INFORMACIJSKI POOBLAŠČENEC
Vošnjakova 1, p.p. 78, SI-1000 Ljubljana
Telefon: + 386 (0) 1 230 97 30
Faks: + 386 (0) 1 230 97 78
www.ip-rs.si
REPUBLIKA SLOVENIJA

Datum: 14. 7. 2008

Zadeva: Mnenje Informacijskega pooblaščenca o varstvu osebnih podatkov pri elektronskem cestninjenju

Informacijski pooblaščenec na podlagi 7. točke prvega odstavka 49. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljevanju: ZVOP-1-UPB1) ter 2. člena Zakona o Informacijskem pooblaščencu (Uradni list RS, št. 113/05 in 51/07 – ZUstS-A, ZInfP) objavlja svoje neobvezno mnenje v zvezi z vprašanji varstva osebnih podatkov pri elektronskem cestninjenju osebnih vozil. Pri tem poudarjamo, da nismo prejeli nobene zahteve glede podaje mnenja na to temo, vendar pa zaradi dejstva, da elektronsko cestninjenje zahteva zelo obsežno obdelavo osebnih podatkov, podajamo svoje mnenje, za katerega pričakujemo, da bo upoštevano s strani pripravljavca zakonodaje in razpisnih postopkov. Podlago za pripravo mnenja daje Informacijskemu pooblaščencu tudi 48. člen ZVOP-1-UPB1, ki določa, da Informacijski pooblaščenec kot državni nadzorni organ za varstvo osebnih podatkov daje predhodna mnenja ministrstvom, državnemu zboru, organom samoupravnih lokalnih skupnosti, drugim državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov zakonov ter ostalih predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke.

Obstoječi standardi glede varstva osebnih podatkov v okviru EU so določeni z Direktivo Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23.11.1995, s spremembami, v nadaljevanju: Direktiva 95/46/ES), Direktivo Evropskega parlamenta in Sveta 2002/58/ES z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (UL L 201, 31.7.2002, v nadaljevanju: Direktiva 2002/58/ES) ter v okviru Sveta Evrope s Konvencijo Sveta Evrope o varstvu posameznikov glede avtomatske obdelave osebnih podatkov (v nadaljevanju: Konvencija 108). Pravica do varstva osebnih podatkov je izrecno priznana tudi v členu 8 Listine Evropske unije o temeljnih pravicah.

Direktiva 95/46/ES v 6. členu določa ključna načela v zvezi s kakovostjo podatkov, in sicer morajo biti osebni podatki: (a) **pošteno in zakonito obdelani**; (b) **zbrani za določene, izrecne ter zakonite namene in se ne smejo naprej obdelovati na način, ki je nezdružljiv s temi nameni**; (c) **primerni, ustrezni in ne pretirani glede na namene, za katere se zbirajo in/ali naprej obdelujejo**; (d) **točni in po potrebi ažurirani**; uporabiti je treba vse primerne ukrepe za zagotovitev, da se podatki, ki so netočni ali nepopolni, zbrišejo ali popravijo, ob upoštevanju namenov, za katere so bili zbrani ali za katere se naprej obdelujejo; (e) **shranjeni** v obliki, ki dopušča identifikacijo posameznikov, na katere se osebni podatki nanašajo, **le toliko časa, kolikor je potrebno za namene**, za katere so bili podatki zbrani ali za katere se naprej obdelujejo. Upravljavec osebnih podatkov pa mora zagotoviti, da ravna v skladu s temi zahtevami.

Direktiva Evropskega parlamenta in Sveta 2004/52/ES z dne 29. aprila 2004 o interoperabilnosti elektronskih cestninskih sistemov v Skupnosti (UL L 166, 30. 4. 2004, v nadaljevanju: Direktiva 2004/52/ES) v 7. odstavku 2. člena določa, da države članice zagotovijo, da se osebni podatki, potrebni za delovanje evropskega elektronskega cestninjenja, obdelujejo v skladu s pravili Skupnosti o varstvu svobode in temeljnih pravic posameznikov, vključno njihove zasebnosti, in še zlasti spoštujejo določbe direktiv

95/46/ES in 2002/58/ES. Direktiva 2004/52/ES tudi izrecno omenja pravna vprašanja, ki jih je potrebno rešiti, in sicer med drugim tudi potrebo po potrditvi veljavnosti izbranih tehničnih rešitev v odnosu do pravil Skupnosti, ki varujejo svobodo in temeljne pravice posameznikov, vključno zasebnost, ter zlasti po zagotovitvi skladnosti z zgoraj omenjenima direktivama.

