REPUBLIKA SLOVENIJA
INFORMACIJSKI POOBLAŠČENEC
Dunajska cesta 22, 1000 Ljubljana
T: 01 230 9730
www.ip-rs.si
gp.ip@ip-rs.si

Izdajatelj: Republika Slovenija
Podpisnik: Alenka Jerše
Potek veljavnosti: 01.12.2026
Ref. št. dokumenta: 07122-1/2026/21
Čas podpisa: 18:48, 22.06.2026
Št. cert: da c2 2f 18 00 00 00 00 56 7d ba 19

Številka: 007-24/2026/2
Datum: 22. 6. 2026

Ministrstvo za okolje, podnebje in energijo
gp.mope@gov.si

Zadeva: Predlog Zakona o spremembah in dopolnitvah Zakona o varstvu okolja (ZVO-2) ter ocena učinka varstva osebnih podatkov – mnenje IP

Zveza: Vaš dopis z dne 23. 5. 2025

Spoštovani,

prejeli smo vaš dopis, s katerim ste nam v mnenje posredovali predlog Zakona o spremembah in dopolnitvah Zakona o varstvu okolja (ZVO-2) ter oceno učinkov v zvezi z varstvom osebnih podatkov pri pripravi Zakona o spremembah in dopolnitvah Zakona o varstvu okolja (ZVO-2).

* * *

1. Uvodoma

Informacijski pooblaščenec (v nadaljevanju: IP) pojasnjuje, da je po določbi prvega odstavka 35. člena 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 razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov; v nadaljevanju: Splošna uredba) ocena učinka v zvezi z varstvom osebnih podatkov (v nadaljevanju: ocena učinka) potrebna, kadar „je možno, da bi [dejanje obdelave] lahko povzročil[o] veliko tveganje za pravice in svoboščine posameznikov“. Upravljavec podatkov mora nato oceniti tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, in opredeliti ukrepe, predvidene za zmanjšanje navedenih tveganj na sprejemljivo raven, ter dokazati skladnost s Splošno uredbo (sedmi odstavek 35. člena). Skladno s priporočili Evropskega odbora za varstvo podatkov (v nadaljevanju: EDPB), kot so navedena v smernicah o ocenah učinka[1] velja, da če je upravljavec podatkov štel, da so tveganja zadosti zmanjšana, se lahko glede na razlago prvega odstavka 36. člena Splošne uredbe ter uvodnih izjav (84) in (94) obdelava nadaljuje brez posvetovanja z nadzornim organom. IP pojasnjuje, da je po določbi drugega odstavka 36. člena Splošne uredbe nadzorni organ v roku do osmih tednov po prejemu zahteve za posvetovanje pisno svetuje upravljavcu, kadar je ustrezno, pa tudi obdelovalcu, in lahko uporabi katero koli pooblastilo iz člena 58. To obdobje se lahko ob upoštevanju kompleksnosti predvidene obdelave podaljša za nadaljnjih šest tednov. Zakon o varstvu osebnih podatkov (Uradni list RS, št. 163/22, 40/25 – ZInfV-1 in 10/26 – ZP-1L; v nadaljevanju: ZVOP-2) v tretjem odstavku 24. člena določa, da kadar se z zakonom določa obdelava osebnih podatkov, za katero je treba izdelati oceno učinka, predlagatelj predlogu zakona priloži oceno učinka v skladu s 35. členom Splošne uredbe. Po proučitvi ocene učinka nadzorni organ poda mnenje glede

[1] Smernice glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je „verjetno, da bi [obdelava] povzročila veliko tveganje“, za namene Uredbe (EU) 2016/679, 17/SL, DS 248 rev.01; dostopno na: https://www.ip-rs.si/fileadmin/user_upload/Pdf/Mednarodno_delovanje/wp248_rev.01_sl.pdf.

obdelave osebnih podatkov, glede katerega se mora predlagatelj zakona opredeliti. Kadar ocene učinka ni treba izdelati, predlagatelj zakona opravi samo predhodno posvetovanje z nadzornim organom v skladu s 36. členom Splošne uredbe.

