REPUBLIKA SLOVENIJA

INFORMACIJSKI
POOBLAŠČENEC
Dunajska cesta 22, 1000 Ljubljana
T: 01 230 9730
F: 01 230 9778
gp.ip@ip-rs.si
www.ip-rs.si

Digitalno podpisal Suzana Piškur
DN: c=SI, o=state authorities, ou=web-certificates, givenName=Suzana, sn=Piškur, serialNumber=1237490814012, cn=Suzana Piškur
Datum: 2020.07.10 15:45:51 +02'00'

Številka: 007-25/2020/2
Datum: 9. 7. 2020

Ministrstvo za infrastrukturo
gp.mzi@gov.si

ZADEVA: Mnenje na Zakon o spremembah in dopolnitvah Zakona o cestninjenju
ZVEZA: Vaše sporočilo po e-pošti s prilogami z dne 2. 7. 2020

Spoštovani,

na podlagi vašega zaprosila in 48. člena Zakona o varstvu osebnih podatkov (ZVOP-1) ter 57. 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 (v nadaljevanju - Splošna uredba) vam posredujemo naše neobvezno mnenje v zvezi z osnutkom predloga zakona.

Informacijski pooblaščenec (IP) uvodoma pozdravlja dejstvo, da se predlagatelj zaveda pomembnosti varstva osebnih podatkov in zlasti v povezavi z uvajanjem sprememb na področju cestninjenja osebnih vozil ter pravočasno vključitev IP v strokovno razpravo in razumevanje, da se lahko le ob ustreznem upoštevanju temeljnih človekovih pravic in svoboščin v polni meri izkoristi možnosti, ki jih prinaša digitalizacija.

Splošno

Cestninjenje osebnih vozil se lahko izvaja na različne načine, pri čemer sta različna tudi obseg in intenzivnost obdelave osebnih podatkov in s tem poseg v človekove pravice. V primeru običajnih vinjet v obliki nalepk, ki se nalepijo na vetrobransko steklo in so kupljene na anonimen način, nadzor pa se izvaja z vizualno kontrolo, lahko govorimo o najmanjšem posegu v osebne podatke in o praktično anonimni uporabi. Dokler ni zaznane kršitve uporabnik vozila ni identificiran, njegove lokacije in gibanje se ne beležijo. Klasične vinjete tako praktično ne posegajo v pravice posameznika, seveda pa imajo določene slabosti z vidika nadzora in praktičnosti. Z digitalizacijo se ta raven varstva osebnih podatkov praktično neizogibno zniža – v kolikšni meri, pa je predvsem odvisno od dizajna sistema. E-vinjete ne morejo nuditi takšne ravni varstva osebnih podatkov kot klasične vinjete, kar pa seveda ne pomeni, da ne morejo biti sprejemljive v demokratični družbi – ob tem, da prinašajo določene prednosti tako za uporabnike kot za upravljavce cest, se lahko z ustreznimi varovalkami v zakonodaji bistveno zmanjša njihov poseg v varstvo osebnih podatkov.

Pri tem je nekaj točk ključnih in sicer:

- zbiranje osebnih podatkov ob nakupu e-vinjete ter
- zajem, hramba in druge obdelave osebnih podatkov pri izvajanju cestninskega nadzora.

Toplo pozdravljamo zelo kvalitetno in celovito pripravljeno oceno učinkov na varstvo osebnih podatkov, ki kaže na vloženi trud in stopnjo razumevanja specifike in pomembnosti varstva osebnih podatkov.

Naj točki zaradi jasnosti želimo opozoriti, da je treba na posege v zasebnost gledati celovito in na široko in ne samo skozi »oči« posameznega subjekta (npr. upravljavca cest). Pri ocenjevanju posegov v zasebnost je namreč vedno treba upoštevati, da obstajajo tudi drugi subjekti, s svojimi pooblastili, s svojimi zbirkami osebnih podatkov in je treba upoštevati tudi možnost povezovanja zbirk osebnih podatkov, rekonstrukcije dogodkov in drugih dejanj, ki lahko posredno razkrijejo določene osebne podatke in tako posežejo v pravice posameznika. Tudi če en upravljavec zagotovi vse, kar je v njegovi moči, to še ne pomeni, da ne bo prišlo do posegov v zasebnost posameznikov, saj je treba upoštevati širši kontekst.

