EUROPSKA
KOMISIJA

Bruxelles, 24.6.2020.
SWD(2020) 115 final

RADNI DOKUMENT SLUŽBI KOMISIJE

[…]

priložen dokumentu

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU

Pravila o zaštiti podataka kao jedan od stupova jačanja položaja građana i pristupa EU-a digitalnoj tranziciji – dvije godine primjene Opće uredbe o zaštiti podataka

{COM(2020) 264 final}

Sadržaj

1 KONTEKST

Opća uredba o zaštiti podataka[1] rezultat je osam godina pripremanja, izrade i međuinstitucijskih pregovora te je stupila na snagu 25. svibnja 2018. nakon dvogodišnjeg prijelaznog razdoblja (svibanj 2016.–svibanj 2018.). Člankom 97. Opće uredbe o zaštiti podataka od Komisije se zahtijeva da izvješćuje o evaluaciji i preispitivanju Uredbe, počevši s prvim izvješćem dvije godine nakon početka primjene te svake četiri godine nakon toga.

Ta je evaluacija dio višedimenzionalnoga pristupa koji je Komisija slijedila i prije početka primjene Opće uredbe o zaštiti podataka i koji je otad nastavila aktivno provoditi. U okviru tog pristupa Komisija se uključila u tekuće bilateralne dijaloge s državama članicama o usklađenosti nacionalnog zakonodavstva s Općom uredbom o zaštiti podataka te je svojim iskustvom i stručnim znanjem aktivno doprinijela radu Europskog odbora za zaštitu podataka (dalje u tekstu „Odbor"). Pružala je potporu tijelima za zaštitu podataka i održavala bliske kontakte sa širokim rasponom dionika u pogledu praktične primjene Uredbe.

Evaluacija se temelji na pregledu stanja koji je Komisija provela za prvu godinu primjene Opće uredbe o zaštiti podataka i čiji je sažetak iznesen u Komunikaciji objavljenoj u srpnju 2019.[2] Nastavlja se i na Komunikaciju o primjeni Opće uredbe o zaštiti podataka objavljenu u siječnju 2018.[3] Komisija je donijela i Smjernice o upotrebi osobnih podataka u kontekstu izbora objavljene u rujnu 2018. i Smjernice o aplikacijama kojima se podupire suzbijanje pandemije bolesti COVID-19 izdane u travnju 2020.

Bez obzira na to što je usredotočena na dva pitanja istaknuta u članku 97. stavku 2. Opće uredbe o zaštiti podataka, a to su međunarodni prijenosi te mehanizmi suradnje i konzistentnosti, evaluaciji se primjenjuje širi pristup kako bi se riješila i pitanja koja su tijekom posljednje dvije godine postavljali razni dionici.

Kako bi pripremila evaluaciju, Komisija je uzela u obzir:

- doprinose Vijeća[4],
- doprinose Europskog parlamenta (Odbora za građanske slobode, pravosuđe i unutarnje poslove)[5],

---

[1] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ – SL L 119, 4.5.2016., str. 1.–88.

[2] Komunikacija Komisije Europskom parlamentu i Vijeću, Pravila o zaštiti podataka kao katalizator povjerenja u EU-u i izvan njega – analiza napretka – COM(2019) 374 final, 24.7.2019.

[3] Komunikacija Komisije Europskom parlamentu i Vijeću: Veća zaštita i nove prilike – Komisija daje smjernice za izravnu primjenu Opće uredbe o zaštiti podataka od 25. svibnja 2018., COM/2018/043 final.

[4] Stajalište Vijeća i zaključci o primjeni Opće uredbe o zaštiti podataka – 14994/2/19 Rev2, 15.1.2020.: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/hr/pdf

[5] Pismo Odbora LIBE Europskog parlamenta od 21. veljače 2020. povjereniku Reyndersu, Ref.: IPOL-COM-LIBE D (2020)6525.

- doprinose Odbora[6] i pojedinačnih tijela za zaštitu podataka[7], na temelju upitnika koji je poslala Komisija,
- povratne informacije članova stručne skupine s više dionika za potporu primjeni Opće uredbe o zaštiti podataka[8], također na temelju upitnika koji je poslala Komisija,
- i *ad hoc* doprinose dionika.

2 PROVEDBA OPĆE UREDBE O ZAŠTITI PODATAKA I FUNKCIONIRANJE MEHANIZAMA SURADNJE I KONZISTENTNOSTI

Općom uredbom o zaštiti podataka uspostavljen je inovativni sustav upravljanja i stvoren je temelj istinske europske kulture zaštite podataka čiji je cilj osigurati ne samo usklađeno tumačenje nego i usklađenu primjenu i provedbu pravila o zaštiti podataka. Neovisna nacionalna tijela za zaštitu podataka i novoosnovani Odbor njegovi su stupovi.

Budući da su tijela za zaštitu podataka ključna za funkcioniranje cijelog sustava EU-a za zaštitu podataka, Komisija pozorno prati njihovu stvarnu neovisnost, među ostalim u pogledu odgovarajućih financijskih, ljudskih i tehničkih resursa.

S obzirom na kratkoću dosadašnjeg iskustva[9], još je prerano da bi se funkcioniranje mehanizama suradnje i konzistentnosti moglo u potpunosti ocijeniti. Osim toga, tijela za zaštitu podataka još nisu u potpunosti iskoristila instrumente predviđene Općom uredbom o zaštiti podataka kako bi dodatno ojačala svoju suradnju.

2.1 Primjena pojačanih ovlasti tijela za zaštitu podataka

Općom uredbom o zaštiti podataka uspostavljaju se neovisna tijela za zaštitu podataka te im se daju usklađene i pojačane provedbene ovlasti. Od početka primjene Opće uredbe o zaštiti podataka ta se tijela koriste širokim rasponom korektivnih ovlasti koje su njome predviđene, kao što su upravne novčane kazne (22 tijela EU-a/EGP-a)[10], upozorenja i službene opomene (23), naredbe da se poštuju zahtjevi ispitanika (26), naredbe za usklađivanje postupaka obrade s Općom uredbom o zaštiti podataka (27) te naredbe za ispravljanje, brisanje ili ograničavanje obrade osobnih podataka (17).

---

6 Doprinos Odbora evaluaciji Opće uredbe o zaštiti podataka u skladu s člankom 97., donesen 18. veljače 2020.: https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_hr

7 https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en

8 Stručna skupina s više dionika za Opću uredbu o zaštiti podataka koju je osnovala Komisija uključuje predstavnike civilnog društva i trgovačkih društava, članove akademske zajednice i stručnjake: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537 Izvješće skupine s više dionika dostupno je na: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=21356

9 Tu činjenicu posebno ističe i Vijeće u svojem stajalištu i zaključcima o primjeni Opće uredbe o zaštiti podataka, a Odbor u svojem doprinosu evaluaciji.

10 Brojke u zagradama pokazuju broj tijela za zaštitu podataka EU-a/EGP-a koja su se koristila navedenim ovlastima u razdoblju od svibnja 2018. do kraja studenoga 2019. Vidjeti doprinos Odbora na stranicama 32.–33.

Otprilike polovina tijela za zaštitu podataka (13) uvela je privremena ili konačna ograničenja obrade, uključujući zabrane. Time se pokazuje svjesna primjena svih korektivnih mjera predviđenih Općom uredbom o zaštiti podataka; tijela za zaštitu podataka nisu se ustručavala izricati upravne novčane kazne uz druge korektivne mjere ili umjesto njih, ovisno o okolnostima pojedinačnih slučajeva.

