EUROPSKI NADZORNIK ZAŠTITE PODATAKA

Sažetak Mišljenja Europskog nadzornika za zaštitu podataka (EDPS) o prijedlogu Uredbe o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ

(Cjeloviti tekst ovog mišljenja dostupan je na engleskom, francuskom i njemačkom jeziku na portalu Europskog nadzornika za zaštitu podataka www.edps.europa.eu)

(2017/C 164/02)

Europska unija uvodi novu generaciju standarda za zaštitu podataka. Donošenje Opće uredbe o zaštiti podataka (GDPR) i Direktive za policijski i pravosudni sektor prije gotovo godinu dana predstavlja dosad najambiciozniji napor zakonodavca EU-a u pogledu osiguranja temeljnih prava pojedinca u digitalnom dobu. Sada je vrijeme da institucije EU-a vode primjerom u pogledu pravila koja same primjenjuju kao voditelji i izvršitelji obrade podataka. Tijekom posljednjih 18 mjeseci EDPS je pokrenuo dijalog s institucijama EU-a na najvišoj razini kako bi ih pripremio za nove izazove oko usklađenosti u području zaštite podataka, pritom naglašavajući novo načelo odgovornosti za način na koji se podatci obrađuju. Ovim Mišljenjem EDPS nastoji upotrijebiti svojih 12 godina iskustva u nezavisnom nadzoru, pružanju savjeta u pogledu politike i aktivnostima aktivnog predlaganja poboljšanja predložene Uredbe o obradi osobnih podataka u institucijama i tijelima EU-a.

Uredba 45/2001 bila je osnova jer je uvela izravno primjenjive obveze za voditelje obrade podataka, prava ispitanika i nezavisno nadzorno tijelo. EU sada mora osigurati dosljednost s GDPR-om naglašavanjem odgovornosti i mjera zaštite pojedinaca umjesto procedura. Opravdane su neke razlike u pravilima primjenjivim na obradu podataka u institucijama EU-a, na isti način na koji su iznimke u javnom sektoru uključene u GDPR, ali te razlike moraju biti svedene na minimum.

Međutim, iz perspektive pojedinca ključno je da se zajednička načela u okviru EU-a za zaštitu podataka primjenjuju dosljedno neovisno o tome tko je voditelj obrade podataka. Ključno je i da se cijeli okvir primijeni istovremeno, u svibnju 2018., što je rok za potpunu primjenu GDPR-a.

Komisija je konzultirala EDPS o prijedlogu nacrta u skladu s dugogodišnjim dogovorom između naših institucija. Smatramo da je Komisija ostvarila dobru sveukupnu ravnotežu između različitih interesa. Mišljenje utvrđuje nekoliko područja u kojima se prijedlog može dodatno poboljšati. Zalažemo se za poboljšanja predložene uredbe, posebice dijela o ograničenju prava ispitanika i odredbe za institucije EU-a da koriste mehanizme certificiranja u određenim prilikama. S obzirom na naše zadatke i ovlasti kao nezavisnog tijela, izgleda da uredba postiže razumnu ravnotežu i odražava normalne funkcije nezavisnog nadležnog tijela za zaštitu podataka u skladu s Poveljom o temeljnim pravima i kako je utvrđeno u nedavnoj sudskoj praksi Suda Europske unije, bilo da se radi o tijelu provedbe, osobi zaduženoj za pritužbe i savjetniku zakonodavca o politici zaštite podataka i privatnosti.

Podržavamo zakonodavca EU-a u što bržem postizanju sporazuma oko prijedloga kako bi se institucijama EU-a omogućilo razumno prijelazno razdoblje prije nego što nova Uredba postane primjenjiva.

1. UVOD I KONTEKST

1.1. Kontekst

1. Europska je komisija 10. siječnja 2017. donijela Prijedlog Uredbe Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ ([1]) („Prijedlog").

([1]) COM(2017) 8 final; 2017/0002 (COD) (later, "the Proposal").

2. Temeljno pravo zaštite osobnih podataka utvrđeno je u članku 8. Povelje Europske unije o temeljnim pravima („Povelja”) i članku 16. Ugovora o funkcioniranju Europske unije („TFEU”).