V Republiki Sloveniji ta določila v celoti konkretizirata Ustava ter ZVOP-1-UPB1. Pooblaščenec želi v skladu s svojimi pristojnostmi in omenjenimi standardi zato v prvi vrsti opozoriti na dejstvo, da bi zaradi neustrezne tehnične in pravne ureditve sistema cestninjenja **lahko prišlo do nedopustnega prekomernega zbiranja oziroma obdelave osebnih podatkov**. V tem smislu je z vidika zakonite in poštene obdelave osebnih podatkov v skladu z ZVOP-1-UPB1 ter zagotavljanja spoštovanja načel namembnosti in sorazmernosti obdelave in zbiranja osebnih podatkov v skladu z ZVOP-1-UPB1 v prvi vrsti bistveno, da zakonodajalec jasno in nedvoumno opredeli osebne podatke, ki se zbirajo, ter namene, za katere se ti podatki zbirajo, ter, da se v tem smislu ustrezno ozko določi obseg njihovega zbiranja in obdelave, ki sta potrebna za doseganje zakonsko opredeljenih ciljev ter namenov, za katere se ti podatki zbirajo. To v praksi v primeru elektronskega cestninjenja pomeni tudi izbiro ustreznih tehničnih rešitev, ki omogočajo izvajanje zakonsko opredeljenih ciljev **brez nepotrebne prekomerne obdelave osebnih podatkov**. V nadaljevanju zato podajamo mnenje Pooblaščenca o potrebnih zahtevah z vidika varstva osebnih podatkov pri elektronskem cestninjenju.

Uvodoma je potrebno poudariti, da elektronsko cestninjenje v prostem prometnem toku po naravi stvari vključuje obdelavo **velike količine osebnih podatkov**, in sicer **lokacijske** in **časovne podatke** o prevoženi poti oziroma nahajališču osebnega vozila. Končni cilj Direktive 2004/52/ES je namreč uvesti plačevanje po načelu »plačaj, kolikor prevoziš«, prav tako pa naj bi vseevropsko delujoči sistem omogočal cestninjenje vseh vrst plačljivih cest, vključno z viadukti, predori in drugimi objekti, pri tem pa brez obdelave omenjenih osebnih podatkov ne gre. Z novim cestninskim sistemom naj bi bilo možno plačevanje cestnine brez vsakršnega oviranja in ustavljanja, poleg tega bi z isto napravo lahko plačevali cestnino na vseh evropskih cestah, ki bodo opredeljene kot cestninske ceste. Direktiva 2004/52/ES dopušča uvedbo obeh najpogosteje preučevanih tehnologij, in sicer tehnologije mikrovalov kratkega dosega (DSRC[1]) ter sistem na osnovi satelitskega določanja položaja vozila in prenosa podatkov po zmogljivih brezžičnih komunikacijskih omrežjih (GNSS/CN[2]) – za slednje se pogosto uporablja kar izraz satelitsko cestninjenje. Možni sta torej obe tehnologiji. Tako ena kot druga imata svoje prednosti in slabosti, mikrovalovne tehnologije so na primer že precej bolj razširjene in preizkušene, niso pa primerne za cestninjenje vseh cest. Prednost satelitskega cestninjenja je predvsem v fleksibilnosti, po drugi strani pa sistem v širšem evropskem prostoru še ni dovolj preizkušen. Tu je potrebno takoj pojasniti, da je neupravičen strah pred tem, da bi sateliti imeli neko vseobsegajočo bazo podatkov o lokacijah vozil – tako GPS kot bodoči Galileo namreč temeljita na pasivnih sprejemnikih, ki zgolj preračunajo svoj položaj glede na podatke, ki jih prejemajo iz satelitov, nikakor pa ti sprejemniki ne morejo satelitom sporočati svoje lokacije. Zato je tudi pri sami opredelitvi tega sistema cestninjenja potrebno upoštevati, da vozilo s pomočjo satelitske navigacije pridobi zgolj podatek o svoji lokaciji, podatke z nadzornim centrom cestninjenja pa si izmenjuje po brezžičnih omrežjih, kot je recimo obstoječe GSM omrežje.

