INFORMACIJSKI
POOBLAŠČENEC

SMERNICE

O orodjih za zaščito zasebnosti na internetu

SMERNICE O ORODJIH ZA ZAŠČITO ZASEBNOSTI NA INTERNETU

Kaj lahko sami storimo za zasebnost na internetu?

Namen dokumenta:	Smernice podajajo spletnim uporabnikom enostavne napotke, kako zaščitijo svoje osebne podatke, shranjene na različnih napravah, omejijo dostop tretjim osebam do svojih podatkov (družabna omrežja, oglaševalske platforme) ter preprečijo zlorabo svojih uporabniških računov.
Ciljne javnosti:	Širok krog uporabnikov spletnih storitev, predvsem so smernice koristno branje za uporabnike mobilnih naprav in družbenih omrežij.
Status:	javno
Verzija:	2.0
Datum verzije:	1. 10. 2019
Avtorji:	Informacijski pooblaščenec
Ključne besede:	Gesla, socialni inženiring, varnostne kopije, kriptiranje, družabna omrežja, nastavitve brskalnika

Smernice Informacijskega pooblaščenca

Namen smernic Informacijskega pooblaščenca je spletnim uporabnikom podati praktične napotke, kako lahko s tehničnimi rešitvami in previdnim obnašanjem na spletu zaščitijo svojo informacijsko zasebnost. Smernice pojasnjujejo najpogostejša varnostna tveganja, povezana z izgubo podatkov, nepooblaščenim dostopom do podatkov in pretiranim deljenjem podatkov, ki vodijo v izgubo nadzora nad lastnimi osebnimi podatki. Našteti so bistveni varnostni ukrepi, programska orodja in nastavitve uporabniških računov, ki spletnim uporabnikom vračajo moč odločanja, komu in pod kakšnimi pogoji dovoljujejo dostop do njihovih osebnih podatkov.

Pravno podlago za izdajo smernic Informacijskemu pooblaščencu daje 3(b) odstavek 58. člena Splošne Uredbe (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; ang. GDPR, v nadaljevanju: Splošna uredba), ki določa, da ima vsak nadzorni organ pooblastila v zvezi z dovoljenji in svetovalnimi pristojnostmi, med drugim, da na lastno pobudo ali na zahtevo izdaja mnenja za nacionalni parlament, vlado države članice ali, v skladu s pravom države članice, druge institucije in telesa, pa tudi za javnost, o vseh vprašanjih v zvezi z varstvom osebnih podatkov. Podobno določa tudi 27. člen Direktive (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (za njen prenos v slovenski pravni red naj bi poskrbel nov Zakon o varstvu osebnih podatkov).

Vse smernice in priročniki, ki jih je izdal Informacijski pooblaščenec, so objavljeni na spletni strani:

https://www.ip-rs.si/publikacije/prirocniki-in-smernice/

Pojasnila o pravicah posameznikov s področja varstva osebnih podatkov in konkretne napotke, kako jih uresničite, najdete na spletni strani www.tiodlocas.si

Kazalo

1. Sami smo prvi varuh svoje zasebnosti!

Posamezniki moramo imeti moč odločanja, komu dovolimo dostop do naših osebnih podatkov in pravico do jasnih informacij, kaj bodo podjetja z njimi počela. Naša pravica v smislu moči odločanja o lastnih osebnih podatkih je omejena, ko je zbiranje podatkov predpisano v zakonodaji, veliko pa lahko za varstvo naših podatkov storimo sami - ko so pri nas in ko jih zaupamo ponudnikom različnih storitev.

Podobno kot na številnih drugih področjih v življenju, spletni uporabniki žal premalo pozornosti posvečamo preventivi, dokler sami ne doživimo slabe izkušnje. Tudi na področju varovanja naših osebnih podatkov se zavemo razsežnosti morebitnih posledic šele takrat, ko sami postanemo žrtev zlorabe. Tako niso več nič nenavadnega obvestila ponudnikov najrazličnejših storitev, da naj zamenjamo naše geslo, saj je prišlo do kraje podatkov ali pa klic prijateljev, da na našem Facebook profilu delimo »čudne objave«. Še posebej neprijetna je izguba podatkov, ki jih je zašifriral izsiljevalski virus in nam tako odvzel tudi precej lepih spominov in pomembnih dokumentov.

Izguba nadzora nad lastnimi podatki in zasebnostjo pa se dogaja tudi pod našim nadzorom, tudi takrat, ko ne gre hujše varnostne incidente, ampak ob povsem vsakodnevni uporabi spleta. Različne sledilne tehnologije (piškotki, slikovna točka oz. pixel, sledilne skripte) omogočajo natančno sledenje, katere spletne strani obiskujemo, katere oglase klikamo in kaj vpisujemo v naš iskalnik. »Nič takšnega,« bi kdo skomignil. »Saj nič ne skrivam!« Zasebnost moramo razumeti kot moč odločanja oziroma našo pravico, da se nas pusti na miru in da se sami odločamo, kaj in kdaj bomo s kom delili. Zakaj bi nekdo moral ali imel pravico vedeti, kaj počnemo, katere knjige beremo, kakšne filme gledamo in kaj iščemo po spletu? Mar ni to nekaj, o čemer bi se morali sami odločati? In ravno to je bistvo pravice do zasebnosti, da imamo svoj mir, v katerem se lahko svobodno udejstvujemo, razmišljamo, delamo in ustvarjamo.

Predvsem se moramo zavedati, da lahko za svojo zasebnost marsikaj postorimo tudi sami in nismo zgolj nemočni opazovalci, ki svoje digitalne življenje prepuščamo spletnim velikanom. Namen pričujočih smernic je ravno ta – prikazati nekaj uporabnih orodij, s katerimi lahko skrb za svojo zasebnost (vsaj do neke mere) vzamemo v svoje roke.

2. Katere nevarnosti prežijo na našo informacijsko zasebnost?

Proti nevarnostim se lahko učinkovito zaščitimo le, če jih dobro poznamo. Tudi zaradi medijskega poročanja v zadnjih letih, so spletnim uporabnikom najbolj poznane in »oprijemljive« predvsem tiste zlorabe, ki so **povezane z varnostjo osebnih podatkov.** Da je naša informacijska zasebnost v nevarnosti, se pogosto zavemo šele takrat, ko npr. spletni goljuf pridobi geslo naše elektronske pošte ali izgubimo pametni telefon in posledično vse shranjene fotografije.

Najpogostejše nevarnosti, ki pretijo povprečnemu spletnemu uporabniku, lahko razdelimo v tri sklope:

a.) Vdori v uporabniške račune

Nepooblaščene osebe lahko dostopajo in posledično tudi zlorabijo uporabniški račun določene spletne storitve, ko pridobijo naše uporabniško ime in geslo. Najpogosteje je to posledica »**phishing**« **kraje podatkov**, kjer spletni napadalci poskušajo pridobiti gesla za različne spletne storitve (elektronska pošta, PayPal račun, Facebook itd.) ali celo izvabijo geslo za dostop do e-bančnega računa. V večini primerov se phishing prevara prične z elektronskim sporočilom, da je potrebno zaradi različnih vzrokov ponovno vnesti geslo (zaradi posodabljanja sistema, zaščite računa itd.). Uporabnik naj bi kliknil na povezavo, ki vodi na ponarejeno spletno mesto - kopijo, ki je skoraj identična originalu. Tako uporabnika preslepi, da vpiše svoje geslo, ki se posreduje spletnemu goljufu.

Drug pogost način, kako goljufi pridobijo naša gesla, je **prek okužbe računalnika** s posebnim zlonamernim programom (virusom, t.i. keylogger), ki beleži vnose na tipkovnici in pošlje prestreženo geslo napadalcu.