* * *

Na podlagi informacij, ki ste nam jih posredovali, vam v nadaljevanju na podlagi 3. točke 55. člena, točke (a) tretjega odstavka 58. člena ZVOP-2, v povezavi s 35. in 36. členom Splošne uredbe ter 2. členom Zakona o informacijskem pooblaščencu (ZInfP; Uradni list RS, št. 113/05, 51/07 – ZUstS-A) posredujemo naše neobvezno mnenje v zvezi s predlogom Zakona o spremembah in dopolnitvah Zakona o varstvu okolja in s predlogom povezano predloženo oceno učinka.

* * *

2. Pregled ocene učinka

2.1 Splošne ugotovitve

IP ugotavlja, da ste predložili zakonodajno oceno učinka, ki **temelji na prilagojeni metodologiji za pripravo zakonodajnih ocen učinka** v zvezi varstvom osebnih podatkov za učinkovito izvajanje 24. člena ZVOP-2. Razlike med t. i. zakonodajnimi in projektnimi ocenami učinka glede varstva osebnih podatkov smo pojasnili na posebni podstrani o ocenah učinka, ki je dostopna na:

https://www.ip-rs.si/varstvo-osebnih-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/ocena-u%C4%8Dinka-v-zvezi-z-varstvom-podatkov/

Namen zakonodajnih ocen učinka je, da se še pred oblikovanjem dokončnega besedila členov opravi pravočasne razmisleke o tem, kako ustrezno upoštevati temeljna načela varstva osebnih podatkov pri določanju besedila zakona. Te razmisleke (npr. kakšne namene zasledujemo, kateri nabor osebnih podatkov je potreben, kakšne varovalke moramo vključiti v zakon, ali bo šlo za povezovanje zbirk podatkov, določitev rokov hrambe ipd.) se opiše v oceni učinkov, jo pošlje IP v mnenje (t. i. predhodno posvetovanje) ter na podlagi izdanega mnenja IP, oblikuje (bolj) dokončno besedilo členov, ki gre lahko nato v medresorsko usklajevanje. Idealno je torej izdelava ocene učinka pred-faza pred dokončnim oblikovanjem členov, včasih pa razumljivo zaradi nujnosti to poteka vzporedno s samim oblikovanjem zakonske ureditve. Proces priprave zakonodajnih ocen učinka in umeščenost teh smo pojasnili tudi v pregledni infografiki, ki je dostopna na:

https://www.ip-rs.si/fileadmin/user_upload/Pdf/infografike/infografika%20-%20DPIA.pdf.

2.2 Formalni pregled celovitosti ocene učinka

Izhodiščno je IP predloženo oceno učinka pregledal z vidika njene celovitosti smiselno skladno s sedmim odstavkom 35. člena Splošne uredbe. **Ugotavljamo, da ocena učinka ne sledi metodologiji, ki jo je za pripravo zakonodajnih ocen učinka pripravil IP,[2] kar priporočamo zaradi celovitosti in kakovosti ocene učinka.**

Iz predložene ocene učinka je razvidno, da je bila posredovana v pregled pooblaščeni osebi za varstvo osebnih podatkov na ministrstvu. **V bodoče priporočamo, da mnenje pooblaščene osebe priložite oceni učinka.**

Posebnih pripomb glede formalne celovitosti ocene učinka nimamo.

[2] https://www.ip-rs.si/fileadmin/user_upload/RAZNO/Metodologija%20zakonodajne%20ocene%20u%C4%8Dinkov_jul202.docx.

2.3 Vsebinski pregled ocene učinka

Kot smo že poudarili, je namen zakonodajnih ocen učinka, da se še pred oblikovanjem dokončnega besedila členov opravi pravočasne razmisleke o tem, kako ustrezno upoštevati temeljna načela varstva osebnih podatkov pri določanju besedila zakona. Idealno je izdelava ocene učinka neke vrste pred-faza pred dokončnim oblikovanjem členov, včasih pa razumljivo zaradi nujnosti to poteka vzporedno s samim oblikovanjem zakonske ureditve. **Priporočamo, da se pri izdelavi zakonodajnih ocen učinka sledi metodologiji IP**, ki je na voljo na povezavi:

https://www.ip-rs.si/fileadmin/user_upload/RAZNO/Metodologija%20zakonodajne%20ocene%20u%C4%8Dinkov_jul202.docx.