Glede vprašanj varstva osebnih podatkov pri elektronskem cestninjenju gre zlasti za naslednja vprašanja:

[1] Dedicated Short Range Communications.
[2] Global Navigation Satellite System/Cellular Networks.

1. lastnosti naprave za obračun cestnine,
2. prostovoljna ali obvezna uporaba,
3. delitev vlog v procesu obračuna cestnine,
4. nadzor nad kršitvami.

Gotovo je do zasebnosti posameznika najbolj prijazen pristop, ko so podatki, ki so potrebni za izvedbo samega cestninjenja, **pod izključnim nadzorom uporabnika**. V tem primeru se obračun cestnine izvrši v napravi sami (t.i. inteligentna naprava ali Smart Client), nadzornemu centru pa se posreduje **samo seštevek potrošene vsote**. Vse štiri faze obračunskega postopka pri elektronskem cestninjenju se torej v tem primeru izvedejo v sami napravi:

1. določitev lokacije,
2. določitev cestninskega segmenta in ustrezne tarife,
3. izračun porabljene vsote za ta segment,
4. seštevek porabljenih vsot.

V takšnem primeru lahko govorimo o tem, da **ohranjamo anonimnost voznika**, **saj ima** uporabnik **vse lokacijske in časovne podatke shranjene pri sebi**, identificirati pa se mora le v primeru, da se pojavijo nepravilnosti, ki to dejansko terjajo: npr. ko uporabnik ne plača pravilno obračunane cestnine, ko mu je bilo ukradeno osebno vozilo, ko njegova naprava za cestninjenje ne deluje pravilno oziroma ne deluje takrat, ko bi morala (med vožnjo po cestninski cesti). Vse dokler ne nastopi ena od takšnih situacij, je potrebno zagotoviti zgolj to, da naprava v vozilu, ki obračunava cestnino po prevoženih kilometrih, na cestninski cesti deluje in da deluje pravilno. Seveda terja takšen pristop tudi določene varovalke, tako je potrebno poskrbeti za ustrezne standarde certificiranja, nameščanja in popravljanja naprav, gotovo pa ne gre odmisliti nekaterih tehničnih izzivov (npr. napajanje, preverjanje pravilnosti delovanja) in stroškovnih vidikov – pametna naprava je gotovo dražja. Nadzorni center pri takšni zasnovi sistema nima podatkov o dejanskih lokacijah osebnega vozila in zgolj preverja pravilnost delovanja naprave. Takšna rešitev ima določene prednosti tudi z ekonomskega vidika, saj takšna »inteligentna« naprava ni občutljiva na komunikacijske izpade (npr. področja, ki niso pokrita z GSM signalom) ali trenutne izpade obračunskega centra, saj zna sama izvesti obračun cestnine, medtem ko pride v primeru naprave, ki ves čas pošilja podatke v obračunski center (t.i. Thin Client, ki ne zmore sama izvesti obračuna), do izpada obračuna v področjih nepokritosti ali v primerih nedelovanja centralnega nadzora. saj naprava na tem področju ne pošlje podatkov v obračunski center. Pri tem je potrebno opozoriti še na to, da mora inteligentna naprava podpirati delovanje tudi v načinu »Thin Client«, in sicer zaradi zahtev po interoperabilnosti v evropskem prostoru. Naprave v vozilu bodo namreč morale znati delovati v različnih režimih in ob vstopu na teritorij določenega operaterja bo naprava dobila navodilo, kako naj deluje. Po podatkih, s katerimi razpolaga Pooblaščenec, mednarodne organizacije za standardizacijo ISO in CEN zdaj za to dogovorjeno rešitev pripravljajo ustrezne tehnične standarde, industrija oz. potencialni proizvajalci pa takšne rešitve imajo. Pooblaščenec je mnenja, da mora na teritoriju Republike Slovenije skladno z načelom sorazmernosti obdelave osebnih podatkov obveljati načelo delovanja obračuna v enoti sami. **Na podlagi zgoraj navedenega je namreč Informacijski pooblaščenec mnenja, da lahko zgolj takšna delitev obračunskega procesa, ki ohranja podatke v izključni posesti posameznika, zadosti kriteriju načela sorazmernosti obdelave osebnih podatkov (3. člen ZVOP-1-UPB1).** Ključni načeli varstva osebnih podatkov sta namreč **načelo namenskosti** in **načelo sorazmernosti**, izhajata pa iz postulata, da vsaka obdelava osebnih podatkov po naravi stvari pomeni poseg v ustavno pravico posameznika do zasebnosti, zato je potrebno zbirati in naprej