Če pa uporabljamo lahko uganljiva, enostavna gesla, npr. password ali 123456, ki se že vrsto let pojavljajo na lestvici najslabših možnih gesel, potem ga lahko **napadalci preprosto - uganejo.**

b.) Izguba podatkov

O izgubi podatkov govorimo, ko shranjeni podatki niso več razpoložljivi (nimamo dostopa do njih, so izbrisani s strani nepooblaščene osebe itd.). Zadnja leta največjo grožnjo za naše podatke predstavljajo izsiljevalski virusi, ki po zagonu zašifrirajo vse shranjene podatke in v zameno za dokumente zahtevajo plačilo odkupnine. Če nimamo dokumentov varno shranjenih v obliki varnostne kopije oz. backupa, potem nam ostane malo upanja, da jih povrnemo brez plačila odkupnine. Pogoste so tudi strojne okvare (okvara diska na računalniku) ali pa izgube in kraje naprav (ukraden prenosnik ali izgubljen pametni telefon).

c.) Socialni inženiring

Socialni inženiring pomeni predvsem pridobivanje različnih koristi z zlorabo zaupanja posameznika oz. **z manipulacijo,** pri čemer napadalci sploh ne potrebujejo naprednih tehnoloških metod, ampak z uporabo različnih socialnih veščin (prepričevanje, vzbujanje zaupanja, grožnje, lažno predstavljanje) pridobijo od žrtve osebne podatke (najpogosteje ime, priimek, št. transakcijskega računa, razna gesla, EMŠO, št. potnega lista …), ki jih nato uporabijo za pridobivanje večinoma premoženjske koristi. Več o tem, kaj je socialni inženiring, kako deluje in kako se pred njim obraniti, lahko preberete v naših smernicah na to temo[1].

[1] https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf

3. Prvi varnostni obroč: Osnovna zaščita naprav in shranjenih podatkov

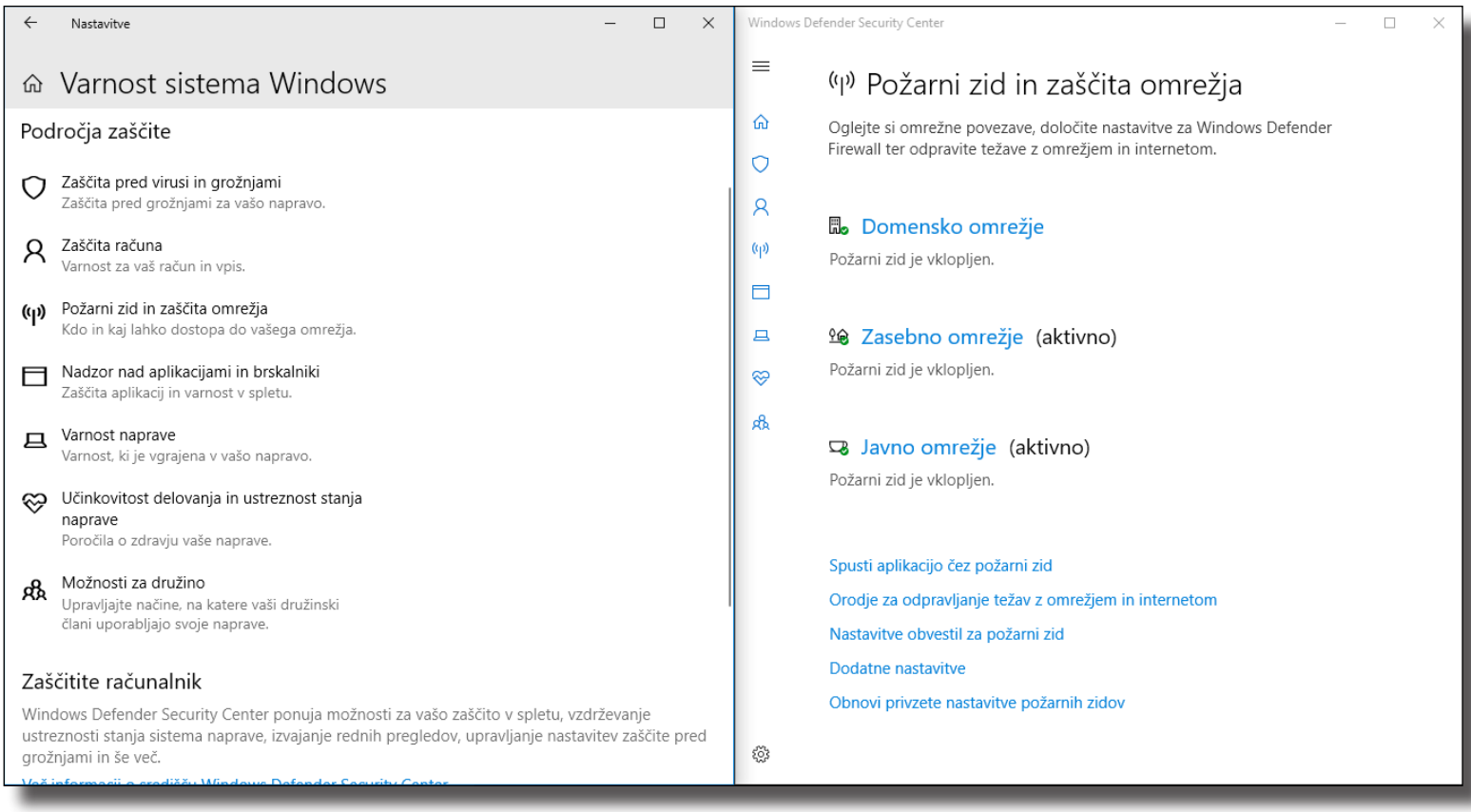
Ker število in pogostost varnostnih groženj še naprej rasteta, so učinkoviti pristopi k zaščiti naprav in shranjenih podatkov bistvenega pomena. Pomembna je uporaba protivirusnih programov in drugih varnostnih orodij. V primeru, ko se zruši sistem, pa so lahko zanesljive varnostne kopije in vzpostavljen načrt za obnovitev sistema odlična prednost.

a.) Posodobitve programske opreme, antivirusni program, požarni zid

Posodobitve operacijskega sistema vsebujejo kritične varnostne popravke, ki zaščitijo računalnik pred nedavno odkritimi ranljivostmi. Če se te posodobitve ne nameščajo, je lahko računalnik veliko bolj ranljiv in občutljiv na varnostne ranljivosti. Ne glede na to, kateri operacijski sistem uporabljate, je pomembno, da je ta **redno posodobljen**. Operacijski sistem Windows se običajno posodablja vsaj enkrat mesečno. Najboljši pristop k redno posodobljenemu sistemu je nastavitev samodejnega posodabljanja operacijskega sistema.

Zlonamerna programska oprema je resna težava, ki lahko tako ali drugače škoduje velikemu številu računalniških uporabnikov, zato je zaščita pred zlonamernimi programi (t.i. *malware*) bistvena za postavitev temeljev varnosti vaših naprav. Zlonamerna programska oprema je programska oprema, ki je namenjena infiltriranju ali poškodovanju računalnika brez vaše vednosti ali soglasja in vključuje računalniške viruse, črve, trojanske konje, vohunsko programsko opremo in drugo. Prisotna je lahko na spletnih mestih, v e-poštnih sporočilih ali skrita v prenosljivih datotekah, fotografijah, videoposnetkih ali brezplačnih programih. Najboljši način, da se izognete okužbi, je **namestitev in redno posodabljanje protivirusnega programa**, redno skeniranje oz. preverjanje računalnika za morebitnimi okužbami in izogib klikanju na sumljive e-poštne povezave ali spletne strani.

