprečevanju in v boju proti hujšim oblikam organiziranega kriminala. Osnovni cilj Europola pa je doseči pomemben prispevek na področju odkrivanja, preprečevanja in pregona kaznivih dejanj v Evropski uniji, posebej v boju proti organiziranemu kriminalu in v boju proti delovanju organiziranih kriminalnih družb.

Pravice posameznikov v zvezi s podatki, ki jih obdeluje Europol:

- Pravica do dostopa (36. člen Uredbe o Europolu)
- Pravica do popravka, izbrisa in omejitve (37. člen Uredbe o Europolu)
- Druge pravice (42. člen Uredbe o Europolu)

Več o tem

- Spletna stran IP: Europol.[71]

Podatki v zvezi z viziumi

Vizumski informacijski sistem (VIS) je skupni vizumski informacijski sistem držav članic schengenskega sporazuma, ki je pričel delovati 11. oktobra 2011. Sistem je namenjen hitrejšemu, preglednejšemu in varnejšemu vizumskemu postopku in hkrati preprečevanju kraj identitete in zlorabe podatkov.

V zvezi z obdelavo osebnih podatkov v VIS ima vsak posameznik sledeče pravice:

- pravico do seznanitve z lastnimi osebnimi podatki v VIS,
- pravico zahtevati popravek netočnih lastnih osebnih podatkov shranjenih v VIS,
- pravico zahtevati izbris nezakonito shranjenih lastnih osebnih podatkov v VIS.

Zahtevo za seznanitev, popravek oz. izbris lastnimi osebnimi podatki v VIS se v Sloveniji vloži pisno ali ustno na zapisnik pri Ministrstvu za zunanje zadeve.

Več o tem

- spletna stran IP: Vizumski informacijski sistem.[72]

OBRAZEC

- Zahteva za seznanitev z lastnimi osebnimi podatki v vizumskem informacijskem sistemu.[73]

68 https://www.ip-rs.si/varstvo-osebnih-podatkov/mednarodni-upravljavci/schengenski-informacijski-sistem/

69 https://www.policija.si/nase-naloge/druga-podrocja/mednarodno-sodelovanje/sirene/schengenski-informacijski-sistem-druge-generacije-pravica-do-seznanitve

70 https://e-uprava.gov.si/podrocja/vloge/vloga.html?id=1115

71 https://www.ip-rs.si/varstvo-osebnih-podatkov/mednarodni-upravljavci/europol/

72 https://www.ip-rs.si/varstvo-osebnih-podatkov/mednarodni-upravljavci/vizumski-informacijski-sistem/

73 https://www.gov.si/zbirke/storitve/zahteva-za-

Podatki o prstnih odtisih prosilcev za azil

Ko ljudje prihajajo v EU zaprosit za azil, morajo organi oblasti, ki so pristojni za izvajanje politike priseljevanja vedeti, katera izmed držav članic mora obravnavati njihovo vlogo. Od leta 2003 naprej ta del azilnega postopka pospešuje Eurodac (evropski avtomatski sistem za identifikacijo prstnih odtisov).

Vsak posameznik, na katerega se nanašajo podatki v Eurodac sistemu, ima pravico:

- biti obveščen o tem, kateri podatki o njem so shranjeni v centralnem sistemu ter katera država članica jih je posredovala v centralni sistem;
- zahtevati, da se dejansko nepravilni podatki popravijo ali nezakonito zapisani podatki izbrišejo;
- vložiti tožbo ali (če je to ustrezno) pritožbo pri pristojnih organih ali sodiščih države, če mu je kratena pravica dostopa, popravka ali izbrisa.

Več o tem:

➔ Spletna stran IP: Eurodac.[74]

Podatki o kršitvah carinske in kmetijske zakonodaje

Carinski informacijski sistem (CIS) je skupni avtomatizirani informacijski sistem za carinske namene, ki omogoča bolj učinkovito preganjanje in preiskovanje kršitev carinske in kmetijske zakonodaje. Cilj CIS je s hitrim razširjanjem informacij pomagati pri preprečevanju, preiskovanju in preganjanju hudih kršitev nacionalnih zakonov, tako da se poveča učinkovitost sodelovanja in nadzornih postopkov carinskih uprav držav članic.