3. Europski nadzornik za zaštitu podataka („EDPS”) nezavisno je nadzorno tijelo odgovorno za to da se institucije, tijela, uredi i agencije („institucije EU-a”) pridržavaju zakona o zaštiti podataka prilikom obrade osobnih podataka ([2]). Zahtjev za nezavisnu kontrolu u sustavu EU-a za zaštitu podataka utvrđen je u primarnom pravu, u članku 16. stavku 2. (TFEU) i u članku 8. stavku 3. Povelje. Sud je dosljedno naglašavao da je nadzor koji provodi neovisno tijelo ključna sastavnica prava na zaštitu podataka i utvrdio je kriterije za takvu neovisnost ([3]). Nadzorno tijelo mora djelovati potpuno neovisno, što podrazumijeva ovlasti odlučivanja neovisne od bilo kojeg izravnog ili neizravnog utjecaja ([4]) i nepostojanje bilo kakve sumnje na pristranost ([5]).

4. Uredba (EZ) br. 45/2001 ([6]) („Uredba 45/2001”), nadopunjena Odlukom br. 1247/2002/EZ ([7]), glavni je pravni instrument primjenjiv na obradu osobnih podataka u institucijama EU-a.

5. Nakon završetka produljenih pregovora o novom okviru EU-a za zaštitu podataka 27. travnja 2016. – Opća uredba o zaštiti podataka („GDPR”) i Direktiva za policijski i pravosudni sektor – ovaj Prijedlog (uz prijedlog Komisije za Uredbu o privatnosti i elektroničkim komunikacijama („Uredba o e-privatnosti” ([8])) označavaju početak ključne faze u procesu dovršavanja ovog okvira EU-a za zaštitu podataka. Njegov je cilj uskladiti odredbe Uredbe 45/2001 s pravilima utvrđenim u GDPR-u kako bi se stvorio snažniji i koherentniji okvir za zaštitu podataka u Uniji i kako bi se omogućila istovremena primjena oba instrumenta ([9]). Osim toga, Prijedlog također sadrži nova pravila za zaštitu opreme terminala krajnjih korisnika, koja su utvrđena u prijedlogu Komisije za novu Uredbu o e-privatnosti.

6. U Strategiji 2015.–2019., EDPS se obvezao na suradnju s Europskim parlamentom, Vijećem i Komisijom kako bi osigurao da se trenutačna pravila uspostavljena u Uredbi 45/2001 usklade s GDPR-om i da revidirani okvir stupi na snagu najkasnije početkom 2018. EDPS pozdravlja to što se Komisija neslužbeno savjetovala s njime prije donošenja Prijedloga i to što prijedlog sadrži brojne elemente koje je istaknuo u svojim dosadašnjim neslužbenim doprinosima. Iz perspektive maksimalnog usklađivanja s GDPR-om EDPS smatra da je trenutačni Prijedlog i više nego zadovoljavajući, osim ako usko definirane specifičnosti javnog sektora EU-a ne budu zahtijevale drukčiji prijedlog, a posebno ga se dojmila ravnoteža koju je Komisija ostvarila između različitih interesa.

7. Iako ovo Mišljenje ukazuje na područja u kojima se prijedlog može dodatno poboljšati, EDPS podržava zakonodavca EU-a u što bržem postizanju dogovora o Prijedlogu kako bi se institucijama EU-a omogućilo razumno prijelazno razdoblje prije nego što nova Uredba postane potpuno primjenjiva.

1.2. **Ciljevi Prijedloga i vremenski okvir**

8. U prošlosti je EDPS preporučio da se materijalna pravila za institucije EU-a uvrste u (tadašnji) nacrt GDPR-a ([10]). Zakonodavac EU-a odabrao je drugu opciju: zaseban pravni instrument koji je primjenjiv na institucije EU-a sukladne s GDPR-om i primjenjive istovremeno kad i GDPR. EDPS podržava ovaj pristup: bilo bi neprihvatljivo da

([2]) Article 286 EC rendered the (then) Community rules on data protection applicable to EU institutions and bodies and mandated the creation of a dedicated independent supervisory authority (later, the EDPS).
([3]) Case C-518/07 *Commission v Germany*, EU:C:2010:125; Case C-614/10 *Commission v Austria*, EU:C:2012:631; Case C-288/12 *Commission v Hungary*, EU:C:2014:237; Case C-362/14 *Maximilian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650.
([4]) Case C-518/07 *Commission v Germany*, *supra* para. 19.
([5]) Case C-288/12 *Commission v Hungary*, *supra* para. 53.
([6]) See *supra* note 3.
([7]) Decision No 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data Protection Supervisor's duties (OJ L 183, 12.7.2002, p. 1).
([8]) Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, 2017/0003 (COD).
([9]) See Article 98 and recital 17 of the GDPR.
([10]) See e.g. the EDPS Opinion of 7 March 2012 on the data protection reform package (OJ C 192, 30.6.2012, p. 7).