obdelovati samo toliko podatkov, kot je potrebno za dosego konkretnega cilja. Če je naš cilj učinkovito in pravično pobiranje cestnine (in to, upamo, da iskreno, poudarjajo vsi akterji), je zgoraj opisani način gotovo tisti, ki zadosti tem kriterijem, ostali izvedbeni načini namreč ne morejo zadostiti kriteriju sorazmernosti, če obstaja način, ki predstavlja manjši poseg v zasebnost posameznika.

Vmesna možnost, ki že **ne zadosti omenjenemu kriteriju sorazmernosti,** je tista, ki temelji na principu delitve podatkov med dvema centroma. Prvi tako pozna identifikacijsko številko naprave o vozilu in z njene strani prejema podatke o prevoženih poteh (časovne in lokacijske podatke), ne ve pa, komu pripada posamezna naprava v vozilu. Center nato izdela obračun cestnine na podlagi prejetih podatkov iz naprave v vozilu (takšen center je lahko tudi zgolj tehnični center - neke vrste posrednik ali proxy v okviru izbranega ponudnika, ki vrši obračun). Agregiran obračun podatkov (samo vsoto zaračunane cestnine v določenem obdobju, ne pa konkretnih časovnih in lokacijskih podatkov), pa nato skupaj z identifikacijsko številko naprave posreduje drugemu centru, ki pa ve, komu pripada določena naprava in ki terja lastnika te naprave za znesek cestnine, ki mu ga je dolžan, ne dobi pa podatkov o tem, kje se je posameznik vozil. Omenjena rešitev **zgolj navidezno ščiti zasebnost posameznika**, četudi prvi center pozna le lokacijske in časovne podatke, ne pozna pa identitete voznika, drugi pa ravno obratno, saj se na ta način **še vedno centralizirano zbirajo (in obdelujejo) izjemne količine osebnih podatkov** (časovnih in lokacijskih podatkov) - v enem centru, na centraliziran način. Skladno s stališči delovne skupine Article 29 Working Party in Informacijskega pooblaščenca je potrebno tudi te podatke nedvomno šteti za osebne podatke, če je možna določljivost posameznika, na katerega se nanašajo osebnih podatkov[3], **pri tem pa se na določljivost posameznika ne gleda zgolj skozi zmožnosti posameznega upravljavca (v konkretnem primeru prvega centra), temveč na splošno.** Ne glede na to, da prvi center ne more sam ugotoviti identitete posameznika, ki mu lokacijski in časovni podatki pripadajo, prvi center **nedvomno obdeluje osebne podatke**, saj je po 1. točki 6. člena ZVOP-1-UPB1 osebni podatek katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Posameznik pa je po 2. točki istega člena določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se jo lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa. Da je temu res tako, je evidentno v primeru neporavnanih računov, saj bo moral upnik ob nestrinjanju oz. zavrnitvi plačila računa na zelo preprost in hiter način reproducirati obračun cestnine (torej obdelovati lokacijske in časovne podatke o določljivem posamezniku).

Enostavno tehtanje po načelu sorazmernosti nam daje vedeti, da je **rešitev, kjer se podatki nahajajo v dveh centrih, slabša od tiste, ko so osebni podatki pod izključnim nadzorom posameznika, zato je potrebno dati prednost tisti rešitvi, ki manj posega v ustavno zagotovljeno pravico posameznika do zasebnosti.**

Zasebnosti najmanj naklonjena zasnova sistema elektronskega cestninjenja je ta, da se vsi podatki o času in lokacijah vozil zbirajo pri enem samem organu ali instituciji, da so hranjeni v centralizirani bazi za vsakega uporabnika posebej, nameni uporabe takšnih podatkov, zavarovanje in obseg uporabnikov pa ostanejo nedefinirani ali nejasni. Tudi na

[3] Več o tem glej *Mnenje 4/2007 o pojmu osebnih podatkov*, ki je dosegljivo na povezavi: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_sl.pdf.