Določitev odgovornih oseb

V točki »1.4 Določitev odgovornih oseb« sta kot upravljavca osebnih podatkov predvidena ministrstvo, pristojno za okolje za informacijski rešitvi Dovoljenja (predlagani 17.b člen) in ePresoje (predlagani 90.a člen) ter Agencija Republike Slovenije za okolje (ARSO) za informacijsko rešitev Monitoring (predlagani 150.a člen). Nadalje ste navedli, da so obdelovalci osebnih podatkov v zvezi z navedenimi informacijskimi rešitvami ministrstvo, pristojno za digitalno preobrazbo (skupne informacijske rešitve, državni oblak), pogodbeni izvajalci razvoja informacijskih rešitev in drugi organi, ki bodo na podlagi predloga zakona dostopali do podatkov.

IP na tem mestu poudarja, da mora iz predpisa nedvoumno izhajati, kdo je upravljavec določene zbirke podatkov oz. glede katerih zbirk bo šlo morebiti celo za skupno upravljanje (26. člen Splošne uredbe) in kdo je obdelovalec. Na posamezno vlogo (upravljavec, obdelovalec, skupni upravljavec) se namreč vežejo obveznosti, določene v Splošni uredbi oz. ZVOP-2. Zato morajo biti v predpisu jasno opredeljene različne vloge posameznih deležnikov, ki so vključeni v postopke zbiranja in obdelave, zlasti v primeru skupnega upravljanja. V primeru skupnih upravljavcev je treba določiti, kdo je odgovoren za zagotavljanje točnosti in ažurnosti podatkov in kdo lahko izvaja popravke v primeru ugotovljenih nepravilnosti. Iz zakona mora prav tako jasno izhajati kdo od morebitnih skupnih upravljavcev je pristojen za izbris. Ključni varnostni ukrepi in morebitna delitev odgovornosti zanje med skupnimi upravljavci bi morali biti opredeljeni v predpisu, podrobnosti pa lahko določajo podzakonski akti. Splošna uredba o varstvu podatkov v 13. in 14. členu tako določa, katere so informacije, ki jih mora upravljavec zagotoviti posameznikom, odvisno od tega, ali so bili osebni podatki pridobljeni s strani posameznika ali iz drugega vira. Informacije morajo biti podane v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku. V primeru skupnega upravljavstva je treba določiti, kdo je odgovoren za podajo teh informacij.

Tako npr. iz predlaganega 150.a člena ni razvidno, da je kot upravljavec predmetne zbirke (Monitoring) predviden ARSO. Iz predlagane določbe celo izhaja, da mora povzročitelj obremenitve podatke obratovalnega monitoringa sporočati ministrstvu (in ne npr. ARSO).

Prav tako iz predlaganih določb ni razvidno katere vrste obdelave naj bi izvajalo ministrstvo, pristojno za digitalno preobrazbo in v okviru katerega informacijskega sistema, niti ni razvidno, v katerem delu obdelave je predvideno, da bo le ta potekala v okviru skupnih informacijskih rešitev in katere so te informacijske rešitve. V tem delu še posebej opozarjamo, da gre lahko pri obdelavi v okviru skupnih informacijskih rešitev za skupno upravljanje, v okviru katerega je treba vloge skupnih upravljavcev in razdelitev obveznosti, ki izhajajo iz konkretne razdelitve vlog, natančno opredeliti.

Na tem mestu še opozarjamo na napačno opredelitev kot pogodbenega obdelovalca organe, ki bodo na podlagi predloga zakona dostopali do podatkov (ministrstvo, pristojno za gradnjo, inšpekcija, pristojna za varstvo okolja itd.). Navedeni organi bodo v okviru predvidene obdelave (najverjetneje)

nastopali kot samostojni upravljavci, pri čemer morajo tudi ti organi razpolagati z ustrezno pravno podlago (zakon).

Povezovanje evidenc

V predmetni oceni učinka je v točki »2.2 Načini in sredstva obdelave« navedeno, da bo *»[P]ovezovanje […] potekalo na podlagi matičnih, davčnih ali parcelnih številk (odvisno od posameznega informacijskega sistema in posameznega povezanega registra oziroma evidence)«*, ni pa podana konkretna opredelitev zgoraj navedenih zahtev v zvezi z novimi členi 17.b, 90.a in 150.a.