Europska komisija i ostale institucije EU-a nisu obvezane pravilima koja su ekvivalentna onima koja će uskoro postati primjenjiva na razini država članica. Štoviše, bilo bi nepoželjno da EDPS nadzire usklađivanje institucija EU-a s materijalnim pravilima koja bi bila inferiorna pravilima koja nadziru slična tijela na nacionalnoj razini, osobito jer će EDPS biti član Europskog odbora za zaštitu podataka („EDPB-a") ([11]).

9. Buduća pravila primjenjiva na obradu osobnih podataka u institucijama EU-a trebaju stoga biti usklađena s odredbama GDPR-a, osim ako usko utvrđene specifičnosti javnog sektora EU-a ne budu opravdavala drukčija pravila. U tom pogledu, EDPS pozdravlja uvodnu izjavu 5. Prijedloga u kojoj se naglašava potreba za najvećim mogućim usklađivanjem te pojašnjava „kad god se odredbe ove Uredbe temelje na istom konceptu kao odredbe [GDPR-a], te dvije odredbe trebaju se protumačiti homogeno, osobito jer se shema ove Uredbe treba shvatiti kao ekvivalent sheme [GDPR-a]."

10. Istovremeno, usklađivanje s GDPR-om ne može biti potpuno ni automatsko. GDPR uključuje brojne klauzule koje omogućuju državama članicama da zadrže ili uvedu posebno zakonodavstvo u određenim područjima, uključujući za državna tijela ([12]). U slučajevima kada GDPR navodi posebna pravila za državna tijela ([13]) ili ostavlja prostor za provedbu svojih odredbi u državama članicama, može se smatrati da Prijedlog ima sličnu ulogu kao nacionalni zakon kojim se „provodi" GDPR, kao primjerice u članku 9., „Prijenos osobnih podataka primateljima koji nisu institucije i tijela Unije" ili u članku 66. „Upravne novčane kazne" Prijedloga (pogledajte odjeljak 2.8.1. u nastavku). Osim toga, važno je osigurati zadržavanje visoke razine zaštite koja se trenutačno primjenjuje na institucije EU-a. Stoga je potrebno zadržati neke specifičnosti Uredbe 45/2001, kao u članku 25. Ograničenja (pogledajte odjeljak 2.3.1. u nastavku) i članku 44. Imenovanje službenika za zaštitu podataka (pogledajte odjeljak 2.4.5.1 u nastavku).

11. Osim materijalnog usklađivanja s GDPR-om nužno je da revidirana pravila postanu potpuno primjenjiva istovremeno kad i GDPR, odnosno 25. svibnja 2018. Postojeća mreža službenika za zaštitu podataka („DPO") predstavlja učinkovit kanal za razmjenu informacija i suradnju. Posljedično, EDPS smatra da se usklađivanje može ostvariti u relativno kratkom prijelaznom razdoblju, npr. u tri mjeseca.

12. Načelo odgovornosti na kojem se temelji GDPR – kao i ovaj Prijedlog – podrazumijeva mnogo više od jednostavnog usklađivanja s pravilima i podrazumijeva promjenu kulture. Kako bi se olakšao prijelaz, EDPS je pokrenuo „projekt odgovornosti". U tu svrhu EDPS je bio u kontaktu sa sedam ključnih institucija i tijela EU-a tijekom 2016. i 2017. kako bi se na vrijeme pripremio za primjenu GDPR-a.

1.3. **Područje primjene i odnos s drugim pravnim instrumentima**

13. EDPS je u nekoliko navrata u prošlosti pozvao Komisiju da predloži velik i *sveobuhvatan* sustav koji bi bio ambiciozan i poboljšao učinkovitost i *koherentnost* zaštite podataka u EU-u, kako bi se osigurali dobri uvjeti za daljnji razvoj u nadolazećim godinama ([14]). Komisija je odabrala drukčiji pristup i predložila zaseban pravni instrument za zaštitu podataka u području provedbe zakona ([15]). Uslijedili su brojni prijedlozi za pravne akte koji uvode zasebne „samostalne" režime zaštite podataka ([16]).

([11]) EDPS Opinion of 7 March 2012 on the data protection reform package, p. 6.

([12]) See in particular Article 6(3) and recital 10 to the GDPR: "Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful."