takšno različico varuhi zasebnosti nikakor ne bodo pristali, saj se tako Informacijski pooblaščenec kot sorodni organi nemalokrat soočijo s pojavom t.i. *function creep*, ko se podatki prvotno zbirajo z enim namenom (ta je lahko tudi povsem legitimen in zakonit), nato se pa podatki uporabljajo za druge namene, dostop do podatkov se širi in tako naprej. Navedeno seveda velja analogno tudi v prejšnjem primeru, kjer so podatki deljeni med dvema subjektoma. Nasprotniki te argumentacije bodo trdili, da je pri podatkih, ki se hranijo centralno in obdelujejo z ustreznimi mehanizmi, kot so nadzor dostopa, sledljivost manipulacij s podatki in podobno, mogoče poskrbeti za višji nivo varnosti, kot pa ga lahko zagotovi posameznik. Na tovrstne argumente je potrebno odgovoriti na način, da tudi če se to resnično zagotovi, ne moremo mimo dejstva, da so v primeru hrambe pod nadzorom posameznika, zlorabi izpostavljeni zgolj njegovi osebni podatki (npr. pri kraji avtomobila, kraji naprave za cestninjenje ipd.), pri centralizirani hrambi pa so zlorabam (kljub morebitni večji varnosti) potencialno izpostavljeni osebni podatki vseh posameznikov, zato je potrebno **rešitvam, ki osebne podatke ohranjajo v izključni lasti in pod nadzorom posameznika, z vidika zasebnosti in zavarovanja podatkov dati prednost pred tistimi, ki podatke hranijo na centraliziran način**, **ne glede na to, ali se podatki hranijo skupaj z identitetami posameznikom v enem centru ali ločeno v dveh centraliziranih zbirkah.**

Vprašanje prostovoljne ali obvezne uporabe naprave za cestninjenje in vpliva te odločitve, ki bo v diskreciji posamezne države, je glede vplivov na zasebnost v veliki meri povezana z vprašanjem nadzora. Načeloma je prostovoljna izbira bolj prijazna do posameznika, saj ta lahko tako poda svojo privolitev v obdelavo osebnih podatkov (podobno kot pri nekdanjem sistemu ABC), a se tu poraja vprašanja nadzora takšne uporabe. Izkušnje iz nemškega sistema za tovornjake (Toll Collect) namreč kažejo, da se tovornjakarji v 90% odločijo za vgradnjo naprave za satelitsko cestninjenje in le slabih 10% uporablja druge načine (npr. napoveš in plačaš pot na avtomatu). Zanesljivost in natančnost pri vgrajenih napravah je 99,75% in tako rekoč vse težave z vidika nadzora in nepravilnosti nastajajo pri tistih, ki se najavljajo in plačujejo ročno (vozila brez vgrajenih naprav). Če nemške izkušnje pri tovornih vozilih prenesemo na cestninjenje osebnih vozil s končnim ciljem uporabe na vseh cestninskih cestah, je realnost prostovoljne uporabe precej dvomljiva. Cestninjenje v prostem prometnem toku ob prostovoljni uporabi namreč lahko terja na vseh cestninskih cestah postavitev izjemno kompleksnih, zahtevnih in dragih preiskovalnih sistemov (videonadzor, prepoznava avtomobilskih tablic ipd.), ki lahko predstavljajo še večji poseg v zasebnost, kot če bi bila uporaba naprave obvezna. Odločitev predlagateljev zakona mora biti zato zelo premišljena, zato je Pooblaščenec mnenja, da mora biti **uporaba alternativnih mehanizmov plačevanja cestnine vsaj destimulativna**. Pri tem želimo opozoriti še na to, da pogosto slišane primerjave z mobilno telefonijo niso upravičene, saj naprave za cestninjenje (na cestninski cesti) ne smemo onemogočiti tako kot lahko mobilni telefon (tudi če se prostovoljno odločimo zanjo!), zato je v tem primeru potreba po ustreznem varstvu osebnih podatkov še toliko bolj izrazita.