87. člen ZVOP-2 natančno opredeljuje vrste uradnih evidenc ali javnih knjig in pogoje, pod katerimi se lahko povezujejo – taksativno navedene se lahko povezujejo med seboj ali z drugimi zbirkami samo, če taka povezovanja izrecno določa zakon.

Glede povezovanja zato pojasnjujemo, da je bistveni del zakonodajne ocene učinka, da se preveri, ali so vsa predvidena povezovanja utemeljena in da so tudi ustrezno zapisana v samem besedilu zakona (**načelo zakonitosti**).

Kot smo opozorili tudi v mnenju na predlog zakona (št. 007-56/2025/3) je v primeru povezovanja uradnih evidenc ali javnih knjig glede na ustaljeno prakso **v zakonu predvsem potrebno določiti**:

- povezovalni znak,
- namen povezovanja,
- upravljavca (-e) povezanih evidenc ter
- katere podatke se iz povezane (-ih) zbirk pridobi.

Ocena učinka mora ovrednotiti, ali so oziroma ali bodo v predlaganih določbah te zahteve upoštevane.

V zvezi s tem predlagamo, da se ocena učinka ustrezno posodobi na način, da bodo upoštevane vse navedene zahteve glede presoje učinka povezovanja evidenc na varstvo osebnih podatkov.

Nabor podatkov

V točki »2.1 Nabor podatkov in informacije o sorazmernosti« so pri presoji nabora podatkov v zvezi s členoma 17.b in 90.a kot skupina navedeni *»podatki o uporabniških vlogah«*, ki pa v oceni učinka in v predlaganih določbah niso podrobneje opredeljeni.

Skladno z načelom omejitve namena obdelave osebnih podatkov se smejo zbirati in drugače obdelovati samo tisti osebni podatki, ki so nujni za doseganje vnaprej opredeljenih zakonitih namenov. Kolikor je cilje mogoče doseči brez obdelave osebnih podatkov (npr. z anonimnimi podatki), je treba predvideti takšno rešitev. Posebej je treba biti pri tem pozoren na razlikovanje med psevdonimiziranimi podatki, ki so še vedno v celoti varovani osebni podatki (četudi to morda na prvi pogled ni videti tako), in anonimnimi podatki. Poleg samega obsega podatkov se sorazmernost nanaša tudi na uporabo manj občutljivih podatkov od tistih, katerih narava oziroma zloraba ima večjo težo (psevdonimi so boljši kot navadni podatki, govoreče šifre so slabše od naključnih nizov ipd.). Upošteva se pravilo, da se zbira osebne podatke tistih oseb, od katerih so potrebni, takrat, ko so potrebni in v obsegu, ki je potreben in ne obratno – nesorazmerno bi bilo zbiranje vseh podatkov, vseh oseb, vnaprej in na zalogo.

Opisano presojo je mogoče opraviti le, če so v oceni učinka in ustrezno in na konkreten način opredeljeni vsi potrebni podatki, natančna opredelitev podatkov pa mora biti prelita tudi v zakonsko določbo. V zvezi s tem predlagamo ustrezno posodobitev ocene učinka.

Rok hrambe

Predlog zakona določa, da se podatki, ki se obdelujejo v informacijskih rešitvah, hranijo pet let po izteku koledarskega leta, v katerem se je uporabnik zadnjič prijavil v informacijski sistem.

Znotraj presoje spoštovanja načela omejitve shranjevanja je treba oceniti, kateri je najkrajši možni rok, ki omogoča doseganje zastavljenih ciljev. Roki hrambe morajo biti opredeljeni dovolj določno (ne npr. „dokler je to potrebno“ ali „trajno“ – če to ni posebej utemeljeno in izjemoma). Ko natančnega roka ni mogoče določiti, se opredeli kriterije, ki na to vplivajo (npr. do preklica privolitve, x let po prenehanju obveznosti ipd.). Po dosegu namena oziroma po preteku zakonsko ali drugače določenega roka je treba osebne podatke izbrisati, uničiti ali anonimizirati.

