

Izjava



Izjava št. 03/2021 o uredbi o e-zasebnosti Sprejeta 9. marca 2021

Evropski odbor za varstvo podatkov je sprejel naslednjo izjavo:

Evropski odbor za varstvo podatkov podpira dogovorjeni pogajalski mandat Sveta o varstvu zasebnosti in zaupnosti pri uporabi elektronskih komunikacijskih storitev (v nadaljevanju: stališče Sveta) kot pozitiven korak k novi uredbi o e-zasebnosti. Izredno pomembno je, da se splošni okvir EU za varstvo podatkov hitro dopolni z usklajenimi pravili za elektronske komunikacije.

Kot je bilo že večkrat navedeno¹, uredba o e-zasebnosti v nobenem primeru ne sme znižati ravni varstva, ki jo zagotavlja sedanja Direktiva o zasebnosti in elektronskih komunikacijah, temveč bi morala Splošno uredbo o varstvu podatkov dopolnjevati z zagotavljanjem dodatnih trdnih jamstev za zaupnost in varstvo vseh vrst elektronskih komunikacij. Uredba o e-zasebnosti se nikakor ne more uporabiti za dejansko spremembo Splošne uredbe o varstvu podatkov. Glede tega stališče Sveta vzbuja več pomislekov, Evropski odbor za varstvo podatkov pa želi poudariti vprašanja, ki bi jih bilo treba obravnavati v prihodnjih pogajanjih.

Ta izjava ne posega v morebitno prihodnjo podrobnejšo izjavo ali mnenje Evropskega odbora za varstvo podatkov o stališčih so-zakonodajalcev.

Pomisleki glede obdelave in hrambe elektronskih komunikacijskih podatkov za namene kazenskega pregona in zaščite državne varnosti

Glede členov 6(1)(d) in 7(4) Evropski odbor za varstvo podatkov vnovič poudarja, da morajo biti zakonodajni ukrepi, ki od ponudnikov elektronskih komunikacijskih storitev zahtevajo hrambo elektronskih komunikacijskih podatkov, skladni s:

-) členoma 7 in 8 Listine EU o temeljnih pravicah,
-) najnovejšo sodno prakso Sodišča Evropske unije² in
-) členom 8 Evropske konvencije o človekovih pravicah.

Evropski odbor za varstvo podatkov meni, da uredba o e-zasebnosti ne sme odstopati od uporabe najnovejše sodne prakse Sodišča EU, ki zlasti določa, da je treba člene 7, 8 in 11 ter člen 52(1) Listine EU o temeljnih pravicah razlagati tako, da nasprotujejo zakonodajnim ukrepom, ki bi preventivno

¹ Glej celoten seznam dokumentov o pravilih o e-zasebnosti, ki sta ga pripravila Evropski odbor za varstvo podatkov in Delovna skupina iz člena 29, priložen k tej izjavi.

² Združene zadeve Sodišča EU C-511/18, C-512/18 in C-520/18, zadeva C-623/17.

zagotavljali splošno in neselektivno hrambo podatkov o prometu in lokaciji. Zato je na podlagi Listine EU o temeljnih pravicah dovoljena samo pravna podlaga za ciljno usmerjeno hrambo podatkov za namene kazenskega pregona in zaščito državne varnosti, v vsakem primeru pa bi zanjo morale veljati stroge časovne in materialne omejitve ter nadzor sodišča ali neodvisnega organa.

Glede izključitve dejavnosti obdelave podatkov s strani ponudnikov iz področja uporabe uredbe, Evropski odbor za varstvo podatkov meni, da je taka izključitev v nasprotju s predpostavko skladnega okvira EU za varstvo podatkov. Vendar Evropski odbor za varstvo podatkov poudarja, da se v primeru izključitve uporablja Splošna uredba o varstvu podatkov.

Zaupnost elektronskih komunikacij zahteva posebno varstvo (členi 6, 6a, 6b in 6c)

Zaupnost komunikacij je temeljna pravica, ki jo varuje člen 7 Listine EU o temeljnih pravicah in je že vpeljana z Direktivo o zasebnosti in elektronskih komunikacijah. Ta pravica do zaupnosti mora veljati za vse elektronske komunikacije, ne glede na način pošiljanja, tako v mirovanju kot tudi med prenosom ter od pošiljatelja do prejemnika, poleg tega pa mora tudi varovati celovitost terminalne opreme vsakega uporabnika.

Splošne prepovedi z redkimi izjemami za obdelavo osebnih podatkov

Evropski odbor za varstvo podatkov v celoti podpira pristop, ki temelji na splošnih prepovedih ter vsebuje ozke, specifične in jasno opredeljene (namensko usmerjene) izjeme.