Obdelava osebnih podatkov pri nakupu e-vinjete

Pozdravljamo predlog, da se pri nakupu e-vinjete na prodajnem mestu ne zbirajo nobeni osebni podatki razen registrske številke vozila, saj je to skladno z načelom sorazmernosti.

Glede možnosti nakupa e-vinjete prek spleta pa poudarjamo, da bi morala biti raven varstva osebnih podatkov kar se da blizu tistemu, ki je zagotovljena kupcu, ki e-vinjeto kupi na prodajnem mestu. Tu je predvsem pomemben nabor zbranih podatkov o kupcu, ki mora upoštevati načelo minimizacije (člen 5 Splošne uredbe). Navedeno v praksi pomeni, da kupcu ne bi bilo treba navesti nobenega osebnega podatka, ki ni nujno potreben za nakup e-vinjete, pred »surovimi« osebnimi podatki bi morali imeti prednost psevdonimizirani osebni podatki. To v praksi pomeni, da pri nakupu ne sme biti obvezno večje število kontaktnih podatkov kupca (telefonska št. se nam npr. ne zdi potrebna), kakor tudi ne njegovo ime in priimek, koristna je opcija, da kupec lahko navede poljuben e-naslov (npr. da si lahko izbere takšen e-naslov, ki ne razkriva njegove identitete) ter da se za samo izvedbo nakupa ne zahteva nič več, kot pri nakupu drugega blaga ali storitve prek spleta. Ime in priimek posameznika ter podatki o telefonski številki se nam zato ne zdijo potrebni in zato ne sorazmerni.

Opozarjamo na upoštevanje določb 13 člena glede informiranja posameznika o obdelavi osebnih podatkov, kar sicer ni predmet zakona temveč izvedbe. Posameznik mora biti o obdelavi osebnih podatkov ob registraciji ustrezno obveščen – naj jasen in razumljiv način mu je treba predstaviti ključne informacije o obdelavi osebnih podatkov (npr. ob registraciji), ki jih zahteva člen 13 Splošne uredbe (ne glede na vrsto pravne podlage[1]).

[1] v pomoč je lahko vzorčni obrazec, ki je dostopen na: https://www.ip-rs.si/fileadmin/user_upload/doc/vzorci/VZOREC_OBVESTILA_POSAMEZNIKOM_GLEDE_OBDELAVE_OSEBNIH_PODATKOV.docx

Pozornost je treba nameniti tudi na videz manj pomembnim podatkom, ki so vendarle osebni podatki – ob vsakem spletnem nakupu se zabeležijo določeni podatki tudi o sami seji uporabnika (npr. IP naslov, datum in čas itd.) in tudi glede tega je treba upoštevati načelo minimizacije in rok hrambe teh podatkov prilagoditi na minimalno nujno potreben, nato pa te podatke brisati ali anonimizirati.

Obdelava osebnih podatkov pri izvajanju cestninskega nadzora

Kot pri ostalih obdelavah osebnih podatkov je ustrezno izvedena minimizacija obdelave osebnih podatkov glede na zasledovane namene ena najmočnejših varovalk za osebne podatke – podatkov, ki jih ni, enostavno ni mogoče zlorabiti in z minimizacijo rokov hrambe bistveno zmanjšamo tudi vsa ostala tveganja.

Izvajanje cestninskega nadzora je točka, ki je ključna za stopnjo posega v zasebnost in varstvo osebnih podatkov pri vseh oblikah elektronskega cestninjenja, saj se pri nadzoru obdelujejo podatki o lokaciji vozila oziroma posameznikov v dejanskem času. V prvi vrsti je seveda pomembno, kot smo že izpostavili, da se osebnim vozilom ne sledi izven zasledovanega namena (cestninskega nadzora), da se ne ugotavlja njihove lokacije ali beleži prevoženih poti.

V drugi vrsti, kot smo že poudarili, morata biti upoštevani premisi:

- da se za izvajanje nadzora uporabi samo tiste podatke, ki so za to minimalno nujno potrebni in
- da se podatki o vozilih, pri katerih ni bilo ugotovljene kršitve, brišejo takoj.