Pri presoji, ali je upoštevano načelo zakonitosti obdelave osebnih podatkov, mora tudi biti podana opredelitev roka hrambe. V zvezi s tem predlagamo, da se v oceni učinka opravi presoja argumentov, zakaj je bil kot najprimernejši izbran predlagani rok petih let.

Načini in sredstva obdelave

V točki »2.2 Načini in sredstva obdelave« ste navedli, da bodo do informacijskih rešitev uporabniki dostopali z osrednjega spletnega mesta državne uprave. Sledil bo vpis v varnostno shemo, ki omogoča prijavo oziroma registracijo uporabnika, pri čemer bodo uporabniške pravice nivojsko urejene. Registracijo uporabnikov bodo upravljali skrbniki ministrstva, po potrditvi registracije pa bo informacijski sistem uporabnika avtomatsko preusmeril na obrazec, ki bo omogočal prijavo v informacijsko rešitev, ki bo mogoča s sredstvom elektronske identifikacije. V nadaljevanju ste še navedli, da se bo obdelava izvajala ob registraciji uporabnika, ob prijavi v informacijsko rešitev, ob vlaganju vlog, ob vodenju postopkov in ob sporočanju podatkov obratovalnega monitoringa, pri čemer se bodo podatki obdelovali v informacijskih rešitvah, v državnem računalniškem oblaku in v registrih oziroma evidencah, s katerimi se bodo informacijski sistemi povezovali.

IP na tem mestu poudarja, da bi morala ocena učinka vse postopke ter sredstva obdelave natančno razdelati, v zvezi s posameznim postopkom obdelave natančno opredeliti vrste osebnih podatkov, ki se bodo v tem postopku obdelovali ter natančno opredeliti informacijsko rešitev, v kateri se bo postopek obdelave izvajal. Tako bi bilo treba npr. razdelati postopek registracije uporabnika, vrsta obdelave, ki se v teh postopku izvaja (npr. identifikacija uporabnika), v kateri informacijski rešitvi se izvaja in kdo je za to obdelavo zadolžen. Od postopka registracije uporabnika bi bilo npr. treba nadalje ločiti postopek prijave uporabnika v informacijsko rešitev, ki naj bi se izvajala na podlagi sredstva elektronske identifikacije in kjer postopek avtentikacije poteka v SI-PASS itd.

Tako razdelane posamezne postopki obdelave in z njimi povezane vrste osebnih podatkov, informacijske rešitve in odgovorne osebe, bi bilo treba ustrezno preliti v zakonske določbe.

Ocena tveganj

IP pozdravlja opravljeno oceno tveganj, ki vključuje oceno resnosti in verjetnosti tveganj ter izračun skupne ravni tveganja, vendar hkrati opozarja, da so določena tveganja v oceni učinka opredeljena premalo podrobno. V zvezi s tem IP priporoča, da si pri oceni tveganj pomagate z infografiko o učinkovitem obvladovanju tveganj na področju varstva osebnih podatkov, ki je na voljo na spodnji povezavi:

https://www.ip-rs.si/fileadmin/user_upload/Pdf/infografike/U%C4%8Dinkovito%20obvladovanje%20tveganj%20na%20podro%C4%8Dju%20varstva%20osebnih%20podatkov.pdf

V oceni tveganj so mestoma napačno navedena tveganja namesto temeljnih načel (npr. načelo odgovornosti, načelo zaupnosti in celovitosti), ki bi morala biti ovrednotena iz vidika tveganj. Takšni primeri so v predloženi oceni učinka (Priloga 1: Tveganja in ukrepi za njihovo obvladovanje v povezavi z varnostjo podatkov) denimo v:

- točki 5: Nepooblaščen dostop do osebnih podatkov,
- točki 6: Prekomerna obdelava osebnih podatkov,
- točki 7: Predolga hramba podatkov,
- točki 10: Nedovoljena povezovanja zbirk,

- točki 11: Izguba podatkov,
- točki 12: Nezadostna informiranost posameznikov,
- točki 14: Kršitev varnosti podatkov.