Tretja nujna varnostna komponenta je aktiviran požarni zid, ki v digitalnem svetu pomeni sistem, ki služi za varnost omrežja in nadzira vhodni in izhodni omrežni promet na podlagi vnaprej določenih varnostnih pravil. Za čim večjo zaščito vaših naprav je pomembno, da je **požarni zid vedno vklopljen**, saj lahko ob izklopu vaša naprava postane veliko bolj ranljiva za nepooblaščen dostop. Večina operacijskih sistemov ima požarni zdi že vgrajen v sam sistem. V privzetih nastavitvah npr. sistema Windows 10 je požarni zid že vklopljen, preverimo oz. ročno vklopimo/izklopimo pa ga lahko v nastavitvah pod kategorijo omrežje in varnost, kjer izberemo varnost sistema Windows in nato požarni zid in zaščita omrežja.



b.) Zaščita pametnih telefonov in tablic

Danes praktično že skoraj vsi nosimo v žepu pametni telefon, tablični računalnik ali pa kar oboje. Vendar se lahko hitro zgodi, pametna naprava zdrsne iz žepa ali torbe, vaši podatki pa lahko tako končajo v rokah nekoga, ki jih lahko uporabi za zlonamerne namene**. Prvi ukrep za zaščito vaših podatkov v primeru izgubljene ali ukradene mobilne naprave se začne z zaklepanjem naprave**. Priporočljiva je tudi **nastavitev oddaljenega brisanja naprave**. Če je vaša naprava izgubljena ali ukradena, vam takšna nastavitev omogoča oddaljeno brisanje občutljivih podatkov, kar nepooblaščenim osebam prepreči dostop do podatkov, shranjenih na napravi. Prav tako je nujen ukrep **varnostno kopiranje podatkov**, shranjenih na napravi, čeprav pri uporabnikih mobilnih naprav pogosto spregledano. Tudi za mobilne naprave obstaja ogromno aplikacij, ki omogočajo samodejno varnostno kopiranje bodisi v oblak, bodisi v osebni računalnik, ko je ta povezan s telefonom.

Na trg mobilnih aplikacij stalno prihajajo nove in nove aplikacije, toda preveč aplikacij, ki se izvajajo v ozadju, ne le da upočasnjuje vašo pametno napravo, ampak lahko nekatere od njih brez vaše vednosti delijo vaše osebne podatke, GPS lokacijo itd. Mobilne aplikacije na svoje naprave vedno nameščajte le iz uradnih virov, torej iz tržnic aplikacij, kjer vse aplikacije pred objavo varnostno preverijo. Če se odločite prenesti aplikacijo tretjega ponudnika mimo uradne tržnice, potem tvegate okužbo z zlonamerno programsko opremo, ki jo boste skupaj z aplikacijo namestili na vašo mobilno napravo. Lahko se zgodi, da od neznanega ponudnika aplikacijo prejmete tudi po elektronski pošti, SMS sporočilu ali pa boste pozvani, da jo prenesete s klikom na določeno povezavo na spletni strani. Takšnih aplikacij nikakor ni priporočljivo nameščati, če niste prepričani, da je ta varna.

c.) Šifriranje shranjenih podatkov

Vaši podatki, shranjeni na prenosnemu računalniku in mobilnih napravah, so izpostavljeni kraji ali izgubi, kar pomeni, da lahko popolni neznanec neovirano brska po vašem digitalnem življenju. Takšna tveganja lahko zaustavite s šifriranjem. Šifriranje podatkov ni samo za tehnološko napredne uporabnike, **sodobna orodja omogočajo vsakomur, da šifrira svojo e-pošto in druge podatke.** Sistem Windows 10 tako uporabnikom ponuja opcijo **BitLocker,** s čimer lahko uporabnik enostavno šifrira podatke na svojem računalniku. Prav tako je na voljo relativno enostavna programska oprema, ki omogoča šifriranje e-pošte in datotek, primer take je Pretty Good Privacy oz. PGP, ki je brezplačna in je na voljo na www.pgpi.org.

d.) Varno ravnanje z digitalnimi certifikati

Digitalno potrdilo, shranjeno na trdem disku osebnega računalnika ali navadnega USB ključka je izpostavljeno kraji in številnim drugim grožnjam. Za preprečevanje zlorab digitalnega potrdila je pomembno, da je takšno potrdilo shranjeno v napravi, ki omogoča zavarovanje občutljivih informacij kot so digitalna potrdila. Med takšne naprave sodijo **pametne kartice in pametni USB ključi, ki so namenjeni varni hrambi.** Digitalna potrdila shranjena na pametni kartici ali in pametnem USB ključu je bistveno težje zlorabiti. Takšne pametne naprave za hrambo digitalnih potrdil delujejo v kombinaciji z pripadajočo programsko opremo, ki omogoča enostavno upravljanje z digitalnimi potrdili.

e.) Varnostne kopije

Eden od najbolj osnovnih, vendar kljub temu pogosto prezrtih nasvetov za varstvo podatkov je varnostno kopiranje. Varnostno kopiranje v bistvu ustvari podvojeno kopijo vaših podatkov zaradi česar v primeru, **da je vaša naprava izgubljena, ukradena ali kako drugače ogrožena ne izgubite svojih pomembnih podatkov**. Najbolje je, da se varnostne kopije ustvarjajo na drugi napravi, na primer zunanjem disku, iz koder lahko kasneje v primeru, da je vaša prvotna naprava ogrožena svoje podatke enostavno obnovite.

4. Drugi varnostni obroč: Kako zaščitim dostop do svojih podatkov?

Skrb za varnost podatkov, ki so shranjeni na različnih pomnilniških napravah, predstavlja prvi varnostni obroč, ki žal ne zadostuje za celostno zaščito naše informacijske zasebnosti. Vsi možni programi nam ne bodo pomagali, če bomo sami, z lastno neprevidnostjo, omogočili dostop do elektronskega predala popolnemu neznancu ali nekritično dovolili neki aplikaciji, da dostopa do vseh podatkov na našem pametnem telefonu. Zato so pomembni tudi drugi ukrepi, s katerimi bomo zaščitili dostop do svojih podatkov, omogočili njihovo stalno razpoložljivost in preprečili dostop drugim osebam, ki jih lahko zlorabijo.

Na prvem mestu je gotovo **vzpostavitev dobrih navad pri ravnanju z našimi gesli, ki predstavljajo prvo obrambno črto pri dostopu do različnih uporabniških računov** in tako ščitijo našo digitalno identiteto.

a.) Upravljanje z gesli

Še vedno velja nasvet, da naj bo geslo dovolj dolgo, kompleksno, naj vsebuje posebne znake, naj ne bo geselska beseda, ki se preprosto ugane, naj ne bo kombinacija lahko uganljivih osebnih podatkov (kombinacija imena, priimka, letnice rojstva, imena otrok itd.) in predvsem naj ne bo enako za vse spletne storitve. Če je včasih veljalo, da je 6 znakov dovolj, danes to ne predstavlja ovire za zmogljive napade z ugotavljanjem gesel ali slovarske napade. Zato naj bodo gesla dolga vsaj 8 znakov, najlažje si boste zapomnili daljši stavek, ki mu dodate posebne znake (*, %, _ / # itd) in številke, npr. Vsak0jut3ogremVslu.