Upravne novčane kazne:

Od 25. svibnja 2018. do. 30. studenoga 2019. 22 tijela za zaštitu podataka EU-a/EGP-a izrekla su približno 785 novčanih kazni. Samo nekoliko tijela još nije izreklo upravne novčane kazne, iako bi postupci koji su u tijeku mogli dovesti do izricanja takvih kazni. Većina novčanih kazni odnosila se na povrede: načela zakonitosti, valjane privole, zaštite osjetljivih podataka, obveze transparentnosti i prava ispitanikâ te na povrede podataka.

Primjeri novčanih kazni koje izriču tijela za zaštitu podataka uključuju[11]:

- 200 000 EUR zbog nepoštovanja prava na podnošenje prigovora na izravni marketing u Grčkoj,
- 220 000 EUR društvu za posredovanje podacima u Poljskoj zbog neobavješćivanja pojedinaca o obradi njihovih podataka,
- 250 000 EUR španjolskoj nogometnoj ligi LaLiga zbog nedostatka transparentnosti u izradi aplikacije za pametni telefon,
- 14,5 milijuna EUR njemačkom društvu za poslovanje nekretninama zbog povrede načela zaštite podataka, posebno zbog nezakonite pohrane,
- 18 milijuna EUR za masovnu nezakonitu obradu posebnih kategorija podataka koju su provodile austrijske poštanske službe,
- 50 milijuna EUR Googleu u Francuskoj zbog uvjeta za dobivanje pristanka korisnika.

Uspjeh Opće uredbe o zaštiti podataka ne bi se trebao mjeriti brojem izrečenih novčanih kazni jer se njome predviđa šira paleta korektivnih ovlasti. Ovisno o okolnostima, odvraćajući učinak zabrane obrade ili suspenzija protoka podataka mogu biti mnogo jači.

Posebna pitanja za javni sektor

Općom uredbom o zaštiti podataka državama članicama omogućuje se da utvrde mogu li se tijelima javne vlasti i javnim tijelima izreći upravne novčane kazne i u kojoj mjeri. Ako države članice primjenjuju tu mogućnost, tijelima za zaštitu podataka ne uskraćuju se sve ostale korektivne ovlasti u pogledu tijela javne vlasti i javnih tijela[12].

Još jedno posebno pitanje jest nadzor sudova: iako se Opća uredba o zaštiti podataka primjenjuje i na aktivnosti sudova, izuzeti su od nadzora tijela za zaštitu podataka kada djeluju u sudbenom svojstvu. Međutim, države članice obvezuju se Poveljom i

[11] Neke odluke o izricanju novčanih kazni još podliježu sudskom preispitivanju.
[12] Članak 83. stavak 7. Opće uredbe o zaštiti podataka.

UFEU-om da u okviru svojih pravosudnih sustava povjere nadzor nad takvim postupcima obrade neovisnom tijelu[13].

Suradnja s drugim regulatornim tijelima

Kako je najavljeno u Komunikaciji iz srpnja 2019., Komisija podupire interakciju s drugim regulatornim tijelima, uz potpuno poštovanje njihovih nadležnosti. Obećavajuća područja suradnje uključuju područja zaštite potrošača i tržišnog natjecanja. Odbor je izrazio spremnost na suradnju s drugim regulatornim tijelima, posebno u pogledu koncentracije na digitalnim tržištima[14]. Komisija je prepoznala važnost privatnosti i zaštite podataka kao kvalitativnog parametra za tržišno natjecanje[15]. Članovi Odbora sudjelovali su s Mrežom za suradnju u području zaštite potrošača na zajedničkim radionicama o suradnji na boljoj provedbi zakonodavstva EU-a o zaštiti potrošača i zaštiti podataka. Taj će se pristup primjenjivati kako bi se potaknulo zajedničko razumijevanje i razvili praktični načini rješavanja konkretnih problema s kojima se susreću potrošači, posebno u digitalnom gospodarstvu.

Kako bi se osigurao dosljedan pristup privatnosti i zaštiti podataka te do donošenja Uredbe o e-privatnosti, nužna je bliska suradnja s tijelima nadležnima za provedbu Direktive o e-privatnosti[16], koja je *lex specialis* u području elektroničkih komunikacija. Bliža suradnja s tijelima nadležnima u skladu s Direktivom o sigurnosti mrežnih i informacijskih sustava[17] i skupinom za suradnju u području o sigurnosti mrežnih i informacijskih sustava bila bi od uzajamne koristi tim tijelima i tijelima za zaštitu podataka.

2.2 Mehanizmi suradnje i konzistentnosti

Općom uredbom o zaštiti podataka uspostavljen je mehanizam suradnje (jedinstveni sustav „sve na jednom mjestu” za subjekte, zajedničke operacije i uzajamnu pomoć među tijelima za zaštitu podataka) i mehanizam konzistentnosti kako bi se potaknula ujednačena primjena pravila o zaštiti podataka dosljednim tumačenjem i rješavanjem mogućih neslaganja između tijela za zaštitu podataka koje provodi Odbor.

Odbor, koji okuplja sva tijela za zaštitu podataka, osnovan je kao tijelo EU-a s pravnom osobnošću te je u potpunosti operativan, a njegov rad podupire tajništvo[18]. To je ključno za funkcioniranje dvaju prethodno navedenih mehanizama. Do kraja

---

[13] Članak 8. stavak 3. Povelje; članak 16. stavak 2. UFEU-a; uvodna izjava 20. Opće uredbe o zaštiti podataka.

[14] Usp. Izjavu Odbora o učincima koncentracije gospodarskih subjekata na zaštitu podataka, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_hr.pdf.

[15] Vidjeti predmet COMP M. 8124 Microsoft/LinkedIn.

[16] Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) – SL L 201, 31.7.2002., str. 37–47.

[17] Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije – SL L 194, 19.7.2016., str. 1.–30.

[18] Vidjeti pojedinosti o aktivnostima tajništva u doprinosu Odbora, stranice 24.–26.

2019. Odbor je donio 67 dokumenata, uključujući 10 novih smjernica[19] i 43 mišljenja[20] [21].

Odbor je dobio važnu ulogu kada je trebalo brzo osigurati dosljedno tumačenje Opće uredbe o zaštiti podataka i pronaći odmah primjenjiva rješenja na razini EU-a. Primjerice, u kontekstu izbijanja bolesti COVID-19, Odbor je u ožujku 2020. donio izjavu o obradi osobnih podataka koja se, među ostalim, odnosi na zakonitost obrade i upotrebu podataka o lokaciji u mobilnim mrežama u tom kontekstu[22], a u travnju 2020. donio je smjernice o obradi podataka koji se odnose na zdravlje u svrhu znanstvenog istraživanja u kontekstu izbijanja bolesti COVID-19[23] i smjernice o upotrebi podataka o lokaciji i alatima za praćenje kontakata u kontekstu pandemije bolesti COVID-19[24]. Odbor je znatno doprinio i osmišljavanju pristupa EU-a aplikacijama za praćenje koje provode Komisija i države članice.

Svakodnevna suradnja među tijelima za zaštitu podataka, bez obzira na to djeluju li u vlastito ime ili kao članovi Odbora, temelji se na razmjeni informacija i obavijesti o slučajevima koje su otvorila ta tijela. Kako bi se olakšala komunikacija među tijelima, Komisija im je pružila znatnu potporu osiguravši sustav za razmjenu informacija[25]. Većina tijela smatra da je taj sustav prilagođen potrebama mehanizama suradnje i konzistentnosti, iako bi se mogao dodatno prilagoditi, primjerice tako da ga se učini pristupačnijim korisnicima.