Vendar Evropski odbor za varstvo podatkov izraža zaskrbljenost, saj se zdi, da nekatere izjeme (zlasti členi 6(1)(c), 6b(1)(e), 6b(1)(f) in 6c), ki jih je uvedel Svet, dopuščajo zelo široke vrste obdelave, in opozarja, da je treba te izjeme omejiti na specifične in jasno opredeljene namene. V vsakem primeru bi bilo treba te posebne namene izrecno navesti, da se zagotovita pravna varnost in najvišja možna stopnja varstva.

Poleg tega bi lahko izjeme iz členov 6(1)(b), 6(1)(c) in 6(1)(d), ki omogočajo dostop do elektronskih komunikacijskih podatkov, vključno do vsebine, za zagotovitev varnosti omrežja in naprav končnih uporabnikov, ponudniku elektronskih komunikacijskih storitev ali njegovim obdelovalcem omogočile popoln dostop do vsebine vseh komunikacij končnih uporabnikov. Ker bi tak dostop lahko ogrozil pravico končnega uporabnika do zaupnosti in pričakovanja glede zasebnosti, bi moral biti sorazmeren in bi ga bilo treba omejiti, s čimer naj bi se vsaj opozorilo, da to ne sme privedi do sistematičnega spremljanja vsebine elektronskih komunikacij, ponudnikom ali obdelovalcem pa se ne sme dovoliti, da zaobidejo kakršno koli šifriranje.

Nazadnje bi bilo treba v uredbi poudariti vlogo anonimizacije kot temeljnega jamstva, ki bi mu bilo treba sistematično dati prednost pri uporabi elektronskih komunikacijskih podatkov.

Razpoložljivost močnega in zaupanja vrednega šifriranja je v sodobnem digitalnem svetu nujna

Močno najsodobnejše šifriranje bi moralo biti splošno pravilo za zagotovitev varnega, prostega in zanesljivega pretoka podatkov med državljani, podjetji in vladami, poleg tega je bistveno za zagotavljanje skladnosti z varnostnimi obveznostmi iz Splošne uredbe o varstvu podatkov, na primer za zdravstvene podatke, in zaščite informacijskih sistemov, ki se soočajo s čedalje več grožnjami. Šifriranje od konca do konca (od pošiljatelja do prejemnika) je tudi edini način za zagotovitev popolnega varstva podatkov med prenosom. Vsakršen poskus oslavitve šifriranja, tudi za namene, kot

je državna varnost, bi popolnoma izničil te zaščitne mehanizme zaradi njihove morebitne nezakonite uporabe. Šifriranje mora ostati standardizirano, močno in učinkovito³.

Nova uredba mora uveljaviti zahtevo po privolitvi za piškotke in podobne tehnologije ter ponudnikom storitev zagotavljati tehnična orodja, ki omogočajo, da pridobijo tako privolitev preprosto (člen 8⁴)

Pri rešitvah „vse ali nič“ je potreben pristop, ki ohranja zasebnost

Opozoriti je treba, da se v okviru pravil e-zasebnosti uporabljajo določbe o privolitvi na podlagi Splošne uredbe o varstvu podatkov. Zato Evropski odbor za varstvo podatkov meni, da bi morala obveznost pridobitve pristne prostovoljne privolitve ponudnikom storitev preprečiti, da bi uporabljali nepošteno prakse, kot so rešitve „vse ali nič“, ki pogojujejo dostop do storitev in funkcij s privolitvijo uporabnika v shranjevanje podatkov ali pridobitev dostopa do informacij, ki so že shranjene na terminalski opremi uporabnika (tako imenovani zidovi piškotkov).⁵

Evropski odbor za varstvo podatkov poudarja, da je treba v uredbo o e-zasebnosti vključiti izrecno določbo za vključitev te prepovedi, da bi uporabnikom omogočili sprejetje ali zavrnitev oblikovanja profilov. Uporabnikom bi bilo zato treba predlagati pošteno alternative, ki jih ponujajo isti ponudniki storitev. Ta načela bi se morala uporabljati enako za vse ponudnike storitev, ne glede na njihov sektor dejavnosti ali njihov sedanji model financiranja (glej uvodno izjavo 21aa stališča Sveta).

Merjenje občinstva mora biti omejeno na nevsiljive prakse, za katere ni verjetno, da bi povzročile tveganja za zasebnost uporabnikov

Stališče Sveta uvaja novo izjemo za merjenje občinstva, kot je predlagala Delovna skupina iz člena 29⁶. Vendar je odstopanje za merjenje občinstva, kot ga je predlagal Svet, preširoko in bi lahko privedlo do preširoke razlage tega, kaj bi lahko spadalo v področje uporabe odstopanja, in posledično znižalo raven varstva terminalske opreme končnih uporabnikov.