Vendar pa povprečni uporabnik spleta uporablja množico različnih storitev in če dodamo še zahtevo, da uporabljamo posebno geslo za vsako storitev, ki jih vsa hranimo v glavi in ne zapisana na papirju poleg monitorja, potem je to precej zahtevna naloga. Zato je priporočljiva uporaba posebnih programov za upravljanje z gesli (*t.i. password manager*), ki omogočijo, da ustvarjamo kompleksna gesla, ki so varno shranjena, hkrati pa si ni potrebno vseh zapomniti. Naštevamo le nekaj upravljalnikov gesel:

- Bitwarden
- KeePass
- LessPass

Še bolj pa je priporočljiva **nastavitev dvokoračnega preverjanja oz. dvofaktorske avtentikacije (2FA),** ki je učinkovita metoda za zaščito dostopov do različnih uporabniških računov in za preprečevanje kraje identitete. 2FA predstavlja dodatno raven zaščite, saj morate najprej vpisati svoje geslo in v naslednjem koraku še dodatno kodo, ki jo storitev pošlje na vaš mobilni telefon v obliki SMS sporočila ali pa jo generira namenska aplikacija. Na ta način, tudi če bi neznanec poznal vaše geslo, ne bi mogel dostopati do uporabniškega računa brez dodatne kode. Gre za rešitev, ki je že dobro znana uporabnikom spletnega in mobilnega bančništva (za generiranje dodatnega gesla je pogosto uporabljen poseben kalkulator ali mobilna aplikacija). Močno priporočamo, da si omogočite 2FA za tiste uporabniške račune, ki jim zaupate pomembne podatke (finančni podatki, fotografije, družbena omrežja), navodila za posamezne ponudnike najdete na povezavah:

- Google
- Facebook
- Microsoft
- Apple ID
- Paypal
- Instagram
- LinkedIn
- Twitter

b.) Deljenje podatkov z oglaševalci

Na internetu še kako velja, da ni zastonj kosila. Številne spletne platforme, od družabnih omrežjih, iskalnikov, medijskih portalov do množice mobilnih aplikacij, ponujajo svoje storitve na prvi pogled brezplačno. Vendar je račun na koncu izstavljen uporabnikom, ki z lastnimi osebnimi podatki poganjamo ekosistem digitalne oglaševalske ekonomije. Spletni uporabniki že s samim obiskovanjem spletnih strani ustvarjamo ogromno količino podatkov, ki jo na drugi strani oglaševalske platforme segmentirajo oz. profilirajo in »ponudijo« oglaševalcem v obliki dostopa do natančno razdelanih ciljnih občinstev. Uspešnejši so jasno tisti, ki oglaševalcu ponudijo dostop do čimbolj natančno ciljanega profila uporabnika, ki se bo posledično bolj verjetno odzval (klik, nakup, prenos aplikacije) na prikazan oglas. Pri tem izstopajo družbena omrežja, ki ponujajo možnost ciljanja na osnovi številnih kriterijev, pri čemer podatke zbirajo na različne načine:

- podatki, ki jih uporabniki sami vnesemo v naš profil (spol, starost, profilna/predstavitvena slika, opis, kraj bivanja itd.),
- podatki, zbrani s samo uporabo družbenih omrežjih: podatki o napravah, ki jih uporabljamo (operacijski sistem, vrsta povezave, GPS lokacija), vsebine, ki jih všečkamo, delimo, povezani prijatelji, povezave, ki jih klikamo itd.,
- podatki, ki so zbrani od drugih spletnih strani s pomočjo vtičnikov družbenih omrežjih (npr. gumbi Like in Share, integrirani na druga spletna mesta),
- podatki, zbrani s pomočjo tehnologije, ki omogoča sledenje uporabnikov na drugih spletnih straneh.

Ne le družbena omrežja, že zgolj uporaba spletnega iskalnika Google daje ponudniku te storitve dostop do naših osebnih podatkov tako, da različnim sledilnim tehnologijam, najpogosteje so to piškotki in sledilne slikovne točke (bolj znan izraz je tracking pixel), omogoči, da se shranijo na naš računalnik ali mobilno napravo. Tako shranjeni sledilni piškotki nosijo unikatni identifikator, po katerem je mogoče točno določenega uporabnika prepoznavati pri različnih aktivnostih na spletu (katere spletne strani obiskuje, katere ključne besede vpisuje v spletni iskalnik itd.). Posameznik nato na spletnih straneh, ki sodelujejo z izvajalcem tovrstnega **vedenjskega oglaševanja**, vidi le oglase, ki so vezani na njegov profil, zanimanja, interese.

Uporabniki vendarle imamo možnost omejiti možnost tovrstnega ciljanja oz. uporabe podatkov o naših spletnih aktivnosti za namen vedenjskega oglaševanja. Že z nekaj kliki lahko preverite in ustrezno ponastavitve dovoljenja za vedenjsko oglaševanje v storitvah Facebook in Google.

DODATEN NASVET: Pomislite še na druge naprave, povezane v internet

Ne pozabite tudi na gesla, ki ščitijo dostope do drugih, **v internet povezanih naprav, ki jih uporabljate v vašem domu:**

- Obvezno zamenjajte privzeto geslo, s katerim se povežete na nadzorno ploščo domačega **usmerjevalnika** (t.*i. router*). Nato določite geslo za dostop do brezžičnega omrežja.
- Zamenjate privzeto nastavljeno (tovarniško) uporabniško ime in geslo administratorskega vmesnika **spletne kamere**, ki jo uporabljate za domačo rabo. Prav tako nastavite močno geslo za dostop do spletne kamere, ki ga občasno tudi spremenite.

c.) Facebook nastavitve oglaševanja

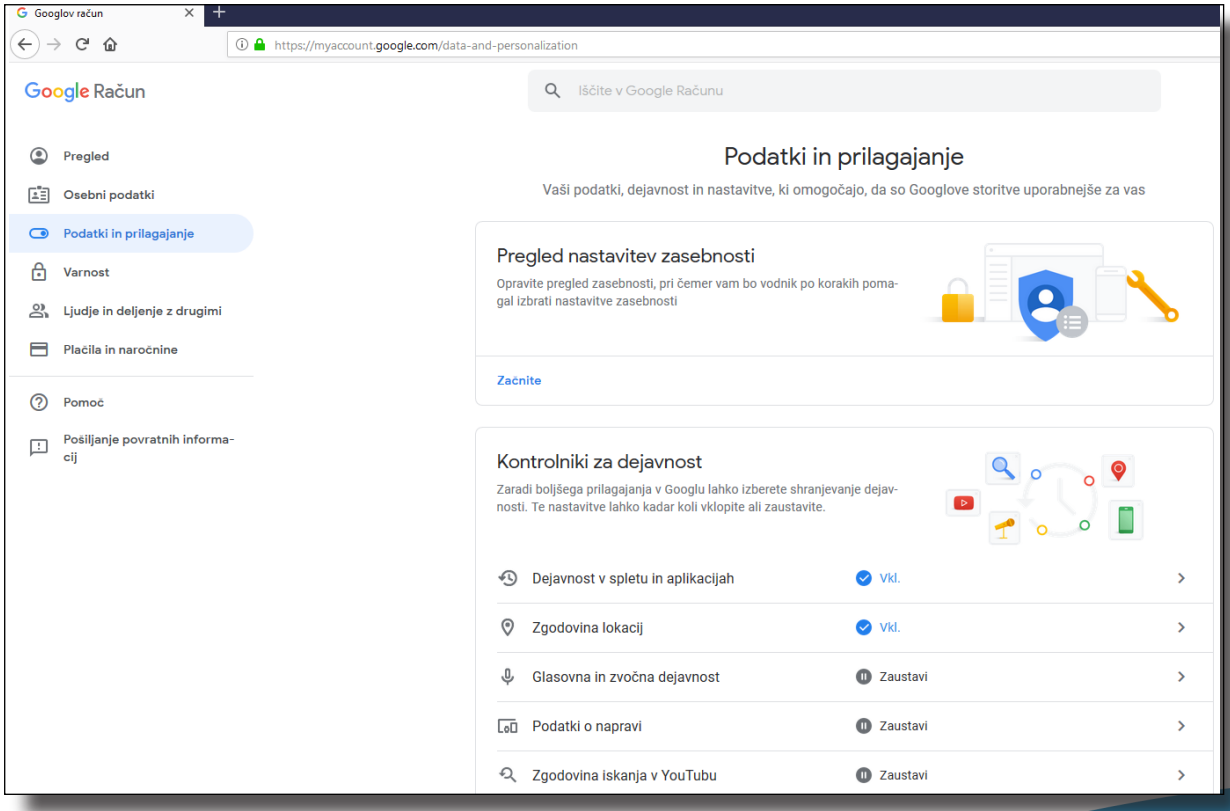
Če imate odprt Facebook profil, lahko na povezavi https://www.facebook.com/ads/settings dostopate do središča za upravljanje oglaševalskih nastavitev, kjer preverite, kateri oglaševalci že uporabljajo vaše podatke in ustrezno omejite obdelavo.

d.) Google nastavitve oglaševanja

V storitvi Google lahko na povezavi https://myaccount.google.com/ dostopate do središča, ki omogoča upravljanje s celotnim Google računom, pri čemer močno priporočamo, da občasno preverite oz. prilagodite nastavitve glede zbiranja podatkov o vaši dejavnosti na spletu.

