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

Številka: 007-44/2019/6
Datum: 22. 5. 2020

Ministrstvo za notranje zadeve (Gp.Mnz@gov.si)
Ministrstvo za javno upravo (Gp.Mju@gov.si)
Ministrstvo za zunanje zadeve (Gp.Mzz@gov.si
Ministrstvo za pravosodje (Gp.Mp@gov.si)
Ministrstvo za delo, družino, socialne zadeve in enake možnosti (Gp.Mddsz@gov.si)
Ministrstvo za finance (Gp.Mf@gov.si)
Ministrstvo za obrambo (glavna.pisarna@mors.si)
Vrhovno sodišče Republike Slovenije (urad.vsrs@sodisce.si)
Služba Vlade Republike Slovenije za zakonodajo (gp.svz@gov.si)

ZADEVA: Predlog sprememb Zakona o osebni izkaznici EVA: 2019-1711- medresorsko usklajevanje – tretji krog

ZVEZA: Vaše sporočilo po e-pošti s prilogami z dne 7.5. 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.

Glede predložene ocene učinka:

Informacijski pooblaščenec (v nadaljevanju: IP) uvodoma pojasnjuje, da je po določbi člena 35(1) 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 (člen 35(7)). Skladno s priporočili Evropskega odbora za varstvo podatkov (ang. EDPB, evropski odbor), 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 člena 36(1) Splošne uredbe ter uvodnih izjav (84) in (94) *obdelava nadaljuje brez posvetovanja z nadzornim organom*. Upravljavec podatkov se mora z

[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

nadzornim organom posvetovati v primerih, ko opredeljenih tveganj ne more ustrezno obravnavati (tj. preostala tveganja ostajajo velika).

Kot je pojasnjeno v smernicah evropskega odbora, med nesprejemljivo veliko preostalo tveganje spadajo primeri, ko lahko posameznika, na katerega se nanašajo osebni podatki, doletijo pomembne ali celo nepopravljive posledice, ki jih ta ne more odpraviti (na primer nezakonit dostop do podatkov, zaradi katerega je ogroženo življenje posameznikov, na katere se nanašajo osebni podatki, ali zaradi katerega je lahko posameznik odpuščen ali v finančnih težavah), in/ali kadar se zdi očitno, da se bo navedeno tveganje uresničilo (na primer ker ne bo mogoče zmanjšati števila oseb, ki imajo dostop do podatkov, zaradi načinov njihove izmenjave, uporabe ali razširjanja, ali kadar znana ranljivost ni odpravljena).

Upravljavec podatkov se mora posvetovati z nadzornim organom vedno, kadar ne najde zadostnih ukrepov za zmanjšanje tveganj na sprejemljivo raven (tj. so preostala tveganja še vedno visoka). Poleg tega se mora upravljavec posvetovati z nadzornim organom vedno, kadar je to potrebno v skladu s pravom države članice in/ali kadar mora v skladu z njim pridobiti predhodno dovoljenje nadzornega organa glede obdelave za izvajanje naloge, ki jo upravljavec izvede v javnem interesu, vključno z obdelavo v zvezi s socialno zaščito in javnim zdravjem (člen 36(5)).

V konkretnem primeru ne gre za »klasično« oceno učinka, ki jo izdela upravljavec«, temveč za oceno učinka zakonodajnega predloga. Ne glede na navedeno IP obravnava prejeto oceno učinka smiselno v luči določb člena 35 Splošne uredbe glede tega, kaj naj bi ocena učinka vsebovala, predvsem z vidika sorazmernosti ter celovite in podrobne obravnave tveganj in ukrepov za njihovo obvladovanje.

IP je najprej pregledal predloženo oceno učinka z vidika njene celovitosti skladno s členom 36(7) Splošne uredbe in priporočili Evropskega odbora za varstvo podatkov (ang. EDPB, evropski odbor), kot so navedena v Prilogi 2 smernic o ocenah učinka.