Posebno pozornost je potrebno – kljub temu, da se hramba podatkov in obračun cestnine izvaja v napravi – nameniti **vprašanju reklamacij** in **oddaljenega dostopa s strani nadzornega centra** ali **tretjih oseb** do surovih podatkov v takšnih primerih. Če želimo resnično zagotoviti, da so osebni podatki pod nadzorom uporabnika, je potrebno zagotoviti, da je možno dostopati do podatkov le na izrecno zahtevo uporabnika, vsak takšen dostop do časovnih in lokacijskih podatkov o prevoženih poteh in obračunanih zneskih pa mora biti ustrezno zabeležen z verodostojno in celovito revizijsko sledjo. Popolnoma nedopustno bi bilo, da bi bil možen nepooblaščen in neevidentiran dostop do podatkov v napravi v vozilu. Pooblaščenec še opozarja na določila 5. točke 1. odstavka in 2. odstavek 24. člena ZVOP-1, ki določata, da mora v okviru ukrepov in postopkov

zavarovanja osebnih podatkov v vseh primerih upravljavec poskrbeti, da je **omogočeno poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil**, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov. V primeru obdelave osebnih podatkov, ki so dostopni preko telekomunikacijskega sredstva ali omrežja, morajo strojna, sistemska in aplikativno programska oprema zagotavljati, da je obdelava osebnih podatkov v zbirkah osebnih podatkov **v mejah pooblastil uporabnika osebnih podatkov**. V skladu s tem bi bilo bodisi v predlogu zakona ali ustreznem podzakonskem aktu potrebno opredeliti, na kakšen način se beleži dostopanje in identifikacija pooblaščene osebe, ki dostopa do posameznih osebnih podatkov v skladu s posameznimi nameni.

Posameznik uživa pravico do vpogleda v lastne osebne podatke ne samo na podlagi zahtevka za reklamacijo, temveč tudi na podlagi 30. člena ZVOP-1-UPB1, ki opredeljuje zakonsko pravico posameznika do seznanitve z lastnimi osebnimi podatki. Gre za pravico, ki je del temeljne človekove pravice do varstva osebnih podatkov, določene v 3. odstavku 38. člena Ustave RS, ki pravi, da ima vsakdo pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi. 30. člen ZVOP-1-UPB1 v 3. točki prvega odstavka določa, da mora upravljavec osebnih podatkov posamezniku na njegovo zahtevo posredovati izpis osebnih podatkov, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj. Upoštevaje navedeno določbo lahko posameznik od upravljavca zahteva samo tiste podatke iz zbirke podatkov, ki se nanašajo nanj.

Pravna podlaga za uvedbo elektronskega cestninjenja nad osebnimi vozili bo morala natančno opredeliti **rok hrambe podatkov** in **možnosti dostopa do podatkov**, ki se nahajajo na napravi v vozilu. V skladu z 21. členom ZVOP-1 se osebni podatki lahko shranjujejo le toliko časa, dokler je to potrebno za dosego namena, zaradi katerega so se zbirali ali nadalje obdelovali (po končanem obračunu cestnin). Glede na obseg osebnih podatkov in stopnjo posega v posameznikovo zasebnost, ki bi ga predstavljal dostop do teh podatkov, je Informacijski pooblaščenec mnenja, da mora biti dostop do teh podatkov ustrezno omejen, in sicer na način, ki je analogen zakonskem varstvu, ki ga uživajo prometni podatki v elektronskih komunikacijah, ki se hranijo na podlagi t. i. retencijske direktive[4]. Dostop do teh podatkov je možen zgolj na podlagi sodne odredbe pristojnega organa za taksativno vnaprej opredeljene namene. Na tem mestu je potrebno opozoriti, da bi morala biti morebitna omejitev pravic posameznika do seznanitve z lastnimi osebnimi podatki izrecno navedena v zakonu, ki uvaja elektronsko cestninjenje nad osebnimi vozili, takšna omejitev pravice posameznika pa mora biti skladna z določbami 36. člena[5] ZVOP-1-UPB1.

Polje možnih zlorab osebnih podatkov, ki terja posebno obravnavo, je tudi **izvajanje nadzora in odkrivanje kršiteljev**. Pooblaščenec je mnenja, da ne sme biti ugotovljena identiteta voznikov, dokler niso storili nečesa, kar je opredeljeno kot kršitev cestninjenja, pri tem pa je potrebno upoštevati temeljno načelo sorazmernosti, in sicer tako, da se

[4] Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij.