Če namreč vozilo ni storilo kršitve pravil cestninjenja, ni podlage za hrambo ali obdelavo osebnih podatkov uporabnika vozila, tudi za 24 ur ne. Tako menimo, da bi se morali podatki o vozilih, pri katerih ni bila ugotovljena kršitev brisati takoj, ko je bilo ugotovljeno, da ni bila storjena kršitev (samo ugotavljanje pa seveda ne sme biti nesorazmerno dolgo).

24-urni, še toliko bolj pa 20-dnevni rok hrambe se morda zdi kratek, a za zlorabe osebnih podatkov je to povsem dovolj. Kot smo večkrat poudarili so lokacijski podatki posameznikov izjemno občutljivi in njihove zlorabe imajo lahko resne posledice. Ob vseh varovalkah, predpisih in varnostnih politikah se na koncu vedno srečamo s človeškim faktorjem in najbrž ni potrebno navajati primerov, ko bo nekdo želel vedeti ali se je določena registrska tablica nahajala na določenem cestninskem odseku v določenem času. Kakorkoli se zdi 24-urni rok hrambe kratek, toliko bolj pa 20-dnevni, daje možnosti za resne zlorabe in posega ne samo v temeljno človekovo pravico do varstva osebnih podatkov temveč tudi v pravico do svobode gibanja. Tudi represivni organi nimajo pravice 24-ur hraniti podatkov o lokacijah vozil in toliko manj ima lahko to pravico upravljavec cest, zato bo **IP na tej točki vztrajal, da hrambe podatkov o vozilih, pri katerih ni bila ugotovljena kršitev, ne sme biti in da se morajo ti podatki sproti brisati oziroma sploh ne hraniti.** S tem *de facto* odpadejo tudi številna preostala tveganja (npr. glede urejanja dostopnih pravic, revizijske sledi in vseh ostalih vidikov informacijske varnosti, tveganja uporabe osebnih podatkov za druge namene itd.), ki ste jih sicer pravilno identificirali. Evidence optično prepoznanih registrskih tablic (podatki naj bi se hranili do potrditve plačila cestnine glede na cestninski razred, vendar ne več kot 20 dni), tako **ne bomo podprli**.

Pri samem izvajanju nadzora mora prav tako biti upoštevano načelo minimizacije obdelave – tu je zlasti pomembno, kateri podatki se obdelajo in prikažejo osebam, ki izvajajo takšen

nadzor, ne glede na to, da gre za stacionarni ali mobilni sistem. **Narobe bi bilo, da se jim prikažejo katerikoli podatki o lastniku vozila, še preden je bila ugotovljena kršitev.** Ponovno poudarjamo, uporabnik vozila mora ostati anonimen za vse, dokler ni bila ugotovljena kršitev, kar vključuje prikaz podatkov na zaslonih nadzornikov. Sistem avtomatske prepoznave registrske tablice torej prebere registrsko tablico in ta podatek je treba preveriti z evidenco registrskih tablic kupljenih e-vinjet s cestninskim razredom, evidenco registrskih tablic vozil oproščenih plačila cestnine ter evidenco registrskih tablic v sistemu DarsGO. Kolikor je uparjanje pozitivno, potem ni potrebe po prikazu nobenega podatka niti po hrambi podatka o prebrani registrski tablici in sistem bi moral upoštevati to zasnovo.

Ko je enkrat ugotovljena kršitev, potem je seveda jasno, da je dopustno obdelati tiste osebne podatke, ki so potrebni za izvedbo ustreznih kaznovalnih postopkov in da za njihovo uporabo ter hrambo veljajo določbe prekrškovne zakonodaje.

Mnenje glede konkretnih določb

IP pozdravlja določbe 8. in 9. odstavka predlaganega 20. člena, ki upoštevajo naša že podana priporočila glede varstva osebnih podatkov. Pomisleke pa moramo izraziti glede predlaganega 10. in 12. odstavka 20. člena.