S pomočjo kontrolnega seznama za celovitost ocene učinka iz priloge 2 smernic o ocenah učinka ugotavljamo, da smernice EDPB opozarjajo, da mora biti v oceni učinka:

- podana ocena izvora, narave, posebnosti in resnosti tveganj (uvodna določba 84), pri čemer so tveganja ocenjena z vidika posameznika, tako da:
    - so upoštevani viri tveganj (uvodna določba 90);
    - so upoštevani možni učinki na pravice posameznika v primeru nezakonitega dostopa, spremembe ali izgube podatkov;
    - sta ocenjeni verjetnost in resnost tveganj (uvodna določba 90);
- so opredeljeni ukrepi za obvladovanje tveganj (člen 35(7d) in uvodna določba 90).

IP ugotavlja, da **nista ocenjeni verjetnost in resnost tveganj** (uvodna določba 90), opredeljeni ukrepi za zamejitev tveganj ter ocenjena tudi raven tveganja po izvedenih ukrepih za zamejitev tveganj. Posledično tudi ni opredeljena metodologija za izračun skupnega tveganja ter stopnje tveganja (npr. nizka, srednja, visoka, zelo visoka). Podani so številni ukrepi za obvladovanje tveganj, vendar pa kot rečeno tveganja niso ocenjena z vidika verjetnosti in resnosti, zato tudi ni mogoče podati ocene, ali so predvideni vsi relevantni ukrepi in koliko prispevajo k zmanjševanju tveganj, saj kot rečeno “teža” tveganj ni ovrednotena. Glede na to, da gre kot kaže za obrazec, ki ga za izdelavo ocen učinka uporablja MNZ posebej poudarjamo kontrolni seznam iz Priloge 2 smernic EDPB, se katerim lahko ugotovi, ali je ocena učinka celovita.

Ocena učinka glede na kontrolni seznam za celovitost ocene učinka iz priloge 2 smernic o ocenah učinka ne vsebuje:

- ukrepov, ki prispevajo k varstvu pravic posameznika:

    - pravica do seznanitve in prenosljivosti podatkov (člena 15 in 20);
    - pravica do popravka in izbrisa podatkov (členi 16, 17 in 19);
    - pravica do ugovora in omejitve obdelave (členi 18, 19 in 21).
- ukrepov, ki prispevajo k informiranju posameznika o obdelavi podatkov (členi 12, 13 in 14).

Glede hrambe biometričnih podatkov

Uredba 2019/1157/EU sledi cilju, da se lahko biometrični identifikatorji za namene preverjanja verodostojnosti dokumentov in identitete imetnika **zbirajo in shranjujejo zgolj na pomnilniškem mediju osebnih izkaznic**. IP meni, da je ključno, da bo uporaba (pregled) biometričnih podatkov, shranjenih na pomnilniškem mediju, omogočena samo za namen preverjanja pristnosti osebne izkaznice in identitete imetnika s pomočjo neposredno dostopnih primerljivih značilnosti, kadar zakon zahteva predložitev osebne izkaznice, to je pri izvajanju mejne kontrole, kjer je tudi zagotovljena tehnologija, ki omogoča preverjanje biometričnih podatkov. Pregled biometričnih identifikatorjev tako ne sme biti mogoč v drugih primerih, npr. pri »klasičnem preverjanju« istovetnosti, ko posameznik na zahtevo uradne osebe na vpogled predloži osebno izkaznico.

Informacijski pooblaščenec je že v preteklih krogih usklajevanja poudarjal, da *Uredba (EU) 2019/1157 Evropskega parlamenta in Sveta z dne 20. junija 2019 o okrepitvi varnosti osebnih izkaznic državljanov Unije in dokumentov za prebivanje, izdanih državljanom Unije in njihovim družinskim članom, ki uresničujejo svojo pravico do prostega gibanja* v tretjem odstavku 10. člena uredbe določa maksimalen rok hranjenja biometričnih podatkov in sicer 90 dni od datuma izdaje dokumenta, s tem da zadevni odstavek določa, da se za namene personalizacije osebnih izkaznic ali dokumentov za prebivanje shranjujejo zelo varno in le do prevzema dokumenta, vsekakor pa največ 90 dni od datuma izdaje dokumenta. Uredba (EU) 2019/1157 še določa, da se biometrični identifikatorji po preteku tega obdobja takoj izbrišejo ali uničijo.