Iako se još uvijek nalazi u ranoj fazi, već je moguće utvrditi niz postignuća i izazova, koji se navode u nastavku. Iz njih je vidljivo da su se tijela za zaštitu podataka dosad učinkovito koristila alatima za suradnju, dajući prednost fleksibilnijim rješenjima.

Točka „sve na jednom mjestu”

Opće je pravilo da u prekograničnim slučajevima tijelo za zaštitu podataka države članice može biti uključeno i. kao vodeće tijelo kada je glavni poslovni nastan subjekta smješten u toj državi članici ili ii. kao predmetno tijelo kada subjekt ima poslovni nastan na području te države članice, ako to znatno utječe na pojedince u toj državi članici ili kada mu je podnesena pritužba.

Takva bliska suradnja postala je svakodnevna praksa: od početka primjene Opće uredbe o zaštiti podataka tijela za zaštitu podataka u svim državama članicama u

---

[19] Nove su smjernice dodatak za deset smjernica koje je Radna skupina iz članka 29. donijela uoči početka primjene Opće uredbe o zaštiti podataka i koje je potvrdio Odbor. Nadalje, Odbor je donio četiri dodatne smjernice između siječnja i kraja svibnja 2020. te ažurirao jednu postojeću.

[20] Od tih je mišljenja 42 doneseno u skladu s člankom 64. Opće uredbe o zaštiti podataka, a jedno je doneseno u skladu s člankom 70. stavkom 1. točkom (s) Opće uredbe o zaštiti podataka, a odnosilo se na odluku o primjerenosti u pogledu Japana.

[21] Za potpuni pregled aktivnosti Odbora vidjeti doprinos Odbora, stranice 18.–23.

[22] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

[23] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_hr

[24] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_hr.pdf

[25] Informacijski sustav unutarnjeg tržišta („IMI”).

nekom su trenutku definirana kao vodeća tijela ili kao predmetna tijela u prekograničnim predmetima, iako u različitoj mjeri.

Od svibnja 2018. do kraja 2019. tijelo za zaštitu podataka u Irskoj djelovalo je kao vodeće tijelo u najvećem broju prekograničnih predmeta (127), nakon čega slijede Njemačka (92), Luksemburg (87), Francuska (64) i Nizozemska (45). Taj poredak posebno odražava specifičnu situaciju u Irskoj i Luksemburgu, u kojima se nalazi nekoliko velikih multinacionalnih tehnoloških poduzeća.

Poredak se razlikuje u pogledu uključenosti u svojstvu predmetnih tijela za zaštitu podataka, pri čemu su tijela u Njemačkoj uključena u najveći broj slučajeva (435), nakon čega slijede Španjolska (337), Danska (327), Francuska (332) i Italija (306)[26].

Od 25. svibnja 2018. do 31. prosinca 2019. u okviru postupka „sve na jednom mjestu" podnesen je 141 nacrt odluka, od kojih je 79 rezultiralo konačnim odlukama. Na datum objave ovog izvješća očekuje se donošenje nekoliko važnih odluka s prekograničnom dimenzijom koje podliježu mehanizmu „sve na jednom mjestu". Neke od tih odluka uključuju velika multinacionalna tehnološka poduzeća[27]. Očekuje se da će se njima pružiti pojašnjenja i dati doprinos većoj usklađenosti tumačenja Opće uredbe o zaštiti podataka.

Uzajamna pomoć

Tijela za zaštitu podataka u velikoj su se mjeri koristila instrumentom uzajamne pomoći.

Do kraja 2019. provedeno je 115 postupaka uzajamne pomoći[28], posebno u vođenju istraga, od kojih su većinu provela tijela za zaštitu podataka Španjolske (26), Njemačke (20), Danske (13), Poljske (12) i Češke (10). S druge strane, najviše zahtjeva zaprimile su Irska (19), Francuska (11), Austrija (10), Njemačka (10) i Luksemburg (9)[29].

Većina tijela smatra da je uzajamna pomoć vrlo koristan instrument za suradnju i nisu naišla ni na kakvu posebnu prepreku u primjeni postupka uzajamne pomoći. Dobrovoljna razmjena uzajamne pomoći, za koju nije predviđen zakonski rok ili stroga dužnost odgovora, primjenjivala se češće, u 2 427 postupaka. Irsko tijelo za zaštitu podataka poslalo je i zaprimilo najveći broj zahtjeva za uzajamnu pomoć (527 poslanih i 359 zaprimljenih), nakon čega su slijedila njemačka tijela (260 poslanih i 356 zaprimljenih).

Nasuprot tome, još nisu provedene zajedničke operacije[30] kojima bi se omogućilo da tijela za zaštitu podataka nekoliko država članica budu uključena već na razini istrage

---

[26] Vidjeti doprinos Odbora, str. 8.

[27] Primjerice, 22. svibnja 2020. irsko tijelo za zaštitu podataka podnijelo je drugim predmetnim tijelima, u skladu s člankom 60. Uredbe, nacrt odluke o istrazi protiv društva Twitter International Company u vezi s izvješćivanjem o povredi podataka. Istoga je dana irsko tijelo za zaštitu podataka objavilo i da je nacrt odluke povezane s društvom WhatsApp Ireland Limited u pripremi za podnošenje u skladu s člankom 60. Navedena odluka odnosi se na transparentnost, među ostalim u pogledu informacija koje se razmjenjuju s Facebookom.

[28] Članak 61. Opće uredbe o zaštiti podataka.

[29] Vidjeti doprinos Odbora, stranice 12.–14.

[30] Članak 62. Opće uredbe o zaštiti podataka.

prekograničnih slučajeva. U Odboru se trenutačno razmatra praktična provedba tog instrumenta i promicanje njegove uporabe.

Mehanizam konzistentnosti

Dosad je upotrijebljen samo prvi dio mehanizma konzistentnosti, odnosno donošenje mišljenja Odbora[31]. S druge strane, rješavanje sporova na razini Odbora[32] ili hitni postupak[33] još nisu pokrenuti.

U razdoblju od 25. svibnja 2018. do 31. prosinca 2019. Odbor je dao 36 mišljenja u kontekstu mjera koje je donio neki od njegovih članova[34]. Većina (31) se odnosila na donošenje nacionalnih popisa postupaka obrade za koje je potrebna procjena učinka na zaštitu podataka. Dva su se mišljenja odnosila na obvezujuća korporativna pravila, druga dva odnosila su se na nacrt akreditacijskih zahtjeva za nadzorno tijelo za kodeks ponašanja, a jedno na standardne ugovorne klauzule[35].

Nadalje, Odbor je donio šest mišljenja na zahtjev[36]. Tri od tih šest mišljenja odnosila su se na nacionalne popise kojima se utvrđuje obrada za koju nije potrebna procjena učinka na zaštitu podataka. Ostala su se odnosila na administrativni dogovor o prijenosu osobnih podataka između financijskih nadzornih tijela država EGP-a i država izvan EGP-a, međudjelovanje Direktive o e-privatnosti i Opće uredbe o zaštiti podataka te nadležnost nadzornog tijela u slučaju promjene okolnosti povezanih s glavnim ili jedinim poslovnim nastanom[37].