Predvsem preverite razdelek **Podatki in prilagajanje**, kjer lahko po korakih preverite vse nastavitve zasebnosti.

V razdelku Prilaganje oglasov imate možnost izključiti prikazovanje oglasov na podlagi interesov (zabeležene spletne aktivnosti znotraj Google storitev in na drugih spletnih mestih).

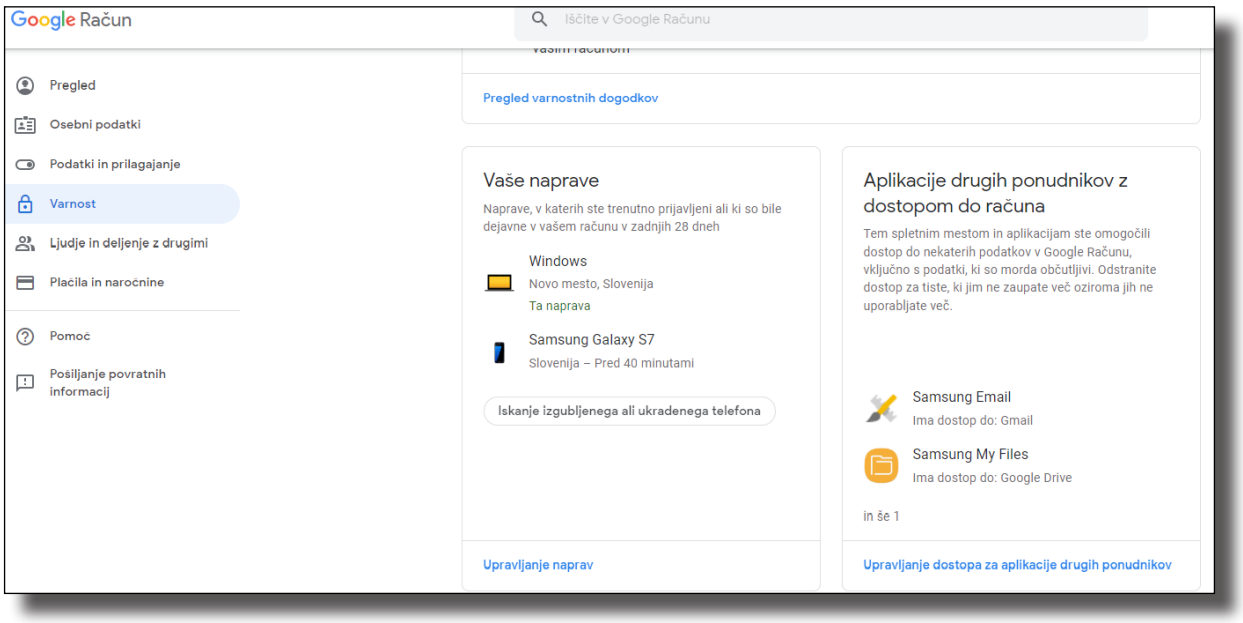


e.) Nadzor nad dostopi s strani tretjih oseb

Posredno imajo dostop do naših podatkov tudi spletna mesta in aplikacije drugih ponudnikov (*t.i. third party apps*), katerim dovolimo dostop do naših uporabniških računov, najpogosteje do Google in Facebook računa. Tako se lahko npr. z Google in Facebook računom prijavimo v določeno aplikacijo ali spletno mesto in nam ni potrebno ustvarjati novega uporabniškega računa (*t.i. social login*), seveda pa tako delimo tudi osnovne podatke o računu z drugim podjetjem. Aplikacije in spletne strani lahko zahtevajo različen nivo dostopa (ogled profila, dovoljenje za kopiranje podatkov, dovoljenje za urejanje ali ustvarjaje vsebine itd.), kar prinaša določena tveganja, povezana s premalo transparentnim obveščanjem, kako bodo podjetja obdelovala naše podatke in skrbela za ustrezno varnost. Zato tudi preverimo, katerim spletnim stranem in aplikacijam dovolimo dostop do uporabniških računov in uporabo podatkov.

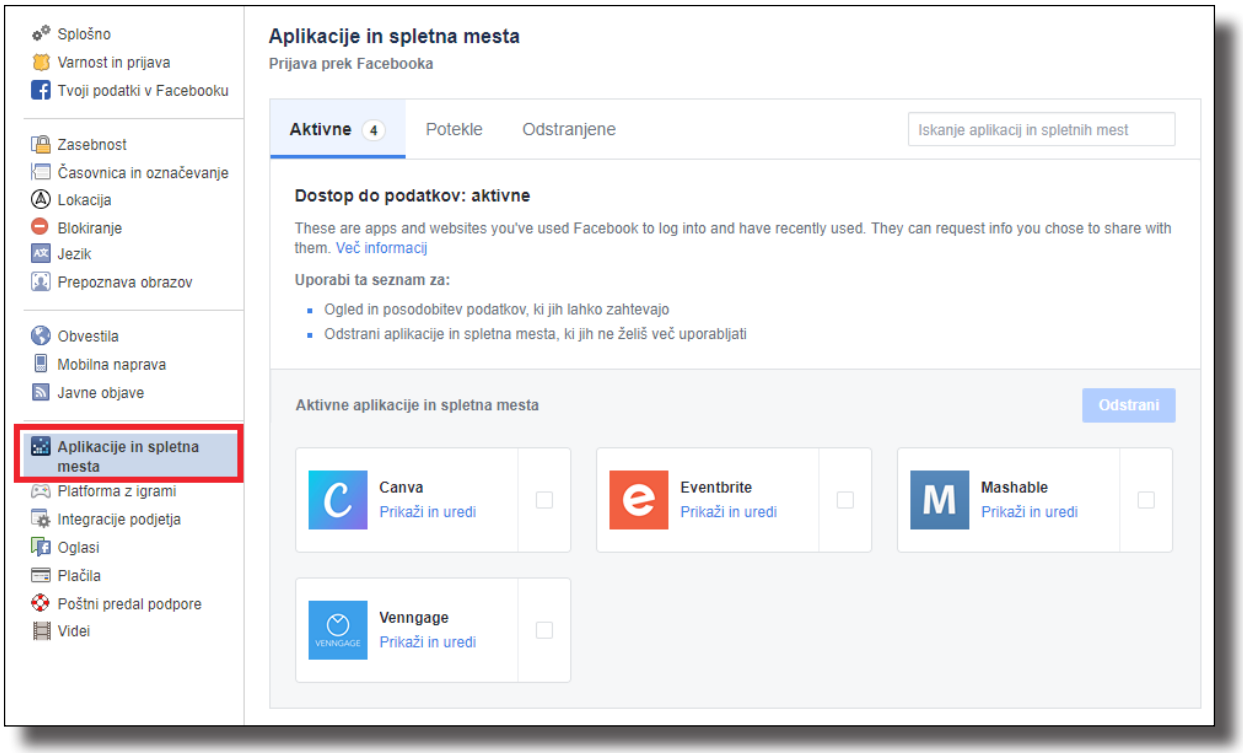
Odstranitev aplikacij in spletnih mest iz Facebook omrežja

Upravljanje iz središča za pomoč https://www.facebook.com/settings?tab=applications



Odstranitev aplikacij in spletnih mest iz Google računa

Upravljanje iz središča za pomoč https://myaccount.google.com/



f.) Nastavitve brskalnika

Za varno in zasebno uporabo interneta je optimizacija nastavitev brskalnika pomemben korak. Današnji priljubljeni brskalniki vključujejo vgrajene varnostne funkcije, vendar uporabniki pogosto te funkcije spregledajo in jih ne uporabljajo.