Pravice oseb glede osebnih podatkov v CIS, zlasti njihova pravica do dostopa, popravljanja, izbrisa ali blokiranja teh podatkov, se uveljavljajo v skladu z zakoni, predpisi in postopki, s katerimi država članica, v kateri se nanje sklicujejo, izvaja Policijsko direktivo (Direktivo (EU) 2016/680).[75]

Več o tem:

➔ Spletna strani IP: Carinski informacijski sistem[76].

seznanitev-s-podatki-v-vizumskem-informacijskem-sistemu-vis-v-sloveniji/

74 https://www.ip-rs.si/varstvo-osebnih-podatkov/mednarodni-upravljavci/eurodac/

75 https://eur-lex.europa.eu/legal-content/SL/ALL/?uri=CELEX%3A32016L0680

76 https://www.ip-rs.si/varstvo-osebnih-podatkov/mednarodni-upravljavci/carinski-informacijski-sistem/

Varnost posameznika na spletu

‘PHISHING’, ‘PHARMING’, SOCIALNI INŽINIRING IN DRUGE OBLIKE SPLETNIH NAPADOV

Na spletu so prisotni tudi zlonamerni uporabniki, ki za lastno korist tako ali drugače želijo izkoristiti dobroverne uporabnike spleta. Načinov zlorab je veliko, nekaj od njih je opisal tudi IP na svoji spletni strani in v izdanih publikacijah (glej spodaj: Več o tem). Pogosti so na primer vdori v uporabniške račune (elektronske pošte, socialnih omrežij, itd.) s pomočjo gesla, ki je napadalec tako ali drugače pridobil od posameznika – t.i. ‚phishing‘. Znani so primeri ponarejenih spletnih strani, kjer napadalec pošlje elektronsko sporočilo, ki imitira grafično podobo ponudnika spletne storitve, sporočilo pa navaja, da je treba ponovno vnesti geslo (denimo zaradi posodabljanja sistema ali zaščite računa ipd.). Povezava za »zamenjavo gesla«, nato vodi na ponarejeno spletno mesto (na las podobno originalni), ki tako uporabnika preslepi, da vpiše svoje geslo in ga posreduje spletnemu goljufu. Če se napadalec poslužuje zgolj te prevare, ga izkušenejši uporabnik relativno enostavno prepozna, ker sam URL naslov spletne povezave izkazuje, da ne gre za pravega ponudnika storitev (npr. http://yourupdateservicesnow.com/ namesto https://www.paypal.com/au/, ko je šlo za spletno prevaro v zvezi z PayPal storitvijo). Poznan pa je tudi način napada t.i. ‚pharming‘, ki zavede uporabnika s navideznim prikazom pravilnih URL povezav, čeprav gre v ozadju za preusmeritev na lažne spletne strani. Navedena phishing in pharming, kot tudi druge oblike zlonamernih spletnih zlorab sodijo na področje t.i. ‚socialnega inženiringa‘, pri katerem gre zlasti zato, da napadalci z različnimi psihološko-tehnološkimi manipulativnimi tehnikami želijo pridobiti o posamezniku čim več informacij, da lahko potem izvedejo svoj napad. Cilji napadov so lahko različni, na primer: kraja denarja iz tekočega računa ali kreditne kartice, vdor v stanovanje, kraja avtomobilov, kraja pomembnih dokumentov, izsiljevanje, kraja identitete in lažno predstavljanje, itd. V vsakem primeru pa napad omogočajo informacije, ki jih napadalci tako ali drugače pridobijo od posameznikov.

Kako se temu izogniti? Treba je slediti trem korakom:

1. ZAVEDANJE

Za svojo varnost moramo najprej poskrbeti sami. To storimo tako, da postanemo zavedni uporabniki spleta. Če bomo pravočasno prepoznali napad, ga lahko naznanimo pristojnim službam, ki bodo lahko učinkovito in pravočasno ukrepale. Že osnovno poznavanje tehnologije in pravil varstva osebnih podatkov lahko razkrinka marsikateri napad, preden pride do resnejših posledic. Obstaja več spletnih strani in služb, kamor se posameznik lahko obrne po nasvet. Na primer spletna stran safe.si[77] ali nacionalni odzivni center za kibernetsko varnost SI-CERT[78] (slednji lahko pomaga tudi s strokovnim nasvetom za preprečevanje posledic, ko že pride do zlorab).