Izazovi koje treba riješiti

Iako tijela za zaštitu podataka vrlo aktivno surađuju u Odboru i već se intenzivno koriste instrumentom za suradnju u obliku uzajamne pomoći, izgradnja istinske zajedničke kulture zaštite podataka proces je koji je i dalje u tijeku.

Konkretno, za rješavanje prekograničnih predmeta potreban je učinkovitiji i usklađeniji pristup te djelotvorna uporaba svih instrumenata suradnje predviđenih Općom uredbom o zaštiti podataka. Postoji vrlo širok konsenzus o tom pitanju jer su ga na različite načine iznijeli Europski parlament, Vijeće, Europski nadzornik za zaštitu podataka, dionici (u okviru skupine s više dionika i šire) i tijela za zaštitu podataka.

Glavna pitanja koja treba riješiti u tom kontekstu uključuju razlike u:

- nacionalnim upravnim postupcima koji se posebno odnose na: postupke za rješavanje pritužbi, kriterije dopuštenosti pritužbi, trajanje postupka zbog različitih rokova ili nepostojanja rokova, trenutak u postupku kada se odobrava pravo na saslušanje, informacije i uključenost podnositelja pritužbe tijekom postupka,
- tumačenjima pojmova povezanih s mehanizmom suradnje, kao što su relevantne informacije, pojam „bez odgode”, „pritužba”, dokument koji je definiran kao

[31] Na temelju članka 64. Opće uredbe o zaštiti podataka.
[32] Članak 65. Opće uredbe o zaštiti podataka.
[33] Članak 66. Opće uredbe o zaštiti podataka.
[34] U skladu s člankom 64. stavkom 1. Opće uredbe o zaštiti podataka.
[35] Članak 28. stavak 8. Opće uredbe o zaštiti podataka.
[36] U skladu s člankom 64. stavkom 2. Opće uredbe o zaštiti podataka.
[37] Vidjeti doprinos Odbora, str. 15.

„nacrt odluke" vodećeg tijela za zaštitu podataka, sporazumno rješenje (posebice postupak koji vodi do sporazumnog rješenja i pravni oblik rješenja), i

- pristupu u pogledu početka postupka suradnje, uključivanja predmetnih tijela za zaštitu podataka i priopćavanja informacija tim tijelima. Podnositeljima pritužbi nedostaju i pojašnjenja o tome kako se njihovi predmeti rješavaju u prekograničnim situacijama, kao što je naglasilo nekoliko članova skupine s više dionika. Nadalje, predstavnici poduzeća navode da u određenim slučajevima nacionalna tijela za zaštitu podataka nisu uputila predmete vodećem tijelu za zaštitu podataka, nego su ih rješavala kao lokalne slučajeve.

Komisija pozdravlja objavu Odbora da je započeo s promišljanjem o tome kako riješiti te probleme. Odbor je posebno naveo da će pojasniti postupovne korake u okviru suradnje između vodećeg tijela za zaštitu podataka i predmetnih tijela za zaštitu podataka, analizirati nacionalne upravne postupovne zakone, raditi na zajedničkom tumačenju ključnih pojmova te ojačati komunikaciju i suradnju (uključujući zajedničke operacije). Promišljanje i analiza Odbora trebali bi dovesti do osmišljavanja učinkovitih radnih rješenja u prekograničnim slučajevima[38], među ostalim na temelju stručnog znanja njegovih članova i većeg sudjelovanja njegova tajništva. Osim toga, treba napomenuti da se dužnost Odbora da osigura dosljedno tumačenje Opće uredbe o zaštiti podataka ne može ispuniti jednostavnim utvrđivanjem najmanjega zajedničkog nazivnika.

Naposljetku, kao tijelo EU-a, Odbor mora primjenjivati i upravno pravo EU-a i osigurati transparentnost u postupku donošenja odluka.

2.3 Savjeti i smjernice

Informiranje subjekata i savjeti tijelâ za zaštitu podataka

Nekoliko tijela za zaštitu podataka osmislilo je nove alate, kao što su telefonske linije za pomoć pojedincima i trgovačkim društvima te paketi instrumenata za trgovačka društva[39]. Mnogi subjekti pozdravljaju pragmatizam koji su ta tijela pokazala pružajući pomoć u primjeni Opće uredbe o zaštiti podataka. Konkretno, neka od njih aktivno su i blisko surađivala i komunicirala sa službenicima za zaštitu podataka, među ostalim preko udruženja službenika za zaštitu podataka. Mnoga tijela izdala su i smjernice o ulozi službenika za zaštitu podataka i njihovim obvezama pružanja potpore službenicima za zaštitu podataka tijekom njihovih svakodnevnih aktivnosti te su održavala seminare koji su posebno osmišljeni za njih. Međutim, to nije slučaj sa svim tijelima za zaštitu podataka.

Povratne informacije dobivene od dionika upućuju i na niz pitanja u pogledu smjernica i savjeta:

- nedostatak dosljednog pristupa i smjernica među nacionalnim tijelima za zaštitu podataka o određenim pitanjima (npr. o kolačićima[40], primjeni legitimnog

[38] Kako je istaknuto i u Stajalištu Vijeća i zaključcima.

[39] Vidjeti točku 7. u nastavku.

[40] Do donošenja Uredbe o e-privatnosti potrebna je bliska suradnja s nadležnim tijelima odgovornima za provedbu Direktive o e-privatnosti u državama članicama. U skladu s tom Direktivom, u nekim državama članicama tijela nadležna za provedbu članka 5. stavka 3. Direktive o e-privatnosti (kojim

interesa, obavijestima o povredi podataka ili o procjenama učinka na zaštitu podataka) ili čak među tijelima za zaštitu podataka u istim državama članicama (npr. u Njemačkoj o pojmovima voditelja obrade i izvršitelja obrade);

- nedosljednost smjernica donesenih na nacionalnoj razini s onima koje je donio Odbor,
- nepostojanje javnih savjetovanja o određenim smjernicama donesenima na nacionalnoj razini,
- različite razine suradnje s dionicima među tijelima za zaštitu podataka,
- kašnjenja u dobivanju odgovora na zahtjeve za informacije,
- poteškoće u dobivanju praktičnih i vrijednih savjeta od tijela za zaštitu podataka,
- potreba za povećanjem razine sektorskoga stručnog znanja u nekim tijelima za zaštitu podataka (npr. u zdravstvenom i farmaceutskom sektoru).

Neka od tih pitanja povezana su i s nedostatkom resursa u nekoliko tijela za zaštitu podataka (vidjeti u nastavku).

Različite prakse u pogledu izvješćivanja o povredama podataka[41]

Iako Vijeće ističe da je opterećenje uzrokovano takvim izvješćivanjima veliko, postoje znatne razlike u izvješćivanju među državama članicama: dok je u razdoblju od svibnja 2018. do kraja studenoga 2019. u većini država članica ukupan broj dostavljenih obavijesti o povredi podataka bio manji od 2 000, a u sedam država članica iznosio između 2 000 i 10 000, nizozemska tijela za zaštitu podataka prijavila su 37 400, a njemačka 45 600 dostavljenih obavijesti[42].

To bi moglo upućivati na nedostatak dosljednog tumačenja i provedbe unatoč postojanju smjernica na razini EU-a o izvješćivanju o povredi podataka.