NASVETI ZA VARNO BRSKANJE Z BRSKALNIKOM GOOGLE CHROME:

Do nastavitev lahko dostopate preko osnovnega menija ali tako, da vpišete »chrome://settings/« v vrstico za iskanje.

Omogočite varno brskanje: Preverite, ali je funkcija »varno brskanje« v brskalniku Chrome omogočena. Najdemo jo v razdelku »Zasebnost in varnost«. Ta funkcija vas bo opozorila, če je spletno mesto, ki ga želite obiskati, morda lažno ali vsebuje zlonamerno vsebino.

Izklopite storitve za predvidevanje: Za optimalno varnost je priporočeno izklopiti funkcijo predvidevanja. Medtem ko ta ponuja nekaj udobja pri iskanju, ta funkcija brskalniku omogoča, da vse, kar vnesete v vrstico za iskanje takoj posreduje Googlu.

Ne uporabljajte sinhronizacije: Prekinite povezavo z e-poštnim računom, kar storite v zavihku "Osebe". Sinhronizacija e-poštnega računa z brskalnikom Chrome pomeni, da so osebni podatki, kot so gesla, podatki za samodejno izpolnjevanje, nastavitve in drugo shranjeni v Googlovih strežnikih. V primeru, da želite sinhronizacijo kljub temu uporabljati, je priporočljivo, da izberete možnost "Možnost šifriranja" in ustvarite unikatno geslo za šifriranje.

Konfiguriranje nastavitev vsebine: V razdelku "Zasebnost in varnost" kliknite "Nastavitve vsebine", kjer je priporočljivo storiti naslednje:

- Piškotki: Izberite "Ohrani lokalne podatke le do zaprtja brskalnika" in "Blokiraj piškotke drugih spletnih mest". Te možnosti zagotavljajo, da bodo vaši podatki izbrisani ob izhodu in Chroma in da vas oglaševalci ne bodo mogli slediti s t.i. Third-party piškotki.
- Pojavna okna in preusmeritve: Odznačimo "Dovoljeno" in izberemo "Blokirano"

Zamenjajte privzeti iskalnik: Večina iskalnikov beleži zgodovino vašega iskanja, ter vam potem na podlagi tega ponuja različne oglase. V nastavitvah lahko zamenjate iskalnik, ter izberite tistega, ki ne beleži zgodovine vašega iskanja (npr. iskalnik DuckDuckGo).

Konfigurirajte nastavitve gesel in obrazcev: Onemogočite samodejno izpolnjevanje in odznačite funkcijo "Ponudi shranjevanje gesel". Enako storite za razdelek plačilna sredstva ter naslovi in drugo. S tem bo Chromu onemogočeno shranjevanje prijav, gesel in drugih občutljivih podatkov, ki jih vnesete v obrazce.

NASVETI ZA VARNO BRSKANJE Z BRSKALNIKOM MOZILLA FIREFOX

Do teh nastavitev lahko dostopate prek menija "Možnosti".

Konfigurirajte nastavitve zasebnosti": V zavihku "Zasebnost in varnost" je priporočljivo izvršiti naslednje ukrepe, ki zagotavljajo, da Firefox shranjuje le toliko vaših podatkov, kot jih potrebuje za normalno delovanje.

- Izberite "Uporablja posebne nastavitve za zgodovino"
- Prekličite izbiro "Shranjuj zgodovino brskanja in prenosov"
- Prekličite izbiro "Shranjuj zgodovino iskanja in obrazcev"
- Izberite zavrni sledilce tretjih oseb
- Izberite funkcijo "Izbriši piškotke in podatke strani, ko se Firefox zapre«
- Izberite funkcijo »Počisti zgodovino ob izhodu iz programa Firefox«

Konfigurirajte varnostne nastavitve: V zavihku »Zasebnost in varnost« je priporočljivo izbrati naslednje nastavitve, ki preprečujejo Firefox-u shranjevanje gesel in preprečevanje obiskovanja potencialno škodljivih spletnih mest:

- Preverite, ali so omogočene možnosti »Zavrni nevarno in zavajajočo vsebino«, »Zavrni nevarne prenose« in »Opozori o neželeni in neobičajni programski opremi«.
- Prekličite izbiro »Ponujaj shranjevanje prijav in gesel za spletna mesta«.

Omogočite blokiranje pojavnih oken: Preverite, ali je v razdelku »Dovoljenja« izbrana možnost »Prepovej pojavna okna«. Običajno je ta funkcija izbrana že privzeto, saj uporabnike ščiti pred nezaželenimi oglasi in okni.

Ne uporabljajte sinhronizacije: Izogibajte se uporabi sinhronizacije. S tem preprečite Firefoxu shranjevanje vaših prijav, gesel in drugih občutljivih informacij.

Vklopite samodejne posodobitve: Preverite, ali je v zavihku »Splošno« v razdelku »Posodobitve Firefox-a« izbrana možnost »Samodejno nameščaj posodobitve«. S tem zagotovite, da brskalnik redno prejema kritične varnostne

g.) Nekaj koristnih dodatkov za brskalnike

Z namestitvijo nekaterih vtičnikov oz. razširitev za brskalnik lahko bistveno povečamo stopnjo zasebnosti, ki jo uživamo med brskanjem po spletu.

Adblock Plus (za Firefox, Chome, Opera, Android): Blokiranje neželenih spletnih oglasov https://adblockplus.org/

Ghostery (za Firefox, Chrome, Safari, Opera): Odkriva in zapre t. i. nevidne elemente programske kode spletne strani, ki vohunijo za uporabniki https://www.ghostery.com/

Privacy Badger (za Firefox, Chrome, Opera): Razširitev brskalnika, ki blokira programske skripte in druge sledilne tehnologije tretjih strani https://www.eff.org/privacybadger

DODATEN NASVET: Anonimen spletni iskalnik

Spletni iskalniki, kot so Google, Yahoo in drugi, hranijo in analizirajo naše vnose. Ko smo neko besedo vnesli v iskalnik, ostane tam dolgo, in če nas lahko iskalnik identificira s pomočjo piškotkov, začne na podlagi naših vnosov izdelovati celoten profil uporabnika. Spletni iskalniki tako zgolj na podlagi našega brskanja po spletu kmalu ugotovijo kakšne so naše navade, naši interesi, želje, družbeni status idr. Temu se je do neke mere mogoče izogniti z uporabo t.i. anonimnih spletnih iskalnikov. Eden od najbolj razširjenih je gotovo **DuckDuckGo,** do zasebnosti zelo prijazen pa je tudi **Startpage (nekdaj Ixquick)**, ki vse dnevniške zapise (o tem kaj smo iskali) samodejno uniči po 48 urah, razen tega pa ta iskalnik sploh nima piškotov, ki bi nas zasledovali med našim sprehodom prek speta. Preskusite lahko tudi druge anonimne iskalnike: **Gibiru** ali **Qwant.**

5. Tretji varnostni obroč: Katere podatke sam delim?

Različne tehnične rešitve (antivirusni programi, redne posodobitve operacijskega sistema in druge programske opreme, pametni USB ključi in kartice itd.) in redni pregledi nastavitev zasebnosti predstavljajo zgolj osnovne ukrepe za zaščito naših osebnih podatkov. **Ustrezna skrb za informacijsko zasebnost mora biti več kot zgolj skrb za programsko opremo.** Ta pa zahteva več razmisleka, preudarnega vrednotenja informacij na spletu in previdnega obnašanja s strani spletnih uporabnikov.

