

MOJE DIGITALNE PRAVICE

PRAKTIČNI VODIČ ZA MLADE

Avtorici: Alla Kvašina, Mirjana Babić



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST
IN MLADINO



Sofinancira
Evropska unija



NOVA
UNIVERZA

Operacijo sofinancirata Republika Slovenija, Ministrstvo za izobraževanje, znanost in mladino ter Evropska unija iz Evropskega socialnega sklada plus (ESS+) v okviru javnega razpisa Problemsko učenje študentov v delovno okolje 2024–2027 (PUŠ 2024–2027).

Kazalo

1. UVOD: ZAKAJ SE DIGITALNE PRAVICE TIČEJO MENE?	2
2. OSNOVE: OSEBNI PODATKI, ZASEBNOST IN DIGITALNA HIGIENA.....	3
3. MOJE PRAVICE V 3 BARVAH	4
4. COOKIES, POGOJI UPORABE IN SOGLASJA.....	7
5. DIGITALNA HIGIENA: 7 NAVAD, KI VARUJEJO MOJE PRAVICE	9
6. SCENARIJI IZ VSAKDANJEGA ŽIVLJENJA.....	10
6.1 Družbena omrežja	10
6.2 Messengerji in sumljive povezave.....	11
6.3 Spletni nakupi.....	13
6.4 Univerza in študijsko okolje.....	14
6.5 Javne e-storitve	15
6.6 AI orodja in chatbot-i	16
7. KAJ NAREDIM, KO GRE KAJ NAROBE?	17
8. KAM PO POMOČ?	18
9. FAQ.....	19
10. CHECKLIST	21
11. ZAKLJUČEK.....	22

1. UVOD: ZAKAJ SE DIGITALNE PRAVICE TIČEJO MENE?

Če uporabljaš telefon, družbena omrežja, spletne trgovine, messengerje, aplikacije za študij, javne e-storitve ali AI orodja, potem vsak dan puščaš digitalne sledi. Nekatere sledi pustiš namenoma: objaviš fotografijo, pošlješ sporočilo, izpolniš obrazec ali naročiš izdelek. Druge nastanejo skoraj neopazno: piškotki, lokacija, podatki o napravi, zgodovina klikov, všečki, čas ogleda videa ali podatki o tem, katera vsebina te zanima.

Digitalne pravice niso nekaj oddaljenega ali samo za pravnike. Gre za vprašanja, ki se pojavljajo sproti in brez opozorila:

- Ali mora aplikacija res vedeti mojo lokacijo?
- Kaj če mi nekdo vdre v račun?
- Kaj če platforma izbriše mojo objavo ali blokira profil?
- Ali lahko zahtevam, da podjetje izbriše moje podatke?
- Kaj če nekdo objavi mojo fotografijo brez dovoljenja?
- Ali je varno pošiljati osebne podatke chatbotu?

Ta vodič ti ne bo razložil vseh zakonov do zadnje podrobnosti. Njegov namen je bolj praktičen: da razumeš, **kaj se dogaja s tvojimi podatki, katere pravice imaš in kaj lahko narediš, ko gre kaj narobe.**

POMNI: Digitalne pravice niso samo teorija. Varuješ jih vsak dan — z nastavitvami zasebnosti, previdnostjo pri klikih, močnimi gesli, vprašanji, ki jih postaviš platformi, in s tem, da veš, kam se obrniti po pomoč.

2. OSNOVE: OSEBNI PODATKI, ZASEBNOST IN DIGITALNA HIGIENA

Kaj so osebni podatki?

Osebni podatki so vse informacije, ki se nanašajo nate kot določeno ali določljivo osebo. Nekateri so očitni, drugi manj.

Neposredno prepoznavni osebni podatki:

- ime in priimek,
- naslov,
- telefonska številka,
- e-mail,
- fotografija obraza,
- uporabniško ime, če te je mogoče prepoznati,
- številka dokumenta,
- podatki o bančni kartici, itd.

Posredni oziroma digitalni osebni podatki:

- IP-naslov,
- lokacija,
- ID naprave,
- cookie ID,
- zgodovina nakupov,
- všečki in komentarji,
- podatki o tem, katere objave gledaš,
- podatki o prijavi v račun,
- podatki iz študijskih platform.

PAZI! Osebni podatek ni samo tvoj EMŠO ali številka osebne izkaznice. Tudi kombinacija več "malih" podatkov lahko pove zelo veliko o tebi.

Kaj je zasebnost?