Zato Evropski odbor za varstvo podatkov poudarja, da bi moralo biti odstopanje za merjenje občinstva omejeno le na stopnjo analize, ki je potrebna za analiziranje uspešnosti zagotavljanja storitve, ki jo zahteva uporabnik, in bi moralo biti omejeno le na zagotavljanje statističnih podatkov izvajalcu storitev, vzpostaviti pa ga mora izvajalec ali njegovi obdelovalci. Zato to dejanje obdelave samo po sebi ali v kombinaciji z drugimi rešitvami sledenja ne more povzročiti določanja ali oblikovanja profilov uporabnikov s strani ponudnika ali drugih upravljavcev podatkov. Poleg tega storitev merjenja občinstva ne bi smela omogočati zbiranja navigacijskih informacij, povezanih z uporabniki, na različnih spletiščih oziroma aplikacijah in bi morala vključevati uporabniku prijazen mehanizem za zavrnitev vsakršnega zbiranja podatkov.

Učinkovit način za pridobitev soglasja za spletišča in mobilne aplikacije (člen 4a)

³ Izjava Delovne skupine iz člena 29 o šifriranju in njegovem vplivu na varstvo posameznikov pri obdelavi njihovih osebnih podatkov v EU, 11. april 2018, je na voljo na: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.

⁴ Ter z njim povezani uvodni izjavi (20aaaa in 21aa stališča Sveta).

⁵ Kot je Evropski odbor za varstvo podatkov že navedel v Izjavi o spremembi uredbe o e-zasebnosti, sprejeti 25. maja 2018, ki je na voljo na: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_sl.pdf, in Smernicah št. 05/2019 o privolitvi na podlagi Uredbe 2016/679, odstavek 39, ki so na voljo na: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_sl.pdf.

⁶ Glej tudi Mnenje št. 04/2012 o piškotkih, ki so izvzeti iz zahteve po soglasju (WP 194), str. 10. Na voljo na spletnem naslovu: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_sl.pdf.

Evropski odbor za varstvo podatkov meni, da bi morala uredba o e-zasebnosti izboljšati sedanje stanje, in sicer tako, da bi uporabnikom vrnila nadzor in odpravila „prenasičenost s privolitvami“. Člen 4a bi moral iti dlje ter od brskalnikov in operacijskih sistemov zahtevati, da vzpostavijo uporabniku prijazen in učinkovit mehanizem, ki upravljavcem omogoča pridobitev privolitve, da se ustvarijo enotni pogoji za vse akterje. Področje uporabe uredbe bi moralo izrecno vključevati tudi ponudnike brskalnikov in operacijskih sistemov.

Nastavitve zasebnosti bi morale ohraniti pravico do varstva osebnih podatkov in privzeto celovitost terminalske opreme uporabnikov ter olajšati izražanje in preklic privolitve na preprost, zavezujoč in izvršljiv način za vse strani.

Nadaljnja obdelava za namene združljivosti (člena 6c in 8(1)(g))

Glede tekočih razprav o nadaljnji obdelavi elektronskih komunikacijskih metapodatkov oziroma podatkov, zbranih s piškotki in podobnimi tehnologijami, Evropski odbor za varstvo podatkov vnovič izraža podporo pristopu iz uredbe o e-zasebnosti, kot ga je prvotno predlagala Evropska komisija in ki mu je sledil Evropski parlament. Pristop temelji na splošni prepovedi, ki ji sledijo redke izjeme in uporaba privolitve. Nadaljnja obdelava za združljive namene pomeni tveganje oslabitve varstva, ki ga zagotavlja uredba o e-zasebnosti, zlasti za obdelavo elektronskih komunikacijskih metapodatkov, in sicer z omogočanjem obdelave za kateri koli namen, za katerega ponudnik storitev meni, da izpolnjuje klavzulo o „združljivosti“, zakonodajalec pa je nedvoumno želel omejiti njeno uporabo na posebne namene brez privolitve. Evropski odbor za varstvo podatkov želi poudariti, da se lahko ti podatki še naprej nadalje obdelujejo brez privolitve in brez tveganja za uporabnike, potem ko so bili anonimizirani.

Prihodnja vloga nadzornih organov, Evropskega odbora za varstvo podatkov in mehanizma sodelovanja (členi 18 do 20)

Evropski odbor za varstvo podatkov poudarja, da je za zagotovitev enotnih pogojev delovanja na enotnem digitalnem trgu bistveno zagotoviti, da se vse določbe o obdelavi podatkov iz uredbe o e-zasebnosti usklajeno razlagajo in izvršujejo v vsej EU.