Smjernice Europskog odbora za zaštitu podataka

Odbor je do danas donio više od 20 smjernica kojima su obuhvaćeni ključni aspekti Opće uredbe o zaštiti podataka[43]. Smjernice su ključan instrument za dosljednu primjenu Opće uredbe o zaštiti podataka i stoga su ih dionici u velikoj mjeri pozdravili. Dionici cijene sustavno javno savjetovanje (od šest do osam tjedana), no traže više dijaloga s Odborom. U tom kontekstu trebalo bi nastaviti i pojačati praksu organiziranja radionica o ciljanim temama prije sastavljanja smjernica kako bi se osigurala transparentnost, uključivost i relevantnost rada Odbora. Dionici zahtijevaju i da se tumačenje najspornijih pitanja iznese u smjernicama jer su ona predmet javnog savjetovanja, a ne mišljenja iz članka 64. stavka 2. Opće uredbe o zaštiti podataka. Neki dionici traže i donošenje praktičnijih smjernica u kojima će se detaljno navesti

---

se utvrđuju uvjeti pod kojima se mogu postaviti „kolačići” i pod kojima im se može pristupiti na terminalnoj opremi korisnika) nisu ista kao nadzorna tijela iz Opće uredbe o zaštiti podataka.

41 Članak 33. Opće uredbe o zaštiti podataka.

42 Vidjeti doprinos Odbora, str. 35.

43 Rad na smjernicama već je počeo prije početka primjene Opće uredbe o zaštiti podataka 25. svibnja 2018. u kontekstu Radne skupine iz članka 29. Potpuni popis smjernica dostupan je na: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_hr

primjena pojmova i odredbi Opće uredbe o zaštiti podataka[44]. Članovi skupine s više dionika naglašavaju potrebu za konkretnijim primjerima kako bi se što više smanjio prostor za različita tumačenja među tijelima za zaštitu podataka. Istodobno, zahtjevima za pojašnjenje načina primjene Opće uredbe o zaštiti podataka i pružanje pravne sigurnosti ne bi se smjelo generirati dodatne zahtjeve ili umanjiti prednosti pristupa temeljenog na riziku i načela odgovornosti.

Teme o kojima bi dionici željeli dodatne smjernice Odbora uključuju: opseg prava ispitanika (među ostalim u kontekstu zapošljavanja), ažuriranje mišljenja o obradi podataka na temelju legitimnog interesa, pojmove voditelja obrade, zajedničkog voditelja obrade i izvršitelja obrade te potrebne dogovore među stranama[45], primjenu Opće uredbe o zaštiti podataka na nove tehnologije (kao što su lanac blokova i umjetna inteligencija), obradu u kontekstu znanstvenog istraživanja (među ostalim u vezi s međunarodnom suradnjom), obradu podataka o djeci, pseudonimizaciju i anonimizaciju te obradu zdravstvenih podataka.

Odbor je već naveo da će izdati smjernice za mnoge od tih tema i da je već započeo rad na nekoliko njih (npr. o primjeni legitimnog interesa kao pravne osnove za obradu).

Dionici traže od Odbora da, prema potrebi, ažurira i revidira postojeće smjernice, uzimajući u obzir iskustvo stečeno od njihove objave te koristeći tu priliku da doda više pojedinosti gdje je potrebno.

2.4 Resursi tijela za zaštitu podataka

Osiguravanje potrebnih ljudskih, tehničkih i financijskih resursa, prostorija i infrastrukture za svako tijelo za zaštitu podataka jest preduvjet za djelotvorno obavljanje njegovih zadaća i izvršavanje njegovih ovlasti, a time i bitan uvjet za njegovu neovisnost[46].

Broj članova osoblja i resursi većine tijela za zaštitu podataka povećali su se od stupanja na snagu Opće uredbe o zaštiti podataka 2016.[47] Međutim, mnoga od njih i dalje izvješćuju da nemaju dovoljno resursa[48].

Broj članova osoblja koji rade za nacionalna tijela za zaštitu podataka

Ukupan broj članova osoblja u tijelima za zaštitu podataka EGP-a, razmatranima zajedno, povećao se za 42 % između 2016. i 2019. (za 62 % ako se uzme u obzir prognoza za 2020.).

Broj članova osoblja tijekom tog razdoblja povećao se u većini nadležnih tijela, a najveće povećanje (izraženo u postotku) zabilježeno je u tijelima u Irskoj (+169 %), Nizozemskoj (+145 %), Islandu (+143 %), Luksemburgu (+126 %) i Finskoj (+114 %). Nasuprot tome, broj članova osoblja smanjio se u nekoliko tijela za zaštitu podataka, a najveća smanjenja zabilježena su u Grčkoj (–15 %), Bugarskoj (–14 %),

[44] To su istaknuli i Europski parlament i Vijeće.
[45] Trenutačno su u pripremi smjernice Odbora o voditeljima obrade i izvršiteljima obrade.
[46] Vidjeti članak 52. stavak 4. Opće uredbe o zaštiti podataka.
[47] Uredba je stupila na snagu u svibnju 2016., a primjenjuje se od svibnja 2018., nakon dvogodišnjeg prijelaznog razdoblja.
[48] Vidjeti doprinos Odbora, stranice 26.–30.

Estoniji (–11 %), Latviji (–10 %) i Litvi (–8 %). U nekim je tijelima do smanjenja broja članova osoblja došlo i zbog odlaska stručnjaka za zaštitu podataka u privatni sektor, koji nudi privlačnije uvjete.

Općenito, prognozom za 2020. predviđa se povećanje broja članova osoblja u odnosu na 2019., osim za tijela u Austriji, Bugarskoj, Italiji, Švedskoj i Islandu (gdje se očekuje da će broj članova osoblja ostati stabilan), Cipru i Danskoj (gdje se očekuje da će se taj broj smanjiti).

Njemačka tijela za zaštitu podataka[49] zajednički imaju najveći broj zaposlenih (888 u 2019./1002 prema prognozi za 2020.), nakon čega slijede tijela za zaštitu podataka u Poljskoj (238/260), Francuskoj (215/225), Španjolskoj (170/220), Nizozemskoj (179/188), Italiji (170/170) i Irskoj (140/176).

Tijela za zaštitu podataka s najmanjim brojem članova osoblja jesu tijela u Cipru (24/22), Latviji (19/31), Islandu (17/17), Estoniji (16/18) i Malti (13/15).

Proračunska sredstva nacionalnih tijela za zaštitu podataka

Ukupna proračunska sredstva tijela za zaštitu podataka EGP-a, razmatranih zajedno, povećala su se za 49 % između 2016. i 2019. (za 64 % ako se uzme u obzir prognoza za 2020.).

Proračunska sredstva većine tijela tijekom tog su se razdoblja povećala, a najveće povećanje (izraženo u postotku) zabilježeno je u tijelima u Irskoj (+223 %), Islandu (+167 %), Luksemburgu (+165 %), Nizozemskoj (+130 %) i Cipru (+114 %). S druge strane, neka su tijela zabilježila tek malo povećanje proračunskih sredstava, pri čemu su najmanja povećanja zabilježena kod tijela za zaštitu podataka u Estoniji (7 %), Latviji (4 %), Rumunjskoj (3 %) i Belgiji (1 %), dok je u Francuskoj zabilježeno smanjenje (–2 %).

Općenito, prognozom za 2020. predviđa se povećanje proračunskih sredstava u odnosu na 2019., osim za tijela u Austriji, Bugarskoj, Estoniji i Nizozemskoj (očekuje se da će njihova proračunska sredstva ostati stabilna).