Zasebnost pomeni, da imaš nadzor nad tem, kaj, kdaj, zakaj in v kakšnem obsegu ve kdo o tebi.

Zasebnost ni isto kot "skrivanje". Tudi če nimaš ničesar za skrivati, imaš pravico, da ne deliš vsega z vsemi.

PRIMER:

Čisto v redu je, da svojo fotografijo pokažeš prijateljem. Ni pa nujno v redu, da jo nekdo brez tvoje vednosti objavi javno, shrani, deli naprej ali uporabi za lažni profil.

Kaj je digitalna higiena?

Digitalna higiena pomeni zaščito tvojih računov, naprav, podatkov in komunikacije pred zlorabo. Sem spadajo gesla, dvofaktorska avtentikacija, posodobitve, previdnost pri povezavah, varnostne kopije in nastavitve zasebnosti.

MIT: "Digitalna higiena je samo za IT strokovnjake."

RESNICA: Osnovna digitalna higiena je za vsakogar. Če znaš zakleniti vrata stanovanja, se lahko naučiš tudi zakleniti svoje digitalne račune.

Kako so pravice in digitalna higiena povezane?

Če imaš pravico do zasebnosti, a uporabljaš isto geslo povsod, je tvoja zasebnost veliko bolj ranljiva. Če imaš pravico do varstva osebnih podatkov, a brez premisleka pošiljaš dokumente neznanim profilom, si povečaš tveganje zlorabe.

Zato digitalna higiena ni nekaj ločenega od pravic. Je način, kako svoje pravice vsak dan praktično varuješ.

3. MOJE PRAVICE V 3 BARVAH

Digitalne pravice niso vse enake. Nekatere lahko uveljavljaš precej neposredno. Nekatere veljajo samo pod določenimi pogoji. Nekatere stvari pa sploh niso univerzalna pravica, ampak so odvisne od pravil platforme.

Zato si jih najlažje zapomniš v treh barvah.

1. Močne pravice: praviloma jih lahko zahtevaš neposredno

Pravica do informacij

Imaš pravico vedeti, kdo zbira tvoje podatke, katere podatke zbira, zakaj jih uporablja, koliko časa jih hrani in komu jih posreduje.

PRIMER:

Aplikacija želi tvoj e-mail, lokacijo in dostop do kontaktov. Imaš pravico vedeti, zakaj potrebuje vsakega od teh podatkov.

Pravica do dostopa

Lahko zahtevaš informacijo, katere osebne podatke ima organizacija o tebi.

POMNI: To ne pomeni nujno, da dobiš vse interne dokumente podjetja. Pomeni pa, da imaš pravico do informacij o svojih osebnih podatkih.

Pravica do popravka

Če so podatki o tebi napačni ali nepopolni, lahko zahtevaš popravek.

PRIMER:

V študijskem sistemu je napačno zapisan tvoj naslov ali e-mail. Lahko zahtevaš popravek.

Pravica do preklica privolitve

Če si za določeno uporabo podatkov dal privolitev, jo lahko praviloma tudi prekličeš.

MIT: "Če sem enkrat kliknil 'strinjam se', ne morem več nič."

RESNICA: Če obdelava temelji na tvoji privolitvi, jo lahko prekličeš. Preklic mora biti praviloma tako enostaven, kot je bila dana privolitev.

Pravica do ugovora pri neposrednem trženju

Če organizacija uporablja tvoje podatke za neposredno trženje, lahko temu ugovarjaš. To je ena močnejših pravic, ki jo mladi pogosto podcenjujejo.

PRIMER:

Spletna trgovina ti nenehno pošilja oglasna sporočila. Lahko se odjaviš od novic oziroma zahtevaš, da tvojih podatkov ne uporablja več za neposredno trženje.

2. Pogojne pravice: mogoče, ampak ne vedno

Pravica do izbrisa

V določenih primerih lahko zahtevaš izbris osebnih podatkov. Toda izbris ni vedno avtomatičen.

Organizacija lahko nekatere podatke hrani, če ima za to zakonit razlog, na primer zakonsko obveznost, pogodbo, varnostni razlog ali pravni zahtevek.

Pravica do omejitve obdelave

V določenih primerih lahko zahtevaš, da organizacija podatkov začasno ne uporablja, na primer dokler se preverja točnost podatkov ali zakonitost obdelave.

Pravica do prenosljivosti

V nekaterih primerih lahko zahtevaš, da dobiš svoje podatke v strukturirani obliki ali da se prenesejo drugemu ponudniku. To ne velja za vse vrste podatkov in vse situacije.

