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: 007-11/2020/5
Datum: 8. 5. 2020

Urška Bukovec
Digitally signed by Urška Bukovec
Date: 2020.05.08 13:52:55 +02'00'

Ministrstvo za javno upravo
Direktorat za informacijsko družbo in informatiko
Ga. Simona Kralj Zatler
simona.kralj-zatler@gov.si

ZADEVA: Predlog uredbe o zasebnosti in elektronskih komunikacijah z dne 6.3.2020 – MNENJE
ZVEZA: kompromisni predlog HR predsedstva, gradivo št. 6543/20

Spoštovani,

zahvaljujemo se vam za kompromisni Predlog uredbe o zasebnosti in elektronskih komunikacijah HR predsedstva, z dne 6.3.2020, gradivo št. 6543/20 in povzeta stališča drugih držav članic EU do členov 6 in 8. Kot že izpostavljeno[1] tudi v naših mnenjih glede posameznih členov predloga, Informacijski pooblaščenec (v nadaljevanju IP) meni, da trenutni predlog evropske uredbe o e-zasebnosti, ki naj bi nadomestila sedaj veljavna pravila glede obdelave podatkov uporabnikov elektronskih komunikacij, niža raven varstva pravic uporabnikov, kot ga zagotavlja Splošna uredba o varstvu podatkov (GDPR) in raven varstva, kot je že zagotovljeno s trenutno veljavno Direktivo o e-zasebnosti in Zakonom o elektronski komunikacijah. Predstavlja tudi velik odmik od prvotnega predloga Evropske komisije iz leta 2017.

Prenovljena pravila za varovanje uporabnikov elektronskih komunikacij so nujno potrebna, saj se ti v vsakodnevnem življenju težko izognejo uporabi elektronskih komunikacijskih naprav in storitev, in s tem deljenju raznovrstnih podatkov o sebi, svojih interesih, svojem gibanju in stanju. Podatki o vsebini komunikacij in meta podatki lahko zgradijo popolno sliko posameznikovega življenja. Današnji razmah uporabe naprednih analiz podatkov, avtomatizacije procesov profiliranja uporabnikov in njihove diskriminacije, uporabe in zlorabe meta podatkov uporabnikov za različne namene, tudi za namene politične manipulacije ob volitvah, pa predstavlja neposredno grožnjo demokratičnim procesom v družbi. Predlog uredbe uvaja vse bolj nejasna pravila, ki nižajo raven varstva pravic posameznikov, kot podrobneje opredeljujemo v nadaljevanju. IP se do predlogov uredbe opredeljuje tudi v okvira Evropskega odbora za varstvo podatkov[2].

K členu 3(1):
Člen 3 določa teritorialno veljavo uredbe in v prvem odstavku navaja, da uredba ureja zagotavljanje storitev elektronskih komunikacij končnim uporabnikom, ki so v uniji, in ureja obdelavo podatkov o vsebini ter metapodatkih, varovanje informacij iz terminalne opreme itd. uporabnikov, ki so v uniji. Postavlja se vprašanje, ali osredotočanje le na kriterij uporabnikov, ki so v uniji in ne (hkrati tudi) na kriterij ustanovitve ponudnika storitve v uniji (režim kot ga v členu 3 pozna Splošna uredba o varstvu podatkov), pomeni, da bo v praksi ponudnik storitev elektronskih komunikacij, ustanovljen v EU, moral upoštevati določbe uredbe o e-zasebnosti le za tiste njegove uporabnike, ki so v uniji. Nadaljnje vprašanje glede kriterija "so v uniji" je, ali so to uporabniki, ki so lokacijsko (v določenem trenutku v času) v uniji ali gre za uporabnike iz EU, v smislu njihovega prebivališča. V vsakem primeru se postavlja vprašanje, ali bo ponudnik storitve iz EU na podlagi tega člena lahko diskriminiral med

[1] https://www.ip-rs.si/novice/novi-predlog-uredbe-o-e-zasebnosti-bistveno-niza-raven-varstva-pravic-posameznikov-pri-upo-1166/
[2] Proti uvajanju pravnih podlag, ki so po svoji vsebini odprte (npr. tehtanje zakonitega interesa), smo se nadzorni organi za varstvo osebnih podatkov v EU izrecno izrekli v izjavi z dne 25. 5. 2018: edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf

lastnimi uporabniki in varstvo zagotavljal le tisti, za katere bo presodil, da so iz unije. IP meni, da je določba neusklajena z določbo člena 3 Splošne uredbe o varstvu podatkov.