([13]) E.g. last sentence of Article 6(1), Article 20(5), Article 27, Article 37, Article 41 or Article 46(2)(a) of the GDPR.

([14]) See in particular the EDPS Opinion of 14 January 2011 on the Communication "A comprehensive approach on personal data in the European Union" (OJ L 181, 22.6.2011, p. 1).

([15]) See *supra* note 5.

([16]) Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, COM(2013) 173 final, now adopted as Regulation 2016/794 and published in OJ L 135, 24.5.2016, p. 53; Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office, COM(2013) 534 final. See also the Council General approach (First reading) on the Proposal for a Regulation on the European Union Agency for Criminal Justice Cooperation (Eurojust) available at: http://data.consilium.europa.eu/doc/document/ST-6643-2015-INIT/en/pdf

14. EDPS priznaje da je trenutačni zakonski okvir za zaštitu osobnih podataka, iako je fragmentiran, najbolji ishod koji se danas može ostvariti ([17]). EDPS razumije da će se ovaj Prijedlog nastaviti primjenjivati na one institucije EU-a koje danas spadaju u područje primjene Uredbe 45/2001 ([18]) (u načelu, sve institucije, tijela, uredi i agencije prijašnjeg prvog ili drugog „stupa" ([19])), ali neće kao takav utjecati na postojeće „samostalne" režime ili one koji su na čekanju ([20]). Takvi režimi bit će pod utjecajem ovog prijedloga samo ako i do mjere do koje je to izričito određeno u relevantnom pravnom instrumentu. EDPS je upoznat s ovim pristupom, ali sugerira da je ovo jasnije navedeno u preambuli Prijedloga i, moguće, u njegovom članku 2. *Područje primjene*. Istovremeno, EDPS naglašava da fragmentacija i sve veća složenost pravnog okvira za obradu podataka u različitim institucijama EU-a aktivnim u prijašnjim prvim i trećim „stupovima" nije potpuno zadovoljavajući ishod te da će zakonodavac EU-a možda trebati riješiti to pitanje srednjoročno.

15. Uredba 45/2001 utvrđuje mjere koje za cilj imaju zaštitu privatnosti i povjerljivosti komunikacija u slučajevima kada institucije EU-a nadziru infrastrukturu koja se upotrebljava za komunikaciju. S tim ciljem uredba uključuje neke odredbe koje pokrivaju dijelove regulatornog opsega Direktive 2002/58/EZ („Direktiva o e-privatnosti") ([21]) i utemeljuje načelo da se pravila za zaštitu temeljenih prava trebaju primijeniti na dosljedan i skladan način u cijeloj Uniji, pozivajući se na relevantne instrumente poput Direktive o privatnosti i elektroničkim komunikacijama ([22]). Potreba za osiguranjem jednake razine privatnosti i povjerljivosti komunikacija koje uključuju institucije EU-a ostaje neizmijenjena i iz tog se razloga načelo dosljednosti i usklađene primjene treba zadržati. EDPS stoga smatra da bi ovaj Prijedlog trebao osigurati da se relevantna pravila GDPR-a i buduća Uredba o e-privatnosti primjenjuju na institucije EU-a *mutatis mutandis*. Navedeno treba uključivati očuvanje povjerljivosti i privatnosti s obzirom na komunikacijske usluge koje kontroliraju institucije EU-a, kao i druga načela buduće Uredbe o e-privatnosti, poput zaštite uređaja terminala i druga pravila, npr. o praćenju i neželjenoj elektroničkoj pošti.

16. Na kraju, dok se zakonodavstvo EU-a o zaštiti podataka također primjenjuje na Europski gospodarski prostor i države koje sudjeluju u EFTA-i moraju osnovati nezavisna tijela za nadzor prema GDPR-u, institucije EFTA-e nisu podložne nikakvim posebnim pravilima ni nadzoru u pogledu zaštite podataka iako razmjenjuju osobne podatke s institucijama EU-a. EDPS smatra da bi ovaj Prijedlog mogao biti prilika za rješavanje navedenog pitanja.

3. **ZAKLJUČCI**

90. Općenito, EDPS smatra da je Prijedlog uspješan u usklađivanju pravila za institucije EU-a s GDPR-om, uzimajući pritom u obzir specifičnosti javnog sektora EU-a. Visoka razina zaštite po pitanju obrade podataka u institucijama EU-a sačuvana je u Prijedlogu. EDPS osobito cijeni ravnotežu koju je Komisija postigla između različitih interesa.