[5] (1) Pravice posameznika iz tretjega in četrtega odstavka 19. člena, 30. in 32. člena tega zakona je mogoče z zakonom izjemoma omejiti iz razlogov varstva suverenosti in obrambe države, varstva nacionalne varnosti in ustavne ureditve države, varnostnih, političnih in gospodarskih interesov države, izvrševanja pristojnosti policije, preprečevanja, razkrivanja, odkrivanja, dokazovanja in pregona kaznivih dejanj in prekrškov, odkrivanja in kaznovanja kršitev etičnih norm za določene poklice, iz monetarnih, proračunskih ali davčnih razlogov, zaradi nadzora nad policijo in varstva posameznika, na katerega se nanašajo osebni podatki, ali pravic in svoboščin drugih.
(2) Omejitve iz prejšnjega odstavka se lahko določijo samo v obsegu, ki je nujen za dosego namena, zaradi katerega se določa omejitev.

najprej preverja obstoj in pravilno delovanje naprave za obračun cestninjenja v vozilu. Če nadzorna enota v zvezi s tem ne zazna kršitve, ne sme nadaljevati s postopki identifikacije naprave in s tem voznika. Šele v primeru, ko nadzorna naprava zazna odsotnost ali nepravilnost delovanja ali nastavitev naprave za obračun cestninjenja v vozilu, lahko skladno z načelom sorazmernosti pristojni organ nadaljuje s postopkom zajema registrske tablice vozila, ki je glede na poročila ekspertnih skupin priporočljiva metoda nadzora.

Pooblaščenec opozarja na posebno previdnost pri upravljanju t.i. **črnih list** kršiteljev v povezavi z avtomatsko prepoznavo registrskih tablic. Za oceno posega v zasebnost s tega vidika so zelo pomembne okoliščine delovanja tovrstnega sistema, zlasti **okoliščine identifikacije posameznika**. Morebitna identifikacija lastnika motornega vozila takoj ob prepoznavi registrske tablice ima seveda povsem drugačne vplive na zasebnost, kot v primeru, da se identifikacija lastnika motornega vozila izvrši šele ob ugotovljenem prekršku. V nadaljevanju predstavljamo izkušnje drugih držav z uvajanjem t.i. sistemov **za avtomatsko preverjanje registrskih tablic (ANPR – Automatic Number Plate Recognition)**, pri čemer pa je pri vsakem tolmačenju podatkov v nadaljevanju nujno potrebno upoštevati vse okoliščine uvajanja in načina delovanja takšnega sistema, kot so:

- namen uporabe,
- obseg dostopa do podatkov,
- roki hrambe podatkov,
- trenutek in pogoji za identifikacijo posameznika,
- ali gre samo za princip je zadetek/ni zadetka ipd.

Po raziskavi, ki jo je med nacionalnimi organi za varstvo osebnih podatkov opravil nizozemski varuh zasebnosti (College Bescherming Persoonsgegevens - CBP), je sistem avtomatske prepoznave registrskih tablic v uporabi v 12 evropskih državah (Bolgarija, Češka republika, Finska, Madžarska, Velika Britanija, Nemčija, Avstrija, Švedska, Irska, Estonija, Francija in Litva), v 6 državah pa v času opravljanja raziskave (marec-april 2008) takšni sistemi še niso bili v uporabi (Belgija, Islandija, Danska, Portugalska, Malta in Slovenija), preostalih 9 držav pa odgovorov ni posredovalo v predvidenem roku. V večini držav se tovrstni sistem uporablja za potrebe organov pregona, od iskanja ukradenih vozil do zelo splošnih preiskav, zaznavanja in pregona kaznivih dejanj. Po podatkih iz raziskave naj bi večina držav uporabljala sistem, ki temelji na principu je **zadetek/ni zadetka** (angl. hit/no hit), takšni sistemi pa so bili v večini držav uvedeni brez nove zakonodaje. Po podatkih iz raziskave so bili v večini primerov konzultirani uradi za varstvo osebnih podatkov, k čemur Informacijski pooblaščenec v primeru nejasnosti glede tega mnenja poziva tudi pristojno ministrstvo. Informacijski pooblaščenec namreč lahko na podlagi 48. člena ZVOP-1-UPB1 daje predhodna mnenja ministrstvom, državnemu zboru, organom samoupravnih lokalnih skupnosti, drugim državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov zakonov ter ostalih predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke.