Pravice pri avtomatiziranem odločanju

Če o tebi pomembno odloča popolnoma avtomatiziran sistem, imaš v določenih primerih posebne pravice, na primer pravico do informacij o logiki, pomenu in posledicah takšne obdelave.

PAZI! To ne pomeni, da imaš vedno pravico do celotne izvirne kode algoritma. Lahko pa imaš pravico do razumljivih informacij o tem, kako odločitev vpliva nate.

Odškodnina

Če pride do kršitve varstva osebnih podatkov, je odškodnina lahko mogoča, vendar ni avtomatična za vsako napako ali vsako uhajanje podatkov. Običajno morajo biti izpolnjeni pogoji, kot so kršitev, škoda in vzročna zveza.

3. Pravila platforme: ni vedno pravica po zakonu

Nekatere stvari niso univerzalna pravica, ampak so odvisne od pravil platforme.

Pravo ime ali psevdonim

Nekatere platforme dovoljujejo psevdonim, druge zahtevajo pravo ime. V EU ni splošnega pravila, da lahko na vsaki platformi vedno uporabljaš izmišljeno ime.

Blokiranje računa

Platforma lahko ukrepa, če meni, da si kršil pravila skupnosti. Toda v EU imajo uporabniki na spletnih platformah tudi določene možnosti pritožbe oziroma izpodbijanja odločitev platforme.

Algoritmi in priporočila

Platforme uporabljajo algoritme za priporočanje vsebin. Lahko imaš določene pravice do informacij in nastavitev, vendar to ne pomeni, da lahko vedno zahtevaš popolno razlago vsakega koraka algoritma.

4. COOKIES, POGOJI UPORABE IN SOGLASJA

Večina nas je že kliknila “sprejmi vse”, ne da bi prebrala, kaj sprejema. To je razumljivo — pogoji so pogosto dolgi, dolgočasni in napisani v jeziku, ki ga skoraj nihče ne bere z veseljem.

Toda to ne pomeni, da moraš klikati na slepo.

Kaj so cookies?

Cookies oziroma piškotki so majhne datoteke ali oznake, ki jih spletna stran shrani v tvojo napravo. Nekateri so potrebni, da stran deluje. Drugi se uporabljajo za analitiko, oglaševanje ali sledenje.

Nujni cookies

Ti so lahko potrebni za osnovno delovanje strani, na primer za prijavo v račun ali košarico v spletni trgovini.

Oglaševalski in sledilni cookies

Ti lahko spremljajo tvoje vedenje za oglase, profiliranje ali merjenje učinkov kampanj.

PAZI! Gumb “sprejmi vse” je pogosto najhitrejši, ni pa nujno najboljši za tvojo zasebnost.

Kaj preverim v 30 sekundah?

Preden klikneš:

1. Ali lahko zavrnem nenujne cookies?
2. Ali je gumb “zavrni” enako viden kot “sprejmi”?
3. Ali je jasno, kdo zbira podatke?
4. Ali gre za oglase ali profiliranje?
5. Ali lahko kasneje spremenim izbiro?

MIT: “Če zavrnem cookies, spletna stran ne sme več delovati.”

RESNICA: Odvisno. Nekateri cookies so nujni za delovanje strani, drugi niso. Stran lahko potrebuje nujne cookies, ne sme pa vedno pogojevati vsega z oglaševalskim sledenjem.

Pogoji uporabe

Pogoji uporabe povedo, kaj smeš in česa ne smeš početi na platformi. Politika zasebnosti pa pove, kako se obdelujejo tvoji podatki. Oboje je pomembno, vendar ni realno, da boš vedno prebral vse.

Zato poišči vsaj ključne točke:

- kateri podatki se zbirajo,
- zakaj se uporabljajo,
- komu se posredujejo,
- kako lahko izbrišeš račun,
- kako uveljavljaš pravice,
- kako se pritožiš.

POMNI: Če ne razumeš, kaj sprejemaš, ne pomeni, da si neumen. Pogosto je problem v tem, da so informacije napisane preveč splošno in zapleteno.

5. DIGITALNA HIGIENA: 7 NAVAD, KI VARUJEJO MOJE PRAVICE

Digitalna higiena pomeni vsakodnevne navade, s katerimi zmanjšaš tveganje zlorab.

1. Uporabljalj unikatna gesla

Za vsak pomemben račun uporabljalj drugo geslo. Posebej za e-mail, banko, družbena omrežja in študijske račune.