Na nekaterih mestih se prav tako večkrat ponavljajo ista načela, ki so nato opredeljena z različnimi tveganji. Takšen primer je npr. načelo zakonitosti, ki se z vidika več različnih tveganj pojavi pri ocenah v točkah 1., 2. in 4. Predlagamo, da naj bodo tveganja, ki so povezana z določenim temeljnim načelom, zaradi večje preglednosti opredeljena na enem mestu.

Prav tako bi moral biti natančneje opredeljen vir tveganja oziroma druge konkretne okoliščine tveganja. Takšni primeri so v predloženi oceni učinka denimo v točkah 1, 13 in 14. V točki 13 bi bilo denimo priporočljivo konkretizirati, kaj bi pomenila izguba ali zloraba SI-PASS prijavnih podatkov, tj. kako bi lahko ogrozila varnost podatkov, do katerih se preko tega sistema dostopa. V oceni učinka bi bilo prav tako priporočljivo podrobneje opisati postopek uporabe SI-PASS (npr. ali bo zahtevana uporaba SI-GOV certifikatov na pametnih karticah ali tudi SI-GEN).

Slabo opredeljena tveganja lahko namreč vodijo v spregled dejanskih tveganj in v neustrezno oblikovanje ukrepov za njihovo obvladovanje. Ustrezno opredeljena tveganja v povezavi z osebnimi podatki so:

- **konkretna** (iz opredelitve tveganja mora biti jasno razvidno, kdo ali kaj je vir tveganja oziroma je kontekst tveganja dovolj natančno opredeljen, da je jasno, na kaj točno se nanaša posamezno tveganje; »zloraba podatkov« je primer premalo konkretiziranega tveganja);

- **granularna** (preveč široko opredeljena tveganja ovirajo dovolj podrobno obravnavo in opredelitev ustreznih ublažitvenih ukrepov; nepooblaščen dostop do podatkov se denimo lahko nanaša na nepooblaščen dostop pooblaščenih uporabnikov, na nepooblaščen dostop oseb pri pogodbenih obdelovalcih, na nepooblaščen dostop pri uporabnikih ali na nepooblaščen oseb tretjih oseb, vsakega od teh pa lahko naslavljajo različni ukrepi za ublažitev tveganj);

- **realna** (pri identifikaciji tveganj je pomembno, da se njihov nabor zastavi sicer široko, npr. z aktivnostjo viharjenja možganov (angl. *brainstorming*), tako da se v prvi fazi ugotovijo vsa možna tveganja, izločijo pa tveganja, ki to dejansko niso (npr. »posamezniki bodo imeli vprašanja glede obdelave osebnih podatkov«), saj obravnava tveganj, ki to dejansko niso ne prispeva k ustreznemu obvladovanju tveganj in kvečjemu umetno in nepotrebno razširja nabor tveganj ter zmanjšuje preglednost in posledično učinkovitost same ocene učinka);

- **ustrezna načelom** (tveganja morajo biti primerno strukturirana glede na temeljna načela varstva osebnih podatkov po 5. členu Splošne uredbe, kar omogoča njihovo celovito obravnavo in spregled določenih načel oziroma zahtev).

3. Zaključno

IP zaključno ugotavlja, da je predložena ocena učinka glede varstva osebnih podatkov v povezavi s predlogom novele ZVO-2 načeloma ustrezno pripravljena, v mnenju pa smo podali nekaj priporočil, za katere priporočamo, da jih upoštevate in ki so lahko koristna tudi pri bodočih zakonodajnih ocenah učinka. Predvsem priporočamo, da se v ocenah učinka več pozornosti nameni bolj natančni in kakovostni opredelitvi in analizi tveganj, kot smo to pojasnili v zadnji točki mnenja.

Izvedba navedenih priporočil za izboljšave pri pripravi oceno učinka v zvezi z varstvom osebnih podatkov, katerih je predvidena s spremembami in dopolnitvami ZVO-2, vam bo v pomoč pri pripravi bolj jasnih, natančnih in preglednih določb predloga ZVO-2.

S spoštovanjem,

dr. Jelena Virant Burnik,

informacijska pooblaščenka

Pripravil/a:

Andraž Stariha, mag. prava,

raziskovalec pooblaščenca

mag. Polonca Štrekelj,

državna nadzornica za varstvo osebnih podatkov

Poslati:

- naslovniku (e-pošta).