Najveća proračunska sredstva imaju tijela za zaštitu podataka u Njemačkoj (76,6 milijuna EUR 2019./85,8 milijuna EUR prema prognozi za 2020.), Italiji (29,1/30,1), Nizozemskoj (18,6/18,6), Francuskoj (18,5/20,1) i Irskoj (15,2/16,9).

Najmanja proračunska sredstva imaju tijela u Hrvatskoj (1,2 milijuna EUR 2019./1,4 milijuna EUR prema prognozi za 2020.), Rumunjskoj (1,1/1,3), Latviji (0,6/1,2), Cipru (0,5/0,5) i Malti (0,5/0,6).

U tablici u Prilogu II. nalazi se pregled ljudskih i proračunskih resursa nacionalnih tijela za zaštitu podataka.

Osim što utječe na njihovu sposobnost provedbe pravila na nacionalnoj razini, nedostatak resursa ograničava i sposobnost tijela za zaštitu podataka da sudjeluju i daju svoj doprinos u mehanizmima suradnje i konzistentnosti te radu koji se obavlja u

[49] U Njemačkoj postoji 18 tijela, od kojih je jedno tijelo savezno, a 17 su regionalna tijela (uključujući dva u Bavarskoj).

okviru Odbora. Kao što je istaknuo Odbor, uspjeh mehanizma „sve na jednom mjestu" ovisi o vremenu i naporima koje tijela za zaštitu podataka mogu posvetiti rješavanju pojedinačnih prekograničnih slučajeva i suradnji u vezi s njima. Problem resursa dodatno pogoršava povećana uloga nadležnih tijela u nadzoru opsežnih informacijskih sustava koji se trenutačno razvijaju. Nadalje, tijela za zaštitu podataka u Irskoj i Luksemburgu imaju posebne potrebe za resursima s obzirom na njihovu ulogu vodećih tijela za provedbu Opće uredbe o zaštiti podataka u odnosu na velika tehnološka poduzeća koja se uglavnom nalaze u tim državama članicama.

Iako Vijeće ističe učinak mehanizma suradnje i njegovih rokova na rad tijela za zaštitu podataka[50], Općom uredbom o zaštiti podataka države članice obvezuju se da svojim nacionalnim tijelima za zaštitu podataka osiguraju odgovarajuće ljudske, financijske i tehničke resurse[51].

Tajništvo Odbora, koje osigurava Europski nadzornik za zaštitu podataka[52], trenutačno se sastoji od 20 osoba, uključujući pravne stručnjake te stručnjake za informacijske tehnologije i komunikaciju. Potrebno je procijeniti treba li ta brojka u budućnosti rasti s obzirom na djelotvorno ispunjavanje njegove funkcije analitičke, administrativne i logističke potpore Odboru i njegovim podskupinama, među ostalim upravljanjem sustavom razmjene informacija.

3 PRAVILA SU USKLAĐENA, ALI I DALJE POSTOJI ODREĐENI STUPANJ RASCJEPKANOSTI I RAZLIČITI PRISTUPI

Općom uredbom o zaštiti podataka predviđa se dosljedan pristup pravilima o zaštiti podataka diljem EU-a, kojim se zamjenjuju različiti nacionalni sustavi koji su postojali u skladu s Direktivom o zaštiti podataka iz 1995.

3.1 Provedba Opće uredbe o zaštiti podataka u državama članicama

Opća uredba o zaštiti podataka izravno se primjenjuje u svim državama članicama od 25. svibnja 2018. Njome se države članice obvezuju da donose zakone, a posebno da uspostave nacionalna tijela za zaštitu podataka i opće uvjete za njihove članove, kako bi se osiguralo da svako tijelo djeluje potpuno neovisno pri obavljanju svojih zadaća i izvršavanju svojih ovlasti u skladu s Općom uredbom o zaštiti podataka. Pravne obveze i javne zadaće mogu biti pravna osnova za obradu osobnih podataka samo ako su utvrđene (pravom Unije ili) nacionalnim pravom. Osim toga, države članice moraju utvrditi pravila o sankcijama, posebno za povrede za koje se ne naplaćuju upravne novčane kazne, te moraju uskladiti pravo na zaštitu osobnih podataka s pravom na slobodu izražavanja i informiranja. Nacionalnim pravom može se predvidjeti i pravna osnova za izuzeće od opće zabrane obrade posebnih kategorija osobnih podataka, primjerice zbog značajnoga javnog interesa u području javnog zdravlja, uključujući zaštitu od ozbiljnih prekograničnih prijetnji zdravlju. Nadalje, države članice moraju osigurati akreditaciju certifikacijskih tijela.

---

[50] Članak 60. Opće uredbe o zaštiti podataka.
[51] Članak 52. stavak 4. Opće uredbe o zaštiti podataka.
[52] Članak 75. Opće uredbe o zaštiti podataka.

Komisija prati provedbu Opće uredbe o zaštiti podataka u nacionalnom zakonodavstvu. U trenutku sastavljanja ovog izvješća sve države članice osim Slovenije donijele su novo zakonodavstvo o zaštiti podataka ili su prilagodile svoje zakone u tom području. Komisija je stoga od Slovenije zatražila pojašnjenje o dosadašnjem napretku te je pozvala da dovrši taj postupak[53].

Usto, usklađenost nacionalnog zakonodavstva s pravilima o zaštiti podataka u pogledu schengenske pravne stečevine ocjenjuje se i u kontekstu mehanizma za evaluaciju schengenske pravne stečevine koji koordinira Komisija. Komisija i države članice zajednički ocjenjuju kako zemlje provode i primjenjuju schengensku pravnu stečevinu u nizu područja. Za potrebe zaštite podataka to se odnosi na opsežne informacijske sustave kao što su Schengenski informacijski sustav i vizni informacijski sustav te uključuje ulogu tijela za zaštitu podataka u nadzoru obrade osobnih podataka unutar tih sustava.

Na nacionalnoj se razini još uvijek radi na prilagodbi sektorskih zakona. Nakon uključivanja Opće uredbe o zaštiti podataka u Sporazum o Europskom gospodarskom prostoru, njezina je primjena proširena na Norvešku, Island i Lihtenštajn. Te su zemlje donijele i svoje nacionalne zakone o zaštiti podataka.

Komisija će upotrijebiti sve instrumente koji su joj na raspolaganju, uključujući postupke zbog povrede, kako bi osigurala da države članice poštuju Opću uredbu o zaštiti podataka.

Glavna pitanja povezana s nacionalnom provedbom

Glavna pitanja koja su do sada utvrđena u okviru procjene nacionalnog zakonodavstva koja je u tijeku i bilateralnih razmjena s državama članicama uključuju:

- ograničenja primjene Opće uredbe o zaštiti podataka: neke države članice, na primjer, potpuno isključuju aktivnosti nacionalnog parlamenta,
- razlike u primjenjivosti nacionalnih zakona o specifikacijama. Neke države članice povezuju primjenjivost svojeg nacionalnog prava s mjestom na kojem se nude roba ili usluge, a druge s mjestom poslovnog nastana voditelja obrade podataka ili izvršitelja obrade podataka. To je u suprotnosti s ciljem usklađivanja koji se želi postići Općom uredbom o zaštiti podataka,
- nacionalne zakone kojima se postavljaju pitanja o proporcionalnosti zadiranja u pravo na zaštitu podataka. Na primjer, Komisija je pokrenula postupak zbog povrede protiv države članice koja je donijela zakon kojim se od sudaca zahtijeva da objave konkretne informacije o svojim neprofesionalnim aktivnostima, što nije u skladu s pravom na poštovanje privatnog života i pravom na zaštitu osobnih podataka[54],

---

[53] Treba napomenuti da je nacionalno tijelo za zaštitu podataka u Sloveniji uspostavljeno na temelju postojećega nacionalnog zakona o zaštiti podataka i nadzire primjenu Opće uredbe o zaštiti podataka u toj državi članici.