Predlagani 10. odstavek 20. člena namreč določa, da "*če nadzorni sistem upravljavca cestninskih cest samodejno ne potrdi izpolnitve obveznosti plačila cestnine za posamezno vozilo (npr. zaradi vremenskih vplivov), lahko upravljavec cestninskih cest hrani podatke o lokaciji vozila najdlje 20 dni od njihove pridobitve. V tem času upravljavec cestninskih cest osebno preveri, če je bila za posamezno vozilo izpolnjena obveznost plačila cestnine. Po poteku roka iz tega odstavka se podatki izbrišejo."*

Razumemo, da v določenih primerih, predvidoma ne na sistemski ravni, lahko pride do tega, da samodejno preverjanje e-vinjet ne bo mogoče (npr. delno prepoznana registrska tablica v slabih vremenskih razmerah), a se nam 20-dnevni rok za osebno preverjanje zdi nesorazmeren in neprimeren, obenem pa bistveno povečuje tveganja. Predvidoma število takšnih primerov ne bi smelo biti veliko in predlagamo, da se ta rok skrajša na največ 24 ur. Poudarjamo, da lahko ta izjema velja samo za primere, ko samodejno preverjanja plačila cestnine iz objektivnih razlogov ni bilo izvedeno, in ne za vse primere. Kot smo večkrat poudarili, podatki po izvedenem upravljanju oz. preverjanju ne bi smeli biti hranjeni, če ni bila zaznana kršitev.

Glede na zgoraj podane pripombe je potrebno smiselno popraviti tudi:

- določbo predlaganega 3. odstavka 23. člena, da bo jasno, da ne gre za evidentiranje podatkov (v smislu hrambe), temveč zgolj za preverjanje;
- določbo 6. odstavka predlaganega 46.a člena glede 24-urnega oziroma 20-dnevnega roka hrambe.

Predlagani 12. odstavek 20. člena določa, da *"je prepovedana uporaba podatkov o lokaciji vozila, s katerimi razpolaga upravljavec cestninskih cest, za namene, za katere je treba v skladu z zakonom, ki ureja kazenski postopek, in zakonom, ki ureja naloge in pooblastila policije, pridobiti odredbo pristojnega organa ali dovoljenje pristojne osebe.«*

Podpiramo namen predlagatelja, ki sledi našim priporočilom glede izrecnih zakonskih prepovedi uporabe teh podatkov za druge namene, vendar se nam predlagana določba zdi

nejasna. V isti okvir je namreč dana *odredba pristojnega organa* – kolikor gre za sodišče, potem takšen zakon ne sme posegati v pristojnosti sodišč – in *dovoljenje pristojne osebe*, pri čemer ni jasno, kdo so te pristojne osebe in pri katerih organih. Glede na navedeno predlagamo, da se določba zapiše bolj jasno in sicer, da je **prepovedana uporaba osebnih podatkov, ki se obdelujejo za namen cestninjenja, za druge namene, razen če tako določa zakon**.

Določbo 10. odstavka predlaganega 46.a člena[2] glede osebnih podatkov kupcev e-vinjet je po našem mnenju potrebno popraviti tako, da se ne zbira osebno ime in telefonska številka kupca, saj za navedene namene (obveščanje kupca o uspešno izvedenem nakupu elektronske vinjete, o potrditvi spremembe in o poteku veljavnosti elektronske vinjete) zadostuje elektronski naslov.

Zaključno se ponovno zahvaljujemo predlagatelju za zavedanje o pomenu varstva osebnih podatkov pri uvajanju e-vinjet, vloženi trud in pravočasno vključitev IP v strokovno razpravo. Verjamemo, da se vsi zavedamo, da je za izkoristek prednosti in priložnosti, ki jih nudi digitalizacija na tem področju, ter za zaupanje državljanov, v zakonodajne rešitve nujno potrebno vgraditi ustrezne varovalke za varstvo osebnih podatkov, s posebnim poudarkom na strogem upoštevanju načela minimizacije obdelave.

S spoštovanjem,

Mojca Prelesnik, univ. dipl. prav.,
informacijska pooblaščenka

Pripravil:
- mag. Andrej Tomšič, namestnik informacijske pooblaščenke

Poslati:
- naslovnikom po e-pošti;
- zbirka dokumentarnega gradiva pri IP.

[2] Opozarjamo tudi, da členi od 39 dalje v predlogu zakona (še) niso obrazloženi.