K členu 4(3):
V točki f uredba definira neposredno trženje kot komunikacijo, ki je poslana preko javno dostopne storitve elektronskih komunikacij neposredno enemu ali več določenih končnih uporabnikov. Vprašanje je, ali nov dostavek "preko javno dostopne storitve" pomeni, da bi v praksi omejitve, ki jih za pošiljanje neželenih sporočil določa uredba, veljale le za manjši krog tovrstnih sporoči (npr. za t. i. spam preko e-pošte, tudi za avtomatizirane glasovne klice), ne pa tudi npr. za enakovrstna sporočila, ki so poslana preko podobnih storitev elektronskega komuniciranja in neposrednega sporočanja ponudnikov tipa WhatsApp, Viber, družbenih omrežij, itd. Na to nakazuje tudi sprememba v uvodni določbi 32, da neposredno trženje naj ne bi zajemalo prikazovanja oglasov na spletnih straneh ali v okviru storitev informacijske družbe, ki jo je zahteval uporabnik. Zagotavljanje, da tudi za funkcionalno ekvivalentne ponudnike storitev elektronskih komunikacij veljajo enake omejitve, se izkazuje kot izredno pomembno tudi v trenutnem kontekstu pandemije, ko je izrazito porastla uporaba različnih ponudnikov neposrednega sporočanja, video klicev itd. zaradi dela in šolanja na daljavo. Varovanje pravic končnih uporabnikov je v tem okviru ključnega pomena.

Posebej je zaskrbljujoča tudi sprememba v uvodni določbi 32, ki je v prejšnjih predlogih med neposredno trženje poleg ponujanja storitev in izdelkov v komercialnem smislu jasno uvrščala tudi komunikacije z namenom politične promocije oz. promocije namenov neprofitnih organizacij. Trenutni predlog to mehča, in državam članicam daje možnost, da to določijo nacionalno. Izkušnje iz premiera Cambridge Analytica so jasno pokazale na pomembnost pravil na področju politične promocije in na veliko škodo demokratičnemu procesu in svobodnim volitvam, ki nastaja ob nejasnih pravilih na tem področju. Prav tako je razlikovanje pravil glede neposrednega trženja v državah članicah že v preteklosti doprineslo k pravni negotovosti in nižanju varstva pravic končnih uporabnikov. Režim za neželene komunikacije komercialne narave in komunikacije politične promocije bi z vidika resnosti posledic za družbo in posameznike vsekakor moral biti enako omejujoč.

K členu 4a:
Nov odstavek 2a uvaja relativno nizek prag za dokazilo, da je končni uporabnik privolil v smislu člena 8, in sicer naj bi bil za to dovolj tehnični protokol, ki izkazuje, da je bila privolitev dana na terminalni opremi, če upravljavec ne more identificirati posameznika. Ob dejstvu, da si terminalno opremo pogosto deli več uporabnikov (npr. v domačem gospodinjstvu) in da so ti uporabniki lahko tudi otroci, tak nizek prag izkazovanja privolitve nujno pomeni nižanje varstva pravic posameznika. Vprašljiva je tudi skladnost z določbami Splošne uredbe o varstvu podatkov, ki v členu 8 posebej določa pogoje glede privolitve otroka ob uporabi storitev informacijske družbe ter dolžnosti ponudnika storitve v zvezi s tem.

V nadaljevanju navajamo pripombe k členom 6, 7 in 8, ki smo vam jih že posredovali dne 4. 3. 2020 ter posebej opozarjamo na pomembnost razumevanja določb glede meta podatkov tudi z vidika situacije epidemije in s tem povezanih tem obdelave lokacijskih podatkov in podatkov iz terminalske opreme posameznika. Pravila glede poseganja v terminalsko opremo posameznika morajo varovati uporabnika, kakršni koli posegi v to varstvo oziroma omejitve tega varstva glede na člen 11 pa morajo biti nujni v demokratični družbi in sorazmerni.

K členu 6(d):
IP opozarja, ni primerno, da uredba vpeljuje nove pravne podlage za obdelavo podatkov uporabnikov elektronskih storitev s strani organov pregona poleg pravil, kot jih določa nacionalna oz. EU zakonodaja.