[54] Taj postupak zbog povrede odnosi se na poljski zakon o pravosuđu od 20. prosinca 2019. koji utječe na neovisnost sudaca i odnosi se, među ostalim, na objavljivanje informacija o sudjelovanju sudaca u neprofesionalnim aktivnostima: https://ec.europa.eu/commission/presscorner/detail/hr/ip_20_772.

- nepostojanje neovisnog tijela za nadzor obrade podataka koji provode sudovi koji djeluju u okviru svoje sudske nadležnosti[55],
- zakonodavstvo u područjima koja su u potpunosti uređena Općom uredbom o zaštiti podataka izvan okvira prostora za djelovanje za specifikacije ili ograničenja. To je osobito slučaj kada se nacionalnim odredbama utvrđuju uvjeti za obradu na temelju legitimnog interesa tako što se osigurava ravnoteža između interesa voditelja obrade i predmetnih pojedinaca, dok se Općom uredbom o zaštiti podataka svakog voditelja obrade obvezuje da takvo uravnoteženje provede pojedinačno i da iskoristi tu pravnu osnovu,
- specifikacije i dodatne zahtjeve za ispunjavanje zakonske obveze ili izvršavanje javne zadaće (npr. za videonadzor u privatnom sektoru ili za izravni marketing) osim obrade te za pojmove koji se upotrebljavaju u Općoj uredbi o zaštiti podataka (npr. „opsežno" ili „brisanje").

Neka od tih pitanja Sud može razjasniti u predmetima koji su još u tijeku[56].

Usklađivanje prava na zaštitu osobnih podataka sa slobodom izražavanja i informiranja

Jedno konkretno pitanje odnosi se na provedbu obveze država članica da zakonski usklade pravo na zaštitu osobnih podataka sa slobodom izražavanja i informiranja[57]. To je pitanje vrlo složeno jer se pri procjeni ravnoteže između tih temeljnih prava moraju uzeti u obzir i odredbe i zaštitne mjere u zakonima o tisku i medijima.

Procjena zakonodavstva država članica pokazala je da se usklađivanju prava na zaštitu osobnih podataka sa slobodom izražavanja i informiranja različito pristupa:

- neke države članice utvrđuju načelo prvenstva slobode izražavanja ili u načelu izuzimaju od primjene cijela poglavlja navedena u članku 85. stavku 2. Opće uredbe o zaštiti podataka ako je u pitanju obrada u novinarske svrhe te u svrhe akademskog, umjetničkog i književnog izražavanja. Zakoni o medijima u određenoj mjeri predviđaju neke zaštitne mjere u pogledu prava ispitanika,
- neke države članice utvrđuju prednost zaštite osobnih podataka i izuzimaju od primjene pravila o zaštiti podataka samo posebne situacije, kao što je slučaj osobe s javnim statusom,
- u drugim državama članicama zakonodavac provodi određeno održavanje ravnoteže i/ili se procjenjuju odstupanja od određenih odredbi Opće uredbe o zaštiti podataka za svaki pojedinačni slučaj.

Komisija će nastaviti s ocjenjivanjem nacionalnog zakonodavstva na temelju zahtjeva Povelje. Usklađivanje mora biti predviđeno zakonom, njime se mora poštovati bit tih temeljnih prava te mora biti proporcionalno i nužno (članak 52. stavak 1. Povelje). Pravila o zaštiti podataka ne bi trebala utjecati na ostvarivanje slobode izražavanja i

[55] Vidjeti članak 8. stavak 3. Povelje; članak 16. UFEU-a; uvodnu izjavu 20. Opće uredbe o zaštiti podataka.

[56] Na primjer, izuzeće parlamentarnog odbora od primjene Opće uredbe o zaštiti podataka predmet je sudskog postupka u vezi sa zahtjevom za prethodnu odluku koji je u tijeku (C-272/19).

[57] Članak 85. Opće uredbe o zaštiti podataka.

informiranja, posebice stvaranjem odvraćajućeg učinka ili tako da ih se tumači kao način vršenja pritiska na novinare da otkriju svoje izvore.

3.2 Odredbe o fakultativnim specifikacijama i njihova ograničenja

Općom uredbom o zaštiti podataka državama članicama daje se mogućnost da dodatno preciziraju način njezine provedbe u ograničenom broju područja. Taj prostor za djelovanje za nacionalno zakonodavstvo treba razlikovati od obveze provedbe nekih drugih odredbi Opće uredbe o zaštiti podataka, kako je prethodno navedeno. Odredbe o fakultativnim specifikacijama navedene su u Prilogu I.

Prostor za djelovanje koji se odnosi na pravo država članica podliježe uvjetima i ograničenjima utvrđenima Općom uredbom o zaštiti podataka te se ne dopušta nastajanje paralelnog nacionalnog sustava zaštite podataka[58]. Države članice obvezne su izmijeniti ili staviti izvan snage nacionalne zakone o zaštiti podataka, uključujući sektorsko zakonodavstvo s aspektima zaštite podataka.

Nadalje, povezano zakonodavstvo država članica ne smije sadržavati odredbe koje bi mogle dovesti do zabune u pogledu izravne primjene Opće uredbe o zaštiti podataka. Stoga, ako se Općom uredbom o zaštiti podataka predviđaju specifikacije ili ograničenja njezinih pravila pravom države članice, države članice mogu uključiti elemente Opće uredbe o zaštiti podataka u svoje nacionalno pravo u mjeri u kojoj je to potrebno radi usklađenosti i kako bi nacionalne odredbe bile razumljive osobama na koje se primjenjuju[59].

Dionici smatraju da bi države članice trebale smanjiti uporabu odredbi o fakultativnim specifikacijama ili se od nje suzdržati jer te odredbe ne doprinose usklađivanju. Nacionalne razlike u provedbi zakona i načinu na koji ih tumače tijela za zaštitu podataka znatno povećavaju trošak pravnog usklađivanja diljem EU-a.

Fragmentacija povezana s uporabom odredbi o fakultativnim specifikacijama

- Dobna granica za privolu djece na usluge informacijskog društva

Niz država članica iskoristio je mogućnost da predvide dob nižu od 16 godina za privolu u pogledu usluga informacijskog društva (članak 8. stavak 1. Opće uredbe o zaštiti podataka). U devet država članica ta je dobna granica 16 godina, njih osam odabralo je 13 godina, šest je odabralo 14 godina, a tri su odabrale granicu od 15 godina[60].

Stoga trgovačko društvo koje pruža usluge informacijskog društva maloljetnicima diljem EU-a mora razlikovati dob potencijalnih korisnika ovisno o tome u kojoj državi članici imaju boravište. To je u suprotnosti s ključnim ciljem Opće uredbe o zaštiti podataka da se osigura jednaka razina zaštite pojedinaca i poslovnih prilika u svim državama članicama.

Takve razlike dovode do situacija u kojima država članica u kojoj voditelj obrade ima poslovni nastan predviđa različitu dobnu granicu od države članice u kojoj ispitanici imaju boravište.