Še vedno lahko uporabniki za varstvo svojih osebnih podatkov največ storite prav sami, z enim preprostim nasvetom – **berite drobni tisk!** Dolžnost vsakega podjetja oziroma institucije, ki zbira in uporablja vaše osebne podatke (upravljavca osebnih podatkov) je, da vam jasno, jedrnato in razumljivo predstavi, kako bo obdeloval vaše osebne podatke in ustrezno poskrbel za njihovo varstvo. Zato pred vsakim sodelovanjem v nagradnih igrah, prijavo na elektronske novičke ali odprtjem novega uporabniškega računa določene spletne storitve, **vedno preberite, zakaj potrebujejo vaše podatke in kaj bodo z njimi počeli.**

a.) Katere informacije vam morajo zagotoviti upravljavci, še preden jim zaupate svoje podatke?

***Kdo** obdeluje vaše podatke?*	Upravljavec mora navesti naziv podjetja ali organizacije in naslov oz. sedež ter podatke o pooblaščeni osebi za varstvo podatkov, če je ta imenovana.
***Zakaj** obdelujejo osebne podatke?*	Upravljavci morajo čim natančneje opredeliti, za kakšen namen in na kateri pravni podlagi (npr. privolitev, zakoniti interes, izvajanje pogodbe,…) obdelujejo vaše osebne podatke. Pri zakonitem interesu morajo upravljavci tudi navesti, v čem je njihov zakoniti interes. Če od vas zahtevajo, da posredujete svoje osebne podatke (npr. zaradi izvajanja pogodbe), naj tudi navedejo, kakšne bodo posledice, če jih ne posredujete.
***Komu** bodo podatke posredovali?*	Če bodo posredovali vaše osebne podatke tretjim osebam (npr. zunanji vzdrževalci spletnega mesta, oglaševalska podjetja, javni organi), vas morajo s tem seznaniti pred vnosom podatkov. Prav tako vas morajo seznaniti, če bodo vaše podatke prenesli v tretje države ali mednarodne organizacije.
***Koliko časa** bodo podatke hranili?*	Upravljavec mora opredeliti, koliko časa bo osebne podatke hranil, kjer to ni mogoče pa vsaj kriterije, po katerih se določi čas hrambe osebnih podatkov (npr. »podatke bomo hranili za čas trajanja prodajne akcije ali podatke bomo hranili do preklica privolitve za prejemanje e-novic«).
*Katere so vaše **pravice**?*	Upravljavec vas mora seznaniti z vašimi pravicami s področja osebnih podatkov. Po Splošni uredbi o varstvu podatkov imate pravico do: » **dostopa (tudi prepisa in kopiranja)**, » **popravka** netočnih ali dopolnitve nepopolnih podatkov, » **izbrisa**, » **omejitve obdelave**, » **ugovora** in » **prenosljivosti** osebnih podatkov. Prav tako vas morajo upravljavci obvestiti o pravici do pritožbe pri nadzornem organu za primere kršitev. V Sloveniji je to Informacijski pooblaščenec. Če podjetje ali organizacija podatke obdeluje na osnovi vaše privolitve, vas morajo obvestiti, da lahko privolitev kadarkoli prekličete (kot na primer če ste podali privolitev, da želite prejemati e-novičke, vas morajo jasno obvestiti, da se lahko odjavite).
*Obdelava za **drug namen***	Kadar namerava upravljavec obdelovati vaše osebne podatke še v druge namene, vam mora sporočiti ta drug namen oz. namene že ob zbiranju, npr. »elektronski naslov, ki ste nam ga posredovali ob spletnem nakupu, bomo uporabili tudi za neposredno trženje«.
Če osebnih podatkov upravljavec ni pridobil neposredno od vas, vam mora zagotoviti vse zgoraj navedene informacije in dodatno še: vrste osebnih podatkov, ki jih je pridobil, od kje izvirajo, in po potrebi, ali izvirajo iz javno dostopnih virov. **Zato vedno preverite, komu zaupate svoje podatke in kaj bodo z njimi počeli. To je vaša pravica do informiranosti in sprejemanja informiranih odločitev!**	

b.) Katere podatke sami delite? Čim manj, tem bolje!

Zavedajte se, da boste veliko težje umaknili določene vsebine s spleta, kot če bi že v izhodišču omejili svoje objave, npr. na družbenih omrežjih ali spletnih forumih. Pomislite, v kakšni luči vas prikažejo določeni komentarji in fotografije, ali bi jih brez težav pokazali na razgovoru za službo? Prav tako ne objavljajte osebnih podatkov drugih oseb brez njihove privolitve (npr. objava fotografij na družbenih omrežjih ali blog zapisih), še posebno pa bodite previdni z objavami fotografij otrok.

Vedno, ko posredujete svoje osebne podatke, se držite pravila, da posredujete le **nujno potrebne podatke**, ki so potrebni za izpolnitev določenega namena. Kaj to pomeni? Zgolj za sodelovanje v nagradni igri verjetno zadostuje vaš elektronski naslov in ne davčna številka ali fizični naslov, ki ju organizator potrebuje šele takrat, ko želi podeliti nagrado izžrebancem. Za prenos priročnika, npr. o zdravi prehrani, prek spleta verjetno prav tako zadostuje elektronski naslov in ni potrebe posredovati tudi mobilne številke za namen prejetja dokumenta.

Natančno preberite, **do katerih podatkov bodo dostopale mobilne aplikacije**, še preden jih prenesete iz tržnice aplikacij. Aplikacije pogosto zahtevajo veliko več podatkov, kot jih dejansko potrebujejo za svoje delovanje. Je res potrebno, da aplikacija, npr. »Svetilka« dostopa do vseh vaših shranjenih fotografij in kontaktov?

Dodatno previdnost terja **posredovanje vaših finančnih podatkov**, npr. številke kreditne kartice in CVV kode. Kadar na spletu vpisujete številko kreditne kartice, skrbno preverite znake, ki zagotavljajo šifriran prenos podatkov (HTTPS povezava, zaklenjena ključavnica v URL vrstici) in natančno preverite spletnega trgovca. Prav tako ne zaupajte elektronskim, telefonskim ali drugim sporočilom, četudi navidezno prihajajo od vaše banke ali hranilnice, s katerimi vas obveščajo o zlorabi vaše kartice in vas hkrati pozivajo, da poveste podatke o svoji kartici ali da jih vpišete v tako imenovane varnostne obrazce na spletu.

DODATEN NASVET: Kaj lahko objavljam o drugih?