MIT: "Moje geslo je močno, zato ga lahko uporabljam povsod."

RESNICA: Če isto geslo uporabiš na več straneh in ena stran izgubi podatke, so ogroženi tudi drugi računi.

2. Uporabi upravitelja gesel

Upravitelj gesel ti pomaga ustvarjati in shranjevati dolga, unikatna gesla. Tako si ni treba zapomniti vseh.

3. Vklopi MFA oziroma 2FA

Dvofaktorska avtentikacija pomeni, da za prijavo ni dovolj samo geslo. Potrebuješ še drugi korak, na primer aplikacijo, kodo ali varnostni ključ.

PAZI! Kode za prijavo nikoli ne pošiljalj drugim. Če te nekdo prosi za MFA kodo, gre skoraj zagotovo za prevaro.

4. Posodabljalj naprave in aplikacije

Posodobitve pogosto odpravljajo varnostne luknje. Če jih odlašaj predolgo, si bolj ranljiv.

5. Preveri povezavo, preden klikneš

Pri sumljivih sporočilih preveri:

- kdo je pošiljatelj,
- ali je povezava čudna (npr. napačno črkovanje imena podjetja, nenavadna končnica domene ali skrita povezava, ki ne ustreza besedilu),

- ali sporočilo seje paniko,
- ali zahteva geslo, kartico ali kodo,
- ali obljublja nekaj predobrega.

6. Nastavi zasebnost profilov

Preveri, kdo vidi tvoje objave, kdo ti lahko piše, kdo te lahko označi in katere aplikacije imajo dostop do tvojega računa.

7. Deli manj podatkov

Ne pošiljaj dokumentov, gesel, kod, intimnih fotografij, podatkov kartice ali občutljivih informacij, če ni jasno, kdo jih zahteva in zakaj.

POMNI: Najvarnejši podatek je tisti, ki ga sploh ni treba deliti.

6. SCENARIJI IZ VSAKDANJEGA ŽIVLJENJA

V tem delu so zbrane situacije, ki se lahko zgodijo vsakomur. Pri vsaki si zapomni osnovno pravilo:

Najprej prepreči nadaljnjo škodo, nato shrani dokaze, potem ukrepaj.

6.1 Družbena omrežja

Družbena omrežja niso samo prostor za objave in sporočila. Tam puščaš podatke o tem, kaj gledaš, všečkaš, komentiraš, komu pišeš in kje se nahajaš.

PRIMER:

Nekdo objavi tvojo fotografijo z zabave, te označi in doda lokacijo. Objave ne želiš imeti javno, ker je neprijetna in jo lahko vidijo tudi ljudje, ki jih ne poznaš.

Kaj je tveganje?

Na družbenih omrežjih lahko pride do:

- objave fotografij ali videov brez dovoljenja,
- pojava lažnih profilov,

- vdora v račun,
- nadlegovanja ali groženj,
- zbiranja podatkov za oglase in profiliranje,
- blokiranja računa ali odstranitve objave.

Kaj naredim?

Če nekdo objavi tvojo fotografijo ali podatke:

1. Shrani dokaz: screenshot, povezavo, datum in ime profila.
2. Zahtevaj odstranitev, če je to varno in smiselno.
3. Prijavi objavo platformi.
4. Preveri nastavitve zasebnosti.
5. Če gre za grožnje, izsiljevanje ali intimne vsebine, poišči pomoč takoj.

Če ti nekdo vdre v račun:

1. dostop obnavljaj samo prek uradne strani platforme,
2. zamenjaj geslo,
3. odjavi vse naprave,
4. vklopi MFA (večfaktorska avtentikacija – dodatna varnostna potrditev poleg gesla),
5. obvesti prijatelje, naj ne klikajo povezav iz tvojega računa.

MIT: “Če nekaj objavim samo za prijatelje, je popolnoma varno.”

RESNICA: Nekdo lahko naredi screenshot, objavo deli naprej ali jo shrani. Nastavitve zasebnosti pomagajo, niso pa čarobni ščit.

PAZI! Vsega, kar se dogaja na platformi, ne urejajo samodejno zakoni o varstvu osebnih podatkov. Včasih gre za pravila platforme, včasih za zasebnost, v hujših primerih pa tudi za kaznivo ravnanje.

POMNI: Preden objaviš, premisli. Če gre kaj narobe, najprej shrani dokaze — šele nato briši, blokiraj ali prijavljaj.