Glede na zgoraj navedeno je nedopustna obdelava osebnih podatkov voznikov, ki niso storili kršitve. Pri takšnem pristopu nadzorni center zgolj preverja pravilnost delovanja naprave v vozilu in zgolj pooblaščena oseba (torej glede na namen, za katerega ima posamezna oseba v skladu z zakonom dostop do osebnih podatkov) lahko zahteva identifikacijo voznika ali podatke o lokaciji in to zgolj v določenih primerih, ki jih je potrebno taksativno navesti, med drugim na primer v primeru predrugačenja elektronske naprave za cestninjenje na vozilu tako, da ne deluje pravilno pri cestninjenju, v primeru nedelovanja elektronske naprave za cestninjenje na vozilu, med vožnjo po cestninskih

cestah ali v primeru, ko je bilo vozilo ukradeno. Za pravilno delovanje sistema t.j. elektronskega pobiranja cestnine zato **ni potrebno upravljavcem cestninskih cest stalno razkrivanje identitete in lokacije vsakega voznika, v kolikor ne nastopijo vnaprej zakonsko opredeljeni primeri, ko je identifikacija in določitev lokacije vozila potrebna**. Predlog zakona bi moral tako natančno določati, v katerih primerih se lahko posameznika identificira ali ugotavlja časovne in lokacijske podatke o prevoženih poteh, prav tako pa mora biti hkrati s tem določeno, katere pooblaščene osebe lahko takšno obdelavo podatkov izvajajo. Pooblaščenec še opozarja, da se osebni podatki v javnem sektorju, kamor sodi tudi policija, lahko obdelujejo le, če tako določa zakon, ki lahko tudi določi, da se določeni osebni podatki obdelujejo le na podlagi osebne privolitve posameznika. To pomeni, da je za obdelavo osebnih podatkov s strani policije potrebna izrecna zakonska podlaga, ki mora, v skladu z načelom sorazmernosti, določno in jasno, predpisati tudi razlog za uvedbo, namen uvedbe zbiranja podatkov ter točno določiti, kateri podatki se lahko zbirajo.

Pooblaščenec zaključuje mnenje s stališčem, da mora biti v relativno negotovih razmerah glede končnih odločitev na evropski ravni odločitev Slovenije glede sistema elektronskega cestninjenja izredno premišljena, saj si ne moremo privoščiti sprejetja zakonodaje in izbire poslovnega modela, ki kasneje ne bo v skladu z evropskimi zahtevami. **Z vidika varstva osebnih podatkov je zato v razmerah negotovosti potrebno stremeti k zagotavljanju najvišjih standardov zasebnosti, ki lahko v danih razmerah predstavljajo tudi model za način uveljavitve evropskega cestninjenja v širšem evropskem prostoru**. Če torej povzamemo, vztrajati je potrebno na ustreznih funkcionalnih zahtevah, ki omogočajo izvajanje zakonsko opredeljenih ciljev tako, da ima uporabnik vse lokacijske in časovne podatke shranjene pri sebi (brez nepotrebnega prekomernega centralnega zbiranja in obdelovanja osebnih podatkov) ter pri strogem zagotavljanju omejenega dostopa pooblaščenih oseb do podatkov ob zagotavljanju sledljivosti tako vpogledov kot ostalih elementov obdelave osebnih podatkov in namenu sorazmernega izvajanja nadzora, ki minimizira poseg v zasebnost posameznika.

Načeloma je vprašanje varstva osebnih podatkov pri elektronskem cestninjenju povsem enostavno. Plačevanje cestnine v osnovi ne zahteva centralizirane obdelave osebnih podatkov (dokler ne pride do kršitev), nesorazmerne obdelave osebnih podatkov pri obračunavanju cestnine, dostopa do podatkov in izvajanju nadzora. Temeljna načela varstva osebnih podatkov stremijo k ohranitvi takšnega stanja in tehnologija mora biti uporabljena na način, ki to stanje ohranja. Vsakršen odmik od tega bi predstavljal le dodaten poseg v že tako načeto zasebnost v informacijski družbi in ustavno varovane pravice posameznika.

S spoštovanjem,

Informacijski pooblaščenec
Nataša Pirc Musar, univ. dipl. prav.
pooblaščenka