Pogosto vprašanje, ki se poraja spletnim uporabnikom, se nanaša na njihove lastne uporabniške profile na družbenih omrežjih, v smislu: »Ali kršim zakonodajo s področja varstva osebnih podatkov, če objavim fotografijo (ali kakšne druge osebne podatke) nekoga drugega?« Objave posameznikov na njihovih lastnih profilih družbenih omrežjih (tudi spletnih forumih, komunikacija prek elektronske pošte ali skupna raba oblačnih storitev), ko ne gre za objave komercialne narave, lahko razumemo kot **izjemo zasebne rabe**, saj v skladu z uvodno določbo 18 Splošne uredbe osebne ali domače dejavnosti lahko vključujejo tudi korespondenco na družbenih omrežjih, pri čemer tovrstne objave lahko tudi predstavljajo obdelavo osebnih podatkov, npr. objava imena in priimka ali fotografije posameznika. **Vendar to nikakor ni zelena luč, da je vsakršno objavljanje osebnih podatkov na zasebnih profilih tudi sicer zakonito.** Objava osebnih podatkov lahko predstavlja poseg v pravico drugih posameznikov do zasebnosti v širšem smislu, katere meje so začrtane v 35. členu Ustave RS (varstvo pravic zasebnosti in osebnostnih pravic). Namreč ravnanje nezakonite objave osebnih podatkov lahko pomeni storitev katerega od kaznivih dejanj zoper čast in dobro ime iz Kazenskega zakonika. Nadalje se je v takšnem primeru mogoče pod določenimi pogoji poslužiti tudi institutov civilnega prava (npr. zahteve za prenehanje s kršitvami osebnostnih pravic iz 134. člena Obligacijskega zakonika, zahteve za povrnitev premoženjske in nepremoženjske škode ter drugih institutov civilnega prava).

Mogoče je pred objavo podatkov drugih na mestu povsem enostavno vprašanje – ali bi jih motilo, če objavim njihove podatke? Morda je pa prav, da to preverim, preden objavim? Če mene kaj takega ne bi motilo, to še ne pomeni, da to ne moti tudi drugih - nikomur nimam pravice odvzeti moči odločanje o lastnih podatkih, zato se je o tem bolje prepričati vnaprej.

c.) KORISTNI NASVETI: odstranitev iz Google zadetkov, zameglitev google street view posnetkov

ODSTRANITEV IZ GOOGLE ZADETKOV

Svetovni splet ima dolg spomin in včasih se zdi, da je odstranitev vsebine na spletu misija nemogoče. Pa vendar posamezniki imamo pravico in tudi načine, kako lahko naše osebne podatke, objavljene na spletu, odstranimo. Najprej je potrebno ločiti med vsebino, ki se nahaja na določeni spletni strani in rezultati Google iskanja, ki pokažejo pot do te strani. Če Google kot **rezultat iskanja imena in priimka uporabnika vrne povezave do spletne strani, ki bi lahko škodila ugledu uporabnika ali razkrila posebne vrste osebnih podatkov (občutljive)**, mora uporabnik za **izbris najprej zaprositi upravljavca spletne strani,** na kateri se nahajajo sporni podatki. Šele ko upravljavec spletne strani izbris zavrne, lahko uporabnik zahteva izbris iz rezultatov iskanja neposredno od Googla.

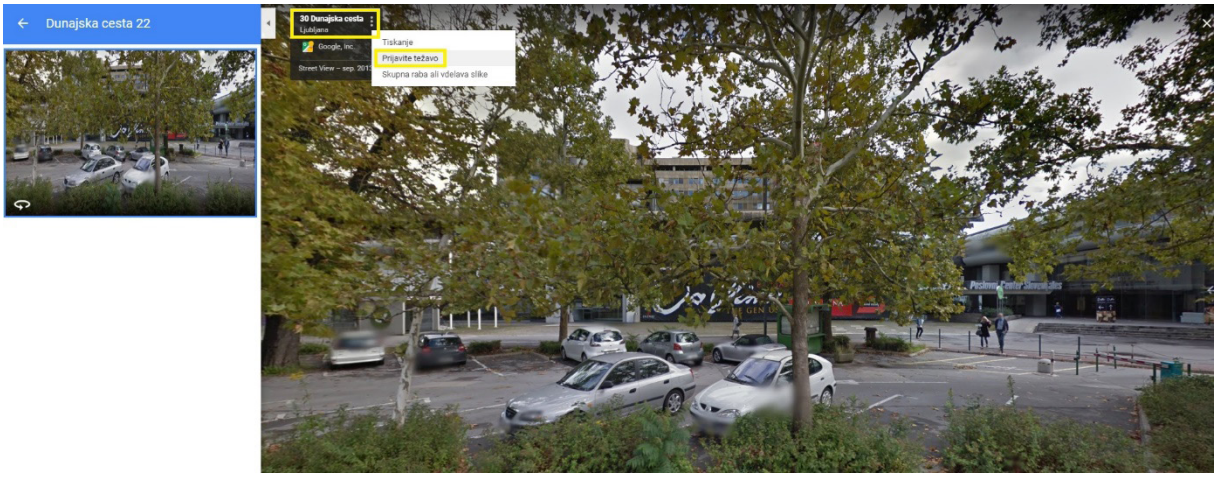
1. Zahtevo za izbris vsebine naslovite neposredno na upravljavca spletne strani.
2. Če upravljavec vaše podatke izbriše iz spletne strani, vendar še vedno ostane posnetek strani (cache), potem uporabite Google obrazec za pomoč pri izbrisu **zastarele vsebine**.

3. Če upravljavec spletne strani ne izpolni zahteve po izbrisu osebnih podatkov, lahko na Google naslovite vašo zahtevo, da izbrišejo iskalni zadetek z vašim imenom in priimkom, ki vodi do spletne strani, kjer se nahajajo vaši podatki. Google bo vsako posamezno zahtevo obravnaval ločeno in skušal presoditi, ali rezultati res vsebujejo zastarele ali neprimerne informacije. Pri tem bodo skušali pretehtati med pravico do zasebnosti in javnim interesom. Javni interes obstaja predvsem pri informacijah, ki se nanašajo na finančne prevare, neprimerno politično ravnanje, kazenske obsodbe ipd.

ZAMEGLITEV GOOGLE STREET VIEW POSNETKOV

Posamezniki imamo tudi možnost **zamegliti obraze in registrske tablice, ki jih pokaže storitev Google Street View.** Čeprav Google tehnologija omogoča avtomatizirano zamegljevanje prepoznanih obrazov ter registrskih tablic, lahko na Google naslovite posebno zahtevo, če ste opazili obraz ali registrsko tablico, ki jo je treba dodatno zamegliti.

Prav tako lahko sporočite zahtevo, če želite zamegliti svojo celotno hišo ali avto, vendar upoštevajte, da ko Google zamegli sliko, tega ni več mogoče razveljaviti. Če pošljete zahtevo za zameglitev svoje hiše na slikah v storitvi Street View, bodo zamegljeni tudi vsi pretekli in prihodnji posnetki hiše.



KAKO ZAHTEVATE ZAMEGLITEV NA GOOGLE STREET VIEW?

V **spletnem brskalniku** kliknite tri pikice, ki se pojavijo ob prikazanem naslovu in izberite možnost »Prijavi težavo«.

» Ko uporabljate storitev Google Street View **v aplikaciji na pametnem telefonu**, potem kliknite na zastavico desno zgoraj, ki vam odpre različne možnosti za sporočanje težav in zamegljevanje.

Namesto zaključka

Naše smernice običajno zaključimo z določenim vsebinskim zaključkom, tokrat pa vas raje usmerjamo na nekaj zanimivih vsebin, kjer:

- boste lahko ugotovili, da imamo mogoče do zasebnosti podoben odnos, kot smo ga imeli včasih do varovanja okolja: poglejte si to spletno stran - https://www.socialcooling.com/.
- lahko bolj plastično vidite, kaj pomeni izguba zasebnosti - ste si ogledali filme Posebno poročilo (Minority report), Mreža (The Net), Življenje drugih (Das Leben der Anderen) ali Gattaca?
- dobite več informacij o vaših pravicah in kako jih uveljavite: obiščite https://tiodlocas.si/.