6.2 Messengerji in sumljive povezave

Messengerji so hitri in osebni, zato jim pogosto zaupamo bolj kot e-mailu. Prav zato so pogost prostor za phishing in prevare.

PRIMER:

Prejmeš sporočilo: "Tvoj paket čaka. Plačaj 1,99 € za dostavo." Sporočilo vsebuje povezavo, stran pa zahteva podatke bančne kartice.

Red flags

Bodi pozoren, če sporočilo:

- zahteva hitro ukrepanje,
- grozi z zaprtjem računa,
- obljublja nagrado,
- zahteva geslo, kartico ali MFA kodo,
- prihaja z neznane številke,
- vsebuje čudno povezavo,
- je napisano v nenavadni slovenščini.

Kaj naredim?

Če še nisi kliknil:

1. Ne klikaj povezave.
2. Preveri pošiljatelja.
3. Uradno stran odpri ročno, ne prek povezave.
4. Sporočilo prijavi kot spam/phishing.
5. Po potrebi ga posreduj pristojni službi (npr. varnostni službi platforme ali centru Safe.si) ali SI-CERT-u.

Če si že kliknil in vpisal podatke:

1. Takoj zamenjaj geslo, če si ga vpisal.
2. Če si vpisal podatke kartice, kontaktiraj banko.
3. Odjavi neznane naprave iz računa.
4. Vklopi MFA.
5. Shrani dokaze.
6. Če je nastala škoda, razmisli o prijavi policiji.

MIT: "Če sporočilo pride od prijatelja, je varno."

RESNICA: V prijateljev račun je lahko nekdo vdrl (ali pa je bil ta zlorabljen). Če ti prijatelj pošlje sumljivo povezavo, ga pokliči ali mu piši prek druge aplikacije in preveri, ali jo je res poslal on.

POMNI: Banka, fakulteta ali platforma te nikoli ne bi smela prositi, da pošlješ geslo ali MFA kodo prek sporočila.

6.3 Spletni nakupi

Spletni nakupi so priročni, vendar lahko hitro naletiš na lažne trgovine, ponarejene izdelke ali krajo plačilnih podatkov.

PRIMER:

Na družbenem omrežju vidiš oglas za zelo poceni telefon. Stran izgleda profesionalno, vendar nima jasnih podatkov o podjetju, pogojev vračila ali varnega načina plačila.

Red flags pri spletni trgovini

Bodi pozoren, če:

- je cena predobro, da bi bila resnična,
- ni podatkov o prodajalcu,
- ni pogojev vračila,
- je domena sumljiva ali nova,
- zahtevajo plačilo na osebni račun,
- ni varnih načinov plačila,
- so ocene sumljive ali preveč popolne,
- stran zahteva nepotrebne podatke.

Kateri podatki so pomembni?

Pri nakupu so običajno potrebni ime, naslov za dostavo, kontakt in plačilni podatki. Ni pa vedno smiselno, da trgovina zahteva datum rojstva, kopijo dokumenta, dostop do kontaktov ali druge nepotrebne podatke.

MIT: "Če trgovina zahteva veliko podatkov, je verjetno bolj zanesljiva."

RESNICA: Zanesljiva trgovina zbira samo podatke, ki jih potrebuje. Preveč zahtev je lahko red flag.

Kaj naredim pred nakupom?

1. Preveri podatke o podjetju.
2. Preveri pogoje vračila in dostave.
3. Poišči neodvisne ocene.
4. Ne plačuj prek sumljivih povezav.
5. Uporabi varne načine plačila.
6. Ne pošiljaj kopije dokumenta brez jasnega razloga.
7. Shrani potrdilo o nakupu.

Če si bil prevaran:

1. takoj kontaktiraj banko,
2. shrani dokaze,
3. prijavi trgovino platformi ali oglasnemu sistemu,
4. pri finančni škodi razmisli o prijavi policiji,
5. pri sumu kibernetске prevare se lahko obrneš tudi na SI-CERT.

POMNI: Pri spletnih nakupih ne varuješ samo denarja, ampak tudi svoje osebne in plačilne podatke.

6.4 Univerza in študijsko okolje

Tudi fakultete, univerze in izobraževalne platforme obdelujejo osebne podatke: tvoje ime, študentski e-mail, ocene, prijave na izpite, prisotnost, naloge, komunikacijo in včasih tudi podatke o uporabi spletnih učilnic.

PRIMER:

V študijskem sistemu opaziš napačen podatek o opravljenem izpitu ali napačen e-mail. Zaradi tega ne prejmeš pomembnega obvestila.