Nadzor nad določbami o zasebnosti iz uredbe o e-zasebnosti bi bilo treba zaupati pristojnim nadzornim organom na podlagi Splošne uredbe o varstvu podatkov, da se dodatno podpre doslednost

Evropski odbor za varstvo podatkov opozarja na jasno medsebojno povezanost pristojnosti med nacionalnimi organi, pristojnimi na podlagi zdajšnje Direktive o zasebnosti in elektronskih komunikacijah, ter organi za varstvo podatkov. Določbe prihodnje uredbe o e-zasebnosti, ki se nanašajo na varstvo zasebnosti, se ne bi smele uporabljati ločeno, saj so tesno povezane z obdelavo osebnih podatkov in Splošno uredbo o varstvu podatkov.

Zato bi bilo treba za uskladitev visoke ravni varstva osebnih podatkov ter pravne in postopkovne varnosti nacionalnim organom, pristojnim za izvrševanje Splošne uredbe o varstvu podatkov, zaupati nadzor nad določbami prihodnje uredbe o e-zasebnosti glede obdelave osebnih podatkov, kot je prvotno predlagala Evropska komisija⁷.

⁷ Predlog Evropske komisije za uredbo Evropskega parlamenta in Sveta o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES (uredba o zasebnosti in elektronskih komunikacijah) z dne 10. januarja 2017, na voljo na: <https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A52017PC0010>, in povezano mnenje Delovne skupine iz člena 29, na voljo na: https://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

Evropski odbor za varstvo podatkov ugotavlja, da so, v nasprotju s prvotnim predlogom Evropske komisije, vsa sklicevanja na mehanizem sodelovanja in skladnosti iz poglavja VII Splošne uredbe o varstvu podatkov, črtana iz stališča Sveta. Iz zgoraj navedenih razlogov Evropski odbor za varstvo podatkov vnovič poudarja, da bi le popolna uskladitev z okvirom za sodelovanje in skladnost iz Splošne uredbe o varstvu podatkov omogočila, da bi uredba o e-zasebnosti dosegla svoje cilje, preprečila razdrobljenost pri njenem izvrševanju in uporabi ter zmanjšala breme za ponudnike, ki bi se morali morda obrniti na več kot 27 nadzornih organov.

Če bi morali nacionalni pristojni organi, ki niso člani Evropskega odbora za varstvo podatkov, tega kontaktirati, kot je trenutno predvideno v stališču Sveta, bi se njihova zmožnost pravočasnega prispevanja k dosledni uporabi uredbe o e-zasebnosti zmanjšala v škodo digitalnega gospodarstva in varstva temeljnih pravic.

Za Evropski odbor za varstvo podatkov

Predsednica

(Andrea Jelinek)

PRILOGA Seznam prejšnjih dokumentov, ki sta jih pripravila Evropski odbor za varstvo podatkov in Delovna skupina iz člena 29

-) Mnenje št. 1/2009 o predlogih sprememb Direktive 2002/58/ES o zasebnosti in elektronskih komunikacijah (direktiva o zasebnosti in elektronskih komunikacijah) je na voljo na: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp159_sl.pdf.
-) Mnenje št. 04/2012 o piškotkih, ki so izvzeti iz zahteve po soglasju (WP 194), je na voljo na: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_sl.pdf.
-) Mnenje št. 03/2016 o oceni in pregledu Direktive o zasebnosti in elektronskih komunikacijah (2002/58/ES) (WP 240) je na voljo na: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=645254.
-) Mnenje Delovne skupine iz člena 29 o predlogu uredbe Evropskega parlamenta in Sveta o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES (uredba o zasebnosti in elektronskih komunikacijah) je na voljo na: https://ec.europa.eu/newsroom/document.cfm?doc_id=44103.
-) Izjava Delovne skupine iz člena 29 o šifriranju in njegovem vplivu na varstvo posameznikov pri obdelavi njihovih osebnih podatkov v EU, z dne 11. aprila 2018, je na voljo na: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.
-) Izjava Evropskega odbora za varstvo podatkov o spremembi uredbe o e-zasebnosti in njenem učinku na varstvo posameznikov glede zasebnosti in zaupnosti njihovih komunikacij, sprejeta 25. maja 2018, je na voljo na: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_sl.pdf.
-) Izjava Evropskega odbora za varstvo podatkov št. 3/2019 glede uredbe o e-zasebnosti, sprejeta 13. marca 2019, je na voljo na: https://edpb.europa.eu/sites/edpb/files/files/file1/201903_edpb_statement_eprivacyregulation_sl_0.pdf.
-) Izjava Evropskega odbora za varstvo podatkov o uredbi o e-zasebnosti ter vlogi nadzornih organov in Evropskega odbora za varstvo podatkov v prihodnje, sprejeta 19. novembra 2020, je na voljo na: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-eprivacy-regulation-and-future-role-supervisory_sl.