K členu 6(b)e:
IP močno nasprotuje preoblikovanju določb glede dopustne obdelave meta podatkov na način, predstavljen v zadnjem osnutku uredbe, z dodajanjem pravne podlage zakonitega interesa ponudnika storitve, kljub varovalom, ki so navedena glede omejitev obdelave podatkov otrok, občutljivih osebnih podatkov, in podatkov uporabljenih za izdelavo profila posameznika. Namen uredbe je usklajevanje ravni varstva osebnih podatkov s Splošno uredbo o varstvu podatkov in nikakor ne nižanje te ravni varstva. Uvajanje pravne podlage, kjer je na ponudniku storitve obveza tehtanja med svojimi interesi in pravicami posameznika odpira vrata legitimaciji posegov v zasebnost uporabnika elektronskih komunikacij zaradi poslovnih interesov ponudnikov storitev, posegov, ki so ob današnjem razmahu

uporabe naprednih analiz podatkov, avtomatizacije procesov profiliranja uporabnikov in njihove diskriminacije, uporabe in zlorabe meta podatkov uporabnikov za različne namene, tudi za namene politične promocije (kar lahko predstavlja neposredno grožnjo demokratičnim procesom v družbi) ena večjih groženj pravicam posameznikov. Uvedba pravne podlage zakonitega interesa kot predlagana niža tudi že doseženo raven varstva pravic elektronskih komunikacij z Direktivo 2002/58/ES, ki obdelavo meta podatkov dopušča le na podlagi privolitve posameznika in za druge, izrecno v zakonu določene namene (npr. zaračunavanje storitev).

Sklicevanje na določbe Splošne uredbe o varstvu podatkov o predhodni oceni vpliva iz člena 35 GDPR in predhodnim posvetovanjem z nadzornim organom, ne pomeni zadostne varovalke, predvsem pa bo organ, ki bo to izvajal, nujno potreboval veliko dodatno kadrovsko, tehnično in finančno okrepitev, da določba ne bo le mrtva črka na papirju. Organ bo namreč soočen s presojo procesov tehtanja velikega števila zavezancev po uredbi, ne glede na to, kdo bo sploh nadzorni organ za to uredbo.

K členu 7(4):
IP izraža enake pomisleke kot pri členu 6(d): ni primerno, da bi določba služila kot nova pravna podlaga za hrambo in dostop do podatkov uporabnikov elektronskih komunikacij za namen organov pregona.

K členu 8:
IP podaja enake komentarje kot pri členu 6(e) glede uvajanja nove pravne podlage zakonitega interesa. V okviru tehnologij, s katerimi je mogoč poseg v uporabnikov terminalno opremo (piškotki, odtisi, piksli, itd..) in sledenje uporabniku predlagana ureditev pomeni nižanje že zagotovljene ravni varstva uporabnikovih pravic z Direktivo 2002/58/ES, kjer spremembe iz leta 2009 izrecno zahtevajo uporabnikovo vnaprejšnjo privolitev in ne več le zagotavljanja možnosti za naknadno zavrnitev (opt-out). Pravna podlaga zakonitega interesa se v tem kontekstu močno približa ureditvi opt-out, kar pomeni veliko nevarnost in nižanje ravni varstva pravic posameznikov, ob zavedanju, da je sledenje uporabnikom preko različnih naprav in uporaba njihovih podatkov za različne namene danes vseprisotno in predstavlja velik poseg v njihove pravice iz razlogov, kot so pojasnjeni ob členu 6(b)e.

Dodatno IP opozarja, da je določba 8(g) člena, ki kot omejitev za uporabo te pravne podlage določa profiliranje posameznikov v neskladju z zadnjim odstavkom recitala 21b, ki tako obdelavo dopušča, če gre za storitev, ki je uporabniku na voljo brezplačno in je financirana z oglaševanjem. Profiliranje je v sodobnem digitalnem oglaševanju, ki temelji na procesih avtomatiziranega programatičnega oglaševanja po načelu dražb uporabniških profilov (*Real Time Bidding*) prevladujoča praksa, kar pomeni, da praktično vse digitalno oglaševanje, na katerega se recital 21b nanaša, vključuje profiliranje.