Katere pravice so pomembne?

V študijskem okolju so posebej pomembne:

- pravica do dostopa do svojih podatkov,
- pravica do popravka napačnih podatkov,
- pravica do informacij o obdelavi,
- varnost uporabniških računov,
- varovanje zasebnosti pri objavi ocen ali seznamov.

PAZI! Podatki o študiju niso “nepomembni”. Napačen podatek lahko vpliva na izpite, štipendijo, status, napredovanje ali komunikacijo.

Kaj naredim?

1. Preveri, kateri podatek je napačen.
2. Shrani dokaz ali naredi screenshot.
3. Obrni se na referat, profesorja, administratorja sistema ali drugo pristojno osebo.
4. Zahtevaj popravek podatka.
5. Če gre za resnejšo težavo z osebnimi podatki, preveri, ali ima institucija pooblaščen osebo za varstvo podatkov.
6. Če težava ni rešena, lahko preveriš možnosti pri IP-RS.

MIT: “Ker gre za univerzo, se z mojimi podatki zagotovo ravna pravilno.”

RESNICA: Tudi javne in izobraževalne institucije lahko naredijo napake. Zato imaš pravico preveriti in zahtevati popravek.

POMNI: Pri študijskih računih uporablaj močno geslo in MFA, če je mogoče. Vdor v študijski račun lahko pomeni dostop do tvojih ocen, dokumentov in komunikacije.

6.5 Javne e-storitve

Javne e-storitve uporabljamo za dostop do uradnih podatkov, obrazcev, vlog in storitev države ali občine. Ker gre pogosto za občutljive ali pomembne podatke, moraš biti posebej previden.

PRIMER:

Prejmeš e-mail, ki izgleda kot obvestilo državnega portala. V njem piše, da moraš takoj potrditi identiteto prek povezave. Stran zahteva tvoje prijavne podatke.

Kaj je tveganje?

Pri javnih e-storitvah so ogroženi:

- tvoji uradni podatki,
- identiteta,
- dokumenti,
- davčni ali socialni podatki,
- dostop do uradnih postopkov.

Kaj naredim?

1. Uradne portale odpiraj ročno, ne prek sumljivih povezav.
2. Preveri spletni naslov.
3. Nikoli ne pošiljaj gesel ali kod po e-mailu ali sporočilu.
4. Uporabljalj močno zaščito računa.
5. Po uporabi se odjavi, posebej na javnih računalnikih.
6. Če sumiš zlorabo, takoj ukrepaj in se obrni na pristojno podporo.

MIT: "Phishing se dogaja samo pri bankah in spletnih trgovinah."

RESNICA: Napadalci lahko posnemajo tudi javne portale, univerze, dostavne službe ali zdravstvene storitve.

POMNI: Uradne e-storitve pogosto vsebujejo več občutljivih podatkov kot družbena omrežja. Z njimi ravnaj posebej previdno.

6.6 AI orodja in chatbot-i

AI orodja so uporabna za učenje, prevajanje, pisanje osnutkov, povzemanje in iskanje idej. Toda tudi pri njih moraš razmišljati o podatkih.

PRIMER:

Chatbotu pošlješ pogodbo, zdravniški izvid, osebni dokument ali zasebno sporočilo, ker želiš razlago. Kasneje se vprašaš, ali si pravkar delil preveč.

Česa ne pošiljam AI orodjem?

Brez dobrega razloga ne pošiljaj:

- gesel,
- MFA kod,
- kopij osebnih dokumentov,
- bančnih podatkov,
- zdravstvenih podatkov,
- intimnih fotografij,
- zaupnih dokumentov,
- osebnih podatkov drugih ljudi,
- študijskih ali delovnih dokumentov, ki niso tvoji za deljenje.

Kaj preverim?

1. Ali orodje shranjuje pogovore?
2. Ali lahko izklopim zgodovino ali uporabo podatkov za izboljšave?
3. Ali pošiljam podatke o sebi ali tudi o drugih?
4. Ali je dokument zaupen?
5. Ali bi bilo varneje vprašanje zastaviti brez imen in osebnih podatkov?

MIT: "Če govorim z AI, je to kot zaseben pogovor."

RESNICA: Ni nujno. Odvisno je od orodja, nastavitev in pogojev uporabe. Zato ne vnašaj občutljivih podatkov, če ni jasno, kako bodo obdelani.

POMNI: AI je lahko pomočnik, ni pa sef za tvoje osebne podatke.