2. UKREPANJE

Če zaznamo, da se nam dogaja napad, je treba nemudoma ukrepati. Lahko spremenimo gesla, prekličemo račune in kartice. Javimo banki, da zažene interne mehanizme nadzora, itd. Pomembno je, da v tem trenutku ne čakamo, saj je lahko od ur ali celo minut odvisno, ali bo napad lahko izpeljan ali ne.

3. PRIJAVA KRŠITEV

Čeprav ta korak pride na koncu, je zelo pomembno, da zaznane kršitve naznanimo pristojnim službam. Ker gre v primerih tovrstnih napadov običajno za kazniva dejanja, je prav da se obrnemo na Policijo.

Več o tem:

- ➔ Spletna stran IP: Varstvo osebnih podatkov na internetu
- ➔ Smernice IP: O orodjih za zaščito zasebnosti na internetu
- ➔ Smernice IP: Smernice o kraji identitete
- ➔ Smernice IP: Socialni inženiring in kako se pred njim ubraniti?

77 https://safe.si/.

78 https://www.cert.si/.

SPLETNO NAKUPOVANJE

Spletno nakupovanje postaja prej kot ne standard sodobnih potrošniških navad in s širjenjem uporabe spleta za ta namen se širijo tudi možnosti za zlorabe. Ravno pri nakupovanju prek spleta, kjer uporabniki praviloma s svojimi osebnimi podatki omogočajo finančne transakcije, obstaja povečana nevarnost, da napadalci izkoristijo nepazljivost potrošnika in ga preusmerijo na »lažno spletno stran«, in ga napeljejo da nakaže denar neznanemu prejemniku.

Več o varnosti pri nakupovanju na spletu

- Smernice IP: Informirani potrošniki - komu dajemo katere osebne podatke in zakaj?

VARNA UPORABA DRUŽBENIH OMREŽIJ IN SPLETNIH FORUMOV

Družbena omrežja, kot je Facebook, TikTok, Twitter, itd. in spletni forumi že dokaj dolgo pomembno dopolnjujejo naše družbeno življenje zato predstavljajo bogat vir informacij o vsakomur, kdor jih uporablja. Neizkušeni ali nepodučeni uporabnik se ne zaveda, kdo vse lahko »privzeto« dostopa do njegovih podatkov, objavljenih slik ali komentarjev – kar je lahko povsem zakonit način pridobivanja informacij o njem. Samo »vohljanje« po »odprtih« profilih uporabnikov družbenih omrežij torej niti ni prepovedano, ni pa izključeno, da vohljač teh podatkov ne bo uporabil za nekaj prepovedanega (kot na primer phishing, socialni inženiring, nadlegovanje ali izkoriščanje, itd.). Zato moramo biti uporabniki spletnih omrežij in forumov podučeni, kako naj jih uporabljamo varno.

Več o tem:

- Spletna stran IP: 10 nastavitev zasebnosti, ki bi jih moral poznati vsak uporabnik Facebooka
- Spletna stran IP: Uporabna orodja za upravljanje zasebnosti
- Smernice IP: Smernice o spletnih forumih

VARNOST OTROK

Sodobne informacijske tehnologije ponujajo neskončne možnosti komuniciranja, informiranja in izobraževanja, žal pa prinašajo tudi številne možnosti zlorab, katerih najbolj ranljive žrtve so prav otroci in mladostniki. Zlorabe so lahko različne, od nadlegovanja med vrstniki, do spolnih in drugih zlorab otrok in mladostnikov. Da se spletnega nadlegovanja in zlorab ubranimo, ga moramo najprej prepoznati, predvsem pa otroke o tem poučiti in jim stati ob strani, če se zgodi. Kako prepoznati, če otroka nekdo nadleguje? Kaj storiti, če odkrijete sovražno spletno stran? Kako postopati, če naletite na spletno stran z otroško pornografijo? Kako otroke poučiti o vseh nevarnostih, ki prežijo nanj na spletu? Kaj lahko stori šola? Kaj o tem pravi zakonodaja? Odgovore na ta vprašanja najdemo na spodnjih povezavah.

Več o tem:

- Spletna stran IP: Prijavna točka za otroško pornografijo in sovražni govor[79]
- Smernice IP: Varstvo pred spletnim nadlegovanjem za mlade - smernice[80]
- Spletna stran IP: Video vsebine na temo varne rabe interneta[81]

79 https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/#c409.

80 https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice-glede-varstva-pred-spletnim-nadlegovanjem.pdf.

81 https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu-samo-za-mlade/multimedija/.