Hkrati je recital 21b nejasen sam po sebi, saj opredeljuje, kdaj se lahko ponudnik storitve zanaša na svoj zakoniti interes, hkrati pa temu za pogoj postavi, da je uporabnik tako rabo podatkov sprejel (*accepted such use*), in se torej nanaša na pravno podlago privolitve. Gre torej za nedopustno mešanje več pravnih podlag, ki se medsebojno izključujejo.

Poledica nejasnih določb in pojasnil v recitalih je pravna nedorečenost in nižanje ravni varstva pravic posameznikov, nejasnosti pri interpretaciji določb pa bodo pomenile velike težave tudi za nadzorne organe, posebej ob upoštevanju, da se praks obdelave meta podatkov poslužuje veliko ponudnikov, ki poslujejo čezmejno in bo nadzor nad določbami uredbe moral vsebovati komponento čezmejnega sodelovanja organov. V tem okviru IP izrecno pozdravlja dodatek v uvodni določbi 38, da morajo bit vsakemu nadzornemu organu za nadzor nad uredbo zagotovljeni dodatni finančni in kadrovski resursi, prostori in infrastruktura.

K poglavju IV:
Uredba državam članicam dopušča popolno fleksibilnost pri določanju organov za nadzor. Trenutni predlog ne vključuje več niti sklica na organe za nadzor nad Splošno uredbo o varstvu podatkov, kljub temu, da uredba predstavlja specialni akt, ki naj bi dopolnil okvir za varstvo osebnih podatkov v EU. Postavlja se vprašanje, kako bi bil nadzor nad uredbo sploh lahko učinkovit, ob prekrivanju pristojnosti organov za varstvo osebnih podatkov s pristojnostmi drugih organov, ki bi jim bil zaupan nadzor nad to uredbo, tudi z vidika izkušenj pri nadzoru nad nacionalnimi implementacijami določb

sedaj veljavne Direktive o e-zasebnosti. Pomanjkljivosti razdrobljenega nadzora ugotavlja tudi Evropska komisija v svojem poročilu[3]. Hkrati predlog uredbe ohranja pristojnosti Evropskega odbora za varstvo podatkov za pripravo smernic s področja uredbe. Če organi za varstvo osebnih podatkov, ki sestavljajo Odbor, ne bodo tudi organi, ki nadzorujejo uredbo, bo priprava smernic vsekakor otežena, poleg tega pa je vprašljivo, kako učinkovito bodo lahko potencialno drugi nadzorni organi izvajali smernice pripravljene s strani odbora in z vidika organov za varstvo osebnih podatkov. Dodatno predlog uredbe zgolj napotuje na to, da morajo organi sodelovati med sabo in doprispevati h konsistentnosti uporabe pravil, izbrisani pa so vsi sklici na mehanizme sodelovanje in zagotavljanja skladnosti po poglavju 7 Splošne uredbe o varstvu podatkov, ki bi zagotavljali večjo formalizacijo sodelovanja in s tem višjo raven pravi posameznikov. V okviru, kot ga predvideva sedanji predlog, je tako sodelovanje kot tudi doseganje skladnosti uporabe uredbe, praktično na ravni priporočila. Hkrati pa iz izkušenj pri nadzoru nad Splošno uredbo o varstvu osebnih podatkov zelo jasno vemo, kako pomembni so mehanizmi za nadzor nad čezmejnimi praksami obdelave osebnih podatkov, saj večina največjih ponudnikov tovrstnih storitev, ki predstavljajo tveganja za pravice posameznikov, posluje čezmejno, so multinacionalna podjetja z veliko močjo, prevladujoča na trgih elektronskih komunikacij. Nadzor nad njimi je otežen in formalizirani postopki čezmejnega sodelovanja po Splošni uredbi o varstvu podatkov ponujajo celostnejši okvir za sodelovanje pri nadzoru[4], ki že kaže nekatere prednosti in uspešne rešitve primerov.

Lepo vas pozdravljamo,

Pripravila:

dr. Jelena Burnik,
vodja mednarodnega sodelovanja in nadzora

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

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

[3] https://ec.europa.eu/digital-single-market/en/news/evaluation-and-review-directive-200258-privacy-and-electronic-communication-sector
[4] Več v letnem poročilu IP, str. 71: https://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Letno_porocilo_2018_FINAL.pdf

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