7. KAJ NAREDIM, KO GRE KAJ NAROBE?

Ko se zgodi težava, je najpomembneje, da ne reagiraš prenagljeno. Ukrepaj hitro, ampak premišljeno.

1. Prepreči nadaljnjo škodo

Če gre za vdor, spremeni geslo. Če gre za kartico, kontaktiraj banko. Če gre za objavo, ne čakaj predolgo s prijavo. Če gre za izsiljevanje, ne pošiljaj dodatnih vsebin in ne plačuj brez posveta.

2. Shrani dokaze

Preden brišeš, blokiraš ali prijavljaš, shrani:

- screenshot,
- povezavo,
- datum in uro,
- ime profila,
- sporočila,
- e-maile,
- obvestila platforme,
- potrdila o plačilu.

PAZI! Če takoj izbrišeš vse, boš kasneje težje dokazal, kaj se je zgodilo.

3. Uporabi možnosti v storitvi

Večina platform ima možnosti:

- report/prijava,
- block/blokiraj,
- appeal/pritožba,
- account recovery/obnova računa,
- privacy request/zahteva glede podatkov.

4. Uveljavi svojo pravico

Če gre za osebne podatke, lahko organizaciji pišeš in zahtevaš na primer dostop, popravek, izbris, preklic privolitve ali ugovor neposrednemu trženju.

Piši jasno:

“Prosim za informacijo, katere moje osebne podatke obdelujete in za kakšen namen.”

“Zahtevam popravek napačnega podatka.”

“Preklicujem privolitev za prejemanje marketinških sporočil.”

“Ugovarjam obdelavi mojih podatkov za neposredno trženje.”

5. Obrni se na pravi naslov

Če platforma ali organizacija ne odgovori, če gre za kibernetiski incident, prevaro, grožnje ali zlorabo podatkov, poišči ustrezno pomoč.

MIT: “Če prijavim težavo, se tako ali tako ne bo nič zgodilo.”

RESNICA: Včasih rešitev ni takojšnja, vendar brez prijave pogosto ni nobene sledi, nobene pritožbe in nobene možnosti ukrepanja.

8. KAM PO POMOČ?

Ni vsaka težava za isti naslov. Pomembno je, da veš, kam se obrniti.

SITUACIJA	KAM NAPREJ?	ZAKAJ?
Nekdo ima moje osebne podatke in ne vem zakaj	organizacija ali podjetje	najprej zahtevaš informacije
Podjetje ne odgovori na zahtevo glede podatkov	IP-RS	nadzor nad varstvom osebnih podatkov
Vdor v račun, phishing, zlonamerna povezava	platforma, SI-CERT	kibernetski incident
Spletna prevara s finančno škodo	banka, policija, SI-CERT	zaščita denarja in prijava
Grožnje, izsiljevanje, intimne vsebine	policija, zaupanja vredna oseba, pomoč uporabnikom	lahko gre za resno kršitev
Težave na družbenem omrežju	platforma, Safe.si	prijava vsebine, nasveti
Napačni podatki v študijskem sistemu	referat, skrbnik sistema, DPO	popravek podatkov
Sum zlorabe osebnih podatkov	organizacija, IP-RS	varstvo osebnih podatkov

Koristni viri v Sloveniji

- Informacijski pooblaščenec Republike Slovenije / IP-RS — za vprašanja varstva osebnih podatkov.
- SI-CERT — nacionalni odzivni center za kibernetsko varnost.
- Safe.si — nasveti o varni rabi interneta, posebej za mlade, starše in učitelje.
- Policija — pri grožnjah, izsiljevanju, prevarah, kraji identitete ali drugi hujši zlorabi.
- Banka — če so ogroženi plačilni podatki ali denar.
- Platforma ali aplikacija — za prijavo vsebin, lažnih profilov, vdora ali blokade računa.
- Univerza, fakulteta ali DPO — pri težavah s študijskimi podatki.

POMNI: Ni ti treba vsega rešiti sam. Prvi korak je pogosto že to, da nekomu poveš in shraniš dokaze.

9. FAQ

Ali moram vedno sprejeti cookies?

Ne. Nujni cookies so lahko potrebni za delovanje strani, nenujne cookies za oglase ali sledenje pa lahko pogosto zavrneš.

Ali lahko zahtevam izbris vseh svojih podatkov?

Včasih da, vendar ne vedno. Pravica do izbrisa obstaja, a ima izjeme.