MNZ pojasnjuje, da je bila pripomba upoštevana na način, da se prstni odtisi v evidenci izdanih osebnih izkaznic »*hranijo 15 dni od vročitve osebne izkaznice oziroma najkasneje 90 dni od izdaje osebne izkaznice*«. Menimo, da takšna rešitev še vedno omogoča pretirano dolg rok hrambe biometrijskih podatkov, ki so, kot smo že večkrat opozorili, povezani z zelo visokimi tveganji, zato predlagamo, da se omenjena določba zapiše, da bo jasno, da se **biometrični podatki** hranijo **najdlje 15 dni od vročitve osebne izkaznice in nobenem primeru več kot 90 dni od izdaje osebne izkaznice**. **Posebej opozarjamo, da mora navedeno veljati za vse biometrične podatke, torej tudi za biometrične fotografije in ne samo za prstne odtise. Pripominjamo, da morajo biti zakoni jasni (lex certa), to zaradi nujnega zagotavljanja pravne varnosti pomeni predvsem to, da tovrstne določbe ne smejo dopuščati različnih interpretacij. Predlagamo tudi, da ponovno razmislite, ali je potreben tako dolg rok.**

Nove osebne izkaznice naj bi vsebovale tudi biometrične fotografije, zato morajo tudi za njih veljati iste varovalke kot za prstne odtise, sicer tveganja za zlorabe biometričnih podatkov niso zmanjšana. Primerjalno opozarjamo, da veljavni Zakon o potnih listinah določa, da **evidenca izdanih potnih listin vsebuje fotografijo imetnika v digitalni obliki, ki je ni mogoče prebrati z napravami za branje biometričnih podatkov** (30. člen) – predlog sprememb ZOIzk-1 pa takšne varovalke ne vsebuje! Če rok hrambe 15 dni od vročitve osebne izkaznice ne bo veljal tudi za biometrične fotografije **bi država *de facto* vzpostavila zbirko biometričnih podatkov vseh imetnikov novih osebnih izkaznic**. Uredba 2019/1157/EU je v uvodni določbi št. 21 jasna: "*Ta uredba ne zagotavlja pravne podlage za vzpostavitev ali vodenje zbirk podatkov na nacionalni ravni za shranjevanje*

biometričnih podatkov v državah članicah, kar je vprašanje nacionalnega prava, ki mora biti skladno s pravom Unije na področju varstva podatkov. Ta uredba tudi ne zagotavlja pravne podlage za vzpostavitev ali vodenje centralizirane zbirke podatkov na ravni Unije." Verjamemo, da je odveč poudarjati resnost tveganj obstoja takšne baze na državnem nivoju za varovanja temeljnih človekovih pravic.

Hramba biometričnih podatkov izven samega dokumenta prav tako ni v skladu s cilji samega zakona, t.j. da se pri prehodu meje ugotavlja, ali je oseba, ki uporablja konkretno osebno izkaznico, res oseba, ki ji je bila ta osebna izkaznica izdana, s primerjavo njene fotografije in prstnih odtisov, zajetih na licu mesta, s fotografijo in prstnimi odtisi, ki so zapisani na pomnilniškem mediju (primerjava 1:1), kakor tudi ne Uredbe 2019/1157/EU, ki sledi cilju, da se lahko biometrični identifikatorji za namene preverjanja verodostojnosti dokumentov in identitete imetnika zbirajo in shranjujejo zgolj na pomnilniškem mediju osebnih izkaznic. Smiselno navedenemu se pod vprašaj postavlja tudi **predlog za avtomatizirano preverjanje istovetnosti (ustreznosti predložene fotografije ob vlogi) na podlagi primerjave fotografij iz evidenc uradnih identifikacijskih dokumentov**, saj tega ni mogoče drugače razumeti kot biometrično preverjanje posameznika izven namenov zakona in Uredbe 2019/1157/EU.

S spoštovanjem,

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