91. EDPS smatra da se Prijedlog još treba poboljšati, ponajviše modaliteti za ograničenja pod člankom 25. Kako bi se osiguralo usklađivanje s prethodno navedenim zahtjevima o kvaliteti prava, članak 25. podstavak 1. Prijedloga treba se izmijeniti tako da se samo pravnim aktima usvojenim na temelju Ugovora smiju ograničiti temeljna prava, namećući na taj način institucijama EU-a iste standarde koji bi bili primjenjivi na države članice prema GDPR-u. Do mjere u kojoj se razmatraju ograničenja članka 34. *Povjerljivost elektroničkih komunikacija*, EDPS poziva zakonodavca EU-a da osigura da moguća ograničenja temeljnog prava na privatnost komunikacija u institucijama EU-a u njihovim vlastitim operacijama prate iste standarde koji su utvrđeni u zakonu Unije na način na koji to tumači Sud u ovoj domeni.

92. EDPS pozdravlja činjenicu da Prijedlog dodjeljuje zaseban članak ulozi EDPS-a kao savjetniku institucija EU-a (članak 42. Prijedloga). Međutim, zabrinut je da tekst „[n]akon donošenja prijedloga" (naspram „[k]ada usvaja zakonski prijedlog" u članku 28. stavku 2. Uredbe 45/2001) može dovesti u pitanje dugotrajnu obvezu Europske

([17]) EDPS Opinion 3/2015 "Europe's big opportunity - EDPS recommendations on the EU's options for data protection reform", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-10-09_GDPR_with_addendum_EN.pdf

([18]) See the list of EU institutions and bodies available at: http://publications.europa.eu/code/en/en-390500.htm.

([19]) Regulation 45/2001 already today applies to, *inter alia*, the European Defence Agency, European Union Institute for Security Studies, and the European Union Satellite Centre.

([20]) Europol, Eurojust, EPPO, *supra* note 21.

([21]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications (OJ L 201, 31.7.2002, p. 37), as amended (later, "the ePrivacy Directive").

([22]) Recitals 10-12 ePrivacy Directive.

komisije za neslužbeno savjetovanje s EDPS-om o nacrtima prijedloga, obično u fazi savjetovanja između službi. S obzirom na važnost neslužbenog savjetovanja, EDPS bi pozdravio uvodnu izjavu u kojoj bi Komisija ponovila svoju posvećenost ovoj dugotrajnoj praksi. Također bi podržao to da se u Prijedlogu zadrži tekst iz članka 28. stavka 2. Uredbe 45/2001 („[k]ada usvaja") koji dopušta veći prostor za manevar. Smatra da se predloženim člankom 42. dovoljno objašnjavaju zadatci EDPS-a i EDPB-a kako bi se izbjeglo nepotrebno udvostručavanje u budućnosti.

93. EDPS smatra da mogućnost izdvajanja funkcije službenika za zaštitu podataka nije prikladna za institucije EU-a koje obavljaju javne ovlasti. Posljedično, druga alternativa članka 44. stavka 4. („ili obavljati zadaće na temelju ugovora o djelu") treba se izbrisati.

94. EDPS pozdravlja članak 66. Prijedloga kojim se EDPS-u daje ovlast određivanja upravnih novčanih kazni. Smatra da bi lišavanje nadzornog tijela EU-a ovlasti za određivanje upravnih novčanih kazni, gdje je prikladno, rezultiralo privilegiranom pozicijom institucija EU-a u usporedbi s institucijama državnog sektora u mnogim državama članicama.

95. EDPS smatra da mehanizmi certificiranja mogu biti veoma koristan instrument za institucije EU-a i već se upotrebljavaju u određenim situacijama, npr. pri potvrđivanju usklađivanja s općeprihvaćenim standardima. Reference na upotrebu certificiranja (ali ne kodeksi ponašanja) trebaju se dodati članku 26. *Obveze voditelja obrade podataka*, članku 27. *Tehnička i integrirana zaštita podataka* kao i članku 33. *Sigurnost*.

96. Iako se u ovom Mišljenju navode područja u kojima se prijedlog može dodatno poboljšati, EDPS bi podržao zakonodavca EU-a u postizanju što bržeg dogovora o Prijedlogu kako bi se institucijama EU-a omogućilo razumno prijelazno razdoblje prije nego što nova Uredba postane primjenjiva istovremeno kad i GDPR, u svibnju 2018.

U Bruxellesu 15. ožujka 2017.

Giovanni BUTTARELLI

Europski nadzornik za zaštitu podataka