Ali lahko prekličem soglasje?

Da, če obdelava temelji na tvoji privolitvi. Preklic praviloma ne sme biti težji kot dajanje privolitve.

Ali lahko podjetje uporablja moje podatke za oglase?

V določenih primerih da, vendar mora imeti ustrezno pravno podlago in ti dati informacije. Pri neposrednem trženju imaš močno pravico do ugovora.

Kaj če sem kliknil phishing povezavo?

Takoj zamenjaj geslo, če si ga vpisal. Če si vpisal kartico, kontaktiraj banko. Shrani dokaze, preveri račun in po potrebi prijavi incident.

Ali je screenshot dokaz?

Lahko je zelo koristen dokaz. Shrani tudi povezavo, datum, uro, ime profila in sporočila.

Ali smem objaviti fotografijo prijatelja?

Ne vedno. Če je oseba prepoznavna, posebej če je fotografija občutljiva ali zasebna, jo najprej vprašaj.

Ali imam pravico uporabljati izmišljeno ime na vsaki platformi?

Ne nujno. To je pogosto odvisno od pravil platforme.

Ali mi platforma lahko blokira račun?

Lahko, če meni, da kršiš njena pravila. Vendar imaš pogosto možnost pritožbe oziroma pregleda odločitve.

Kaj naj ne pošiljam AI chatbotu?

Ne pošiljaj gesel, dokumentov, bančnih podatkov, zdravstvenih podatkov, intimnih fotografij, zaupnih informacij ali osebnih podatkov drugih ljudi brez jasnega razloga.

Kam prijavim vdor v račun?

Najprej uporabi obnovo računa pri platformi. Nato zamenjaj geslo, vklopi MFA in shrani dokaze. Pri resnejšem incidentu se lahko obrneš na SI-CERT, pri kaznivem dejanju pa na policijo.

Kaj če ne vem, kdo je pravi naslov?

Začni pri storitvi ali organizaciji, kjer se je problem zgodil. Če gre za osebne podatke, preveri IP-RS. Če gre za kibernetični incident, SI-CERT. Če gre za grožnje ali finančno škodo, policijo oziroma banko.

10. CHECKLIST

Preden kliknem povezavo

- ✓ Preverim pošiljatelja.
- ✓ Pogledam, kam vodi povezava.
- ✓ Ne vpisujem gesla na strani, odprti iz sumljivega sporočila.
- ✓ Ne pošiljam MFA kod.
- ✓ Če nisem prepričan, odprem uradno stran ročno.

Preden sprejemem cookies ali pogoje

- ✓ Preverim, ali lahko zavrnem nenujne cookies.
- ✓ Pogledam, ali gre za oglase ali profiliranje.
- ✓ Preverim, kdo zbira podatke.
- ✓ Ne kliknem "sprejmi vse" samo zato, ker je najhitreje.

Preden objavim

- ✓ Vprašam se, kdo bo to videl.
- ✓ Ne objavim tuje fotografije brez premisleka.
- ✓ Ne objavljam lokacije v realnem času, če ni potrebno.
- ✓ Ne delim dokumentov, kartic ali osebnih podatkov.

Preden pošljem podatke

- ✓ Vem, komu jih pošiljam.
- ✓ Vem, zakaj jih potrebuje.
- ✓ Pošiljam samo tisto, kar je nujno.
- ✓ Ne pošiljam gesel, kod ali občutljivih podatkov prek sporočil.

Če gre kaj narobe

- ✓ Prepreči nadaljnjo škodo.
- ✓ Shrani dokaze.
- ✓ Zamenjam geslo ali blokiram kartico, če je potrebno.
- ✓ Prijavim objavo, profil ali incident.
- ✓ Obrnem se na pravi naslov.
- ✓ Ne ostanem sam s težavo.

11. ZAKLJUČEK

Digitalne pravice niso nekaj, kar obstaja samo v zakonih. Pomembne so takrat, ko klikneš povezavo, objaviš fotografijo, sprejmeš cookies, naročiš izdelek, uporabljaš študijski portal, pišeš chatbotu ali se prijaviš v svoj račun.

Ni treba, da znaš vse pravne izraze. Pomembno je, da znaš prepoznati tveganje, postaviti pravo vprašanje in narediti prvi korak.

Najpomembnejše pravilo:

Če ne razumeš, preveri.

Če je nekaj sumljivo, ne klikaj.

Če je nekaj narobe, shrani dokaze in ukrepaj.

Če ne zmoreš sam, poišči pomoč.