---

[58] Pojam „uvodne odredbe” koji se često upotrebljava u značenju odredbi o specifikaciji zavarava jer bi mogao stvoriti dojam da države članice imaju manevarski prostor koji nadilazi odredbe Uredbe.

[59] Uvodna izjava 8. Opće uredbe o zaštiti podataka.

[60] Trinaest godina u Belgiji, Danskoj, Estoniji, Finskoj, Latviji, Malti, Portugalu i Švedskoj; 14 godina u Austriji, Bugarskoj, Cipru, Španjolskoj, Italiji i Litvi; 15 godina u Češkoj, Grčkoj i Francuskoj; 16 godina u Njemačkoj, Mađarskoj, Hrvatskoj, Irskoj, Luksemburgu, Nizozemskoj, Poljskoj, Rumunjskoj i Slovačkoj.

- Zdravlje i istraživanje

Pri provedbi odstupanja od opće zabrane obrade posebnih kategorija osobnih podataka[61] zakonodavstvo država članica slijedi različite pristupe u pogledu razine specifikacije i zaštitnih mjera, među ostalim u zdravstvene i istraživačke svrhe. Većina država članica uvela je ili zadržala dodatne uvjete za obradu genetskih podataka, biometrijskih podataka ili podataka koji se odnose na zdravlje. To vrijedi i za odstupanja povezana s pravima ispitanika za potrebe istraživanja[62], u pogledu opsega odstupanja i u pogledu povezanih zaštitnih mjera.

Buduće smjernice Odbora o uporabi osobnih podataka u području znanstvenih istraživanja doprinijet će usklađenom pristupu u tom području. Komisija će Odboru dati svoj doprinos, posebno u pogledu istraživanja u području zdravlja, među ostalim u obliku konkretnih pitanja i analize konkretnih scenarija koje je dobila od istraživačke zajednice. Bilo bi korisno da se te smjernice donesu prije pokretanja okvirnog programa Obzor Europa u cilju usklađivanja praksi zaštite podataka i olakšavanja razmjene podataka radi napretka u istraživanju. Korisne bi mogle biti i smjernice Odbora o obradi osobnih podataka u području zdravlja.

Općom uredbom o zaštiti podataka pruža se čvrst okvir za nacionalno zakonodavstvo u području javnog zdravlja i njome su izričito obuhvaćene prekogranične prijetnje zdravlju te praćenje epidemija i njihova širenja[63], što je bilo relevantno u kontekstu suzbijanja pandemije bolesti COVID-19.

Na razini EU-a Komisija je 8. travnja 2020. donijela Preporuku o zajedničkom paketu mjera za primjenu tehnologije i podataka u tom kontekstu, uključujući mobilne aplikacije i uporabu anonimiziranih podataka o mobilnosti[64], a 16. travnja 2020. smjernice o aplikacijama kojima se podupire suzbijanje pandemije u vezi sa zaštitom podataka[65]. Odbor je 19. ožujka 2020. objavio izjavu o obradi podataka u tom kontekstu[66], nakon čega su 21. travnja 2020. uslijedile smjernice o obradi podataka u istraživačke svrhe te o uporabi podataka o lokalizaciji i alatima za praćenje kontakata u tom kontekstu[67]. U tim se preporukama i smjernicama pojašnjava kako se načela i pravila o zaštiti osobnih podataka primjenjuju u kontekstu suzbijanja pandemije.

- Opsežna ograničenja prava ispitanika

U većini nacionalnih zakona o zaštiti podataka kojima se ograničavaju prava ispitanika ne navode se ciljevi od općega javnog interesa zaštićeni tim ograničenjima i/ili se u dovoljnoj mjeri ne ispunjavaju uvjeti i zaštitne mjere propisane člankom 23. stavkom 2. Opće uredbe o zaštiti podataka[68]. Nekoliko država članica ne ostavlja

---

61 Članak 9. Opće uredbe o zaštiti podataka.
62 Članak 89. stavak 2. Opće uredbe o zaštiti podataka.
63 Vidjeti članak 9. stavak 2. točku (i) Opće uredbe o zaštiti podataka i uvodnu izjavu 46.
64 https://ec.europa.eu/transparency/regdoc/rep/3/2020/HR/C-2020-3300-F1-HR-MAIN-PART-1.PDF.
65 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417 (08) & from = EN.
66 https://edpb.europa.eu/news/news/2020/statement-processing-personal-data-context-covid-19-outbreak_hr
67 https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_hr
68 Na primjer, jer samo ponavljaju tekst članka 23. stavka 1. Opće uredbe o zaštiti podataka.

prostora za ispitivanje proporcionalnosti ili proširuju ograničenja čak i izvan područja primjene članka 23. stavka 1. Opće uredbe o zaštiti podataka. Na primjer, nekim se nacionalnim zakonima uskraćuje pravo pristupa zbog nerazmjernih napora voditelja obrade, kad je riječ o osobnim podacima koji se pohranjuju na temelju obveze zadržavanja ili su povezani s izvršavanjem javnih zadaća, a da se to ograničenje ne odnosi samo na ciljeve od općega javnog interesa.

- Dodatni zahtjevi za poduzeća

Iako se zahtjev za obveznim imenovanjem službenika za zaštitu podataka temelji na pristupu temeljenom na riziku[69], jedna ga je država članica[70] proširila na kvantitativne kriterije, obvezujući poduzeća u kojima je 20 ili više zaposlenika trajno uključeno u automatiziranu obradu osobnih podataka da imenuju službenika za zaštitu podataka, neovisno o rizicima povezanima s aktivnostima obrade[71]. To je dovelo do dodatnih opterećenja.

4 JAČANJE POLOŽAJA POJEDINACA U POGLEDU KONTROLE NJIHOVIH PODATAKA

Općom uredbom o zaštiti podataka temeljna prava postaju djelotvorna, posebice pravo na zaštitu osobnih podataka, ali i druga temeljna prava priznata Poveljom, uključujući poštovanje privatnog i obiteljskog života, slobodu izražavanja i informiranja, nediskriminaciju, slobodu mišljenja, savjesti i vjeroispovijesti, slobodu poduzetništva i pravo na učinkoviti pravni lijek. Ta se prava moraju međusobno uravnotežiti u skladu s načelom proporcionalnosti[72].

Općom uredbom o zaštiti podataka pojedincima se pružaju ostvariva prava, kao što su pravo na pristup, ispravak, brisanje, prigovor, prenosivost i poboljšanu transparentnost. Pojedincima se daje i pravo na podnošenje pritužbe tijelu za zaštitu podataka, među ostalim udružnim tužbama, te pravo na sudsku zaštitu.

Pojedinci su sve svjesniji svojih prava, što je vidljivo iz rezultata Eurobarometra[73] iz srpnja 2019. te iz istraživanja koje je provela Agencija za temeljna prava[74].

Prema istraživanju o temeljnim pravima koje je provela Agencija za temeljna prava:

- 69 % stanovništva EU-a u dobi od 16 i više godina čulo je za Opću uredbu o zaštiti podataka,
- 71 % ispitanika u EU-u čulo je za svoje nacionalno tijelo za zaštitu podataka; ta brojka kreće se od 90 % u Češkoj do 44 % u Belgiji,
- 60 % ispitanika u EU-u svjesno je zakona kojim im se omogućuje pristup njihovim osobnim podacima koje posjeduju tijela javne uprave; međutim, taj postotak iznosi tek 51 % u slučaju privatnih poduzeća,

[69] Članak 37. stavak 1. Opće uredbe o zaštiti podataka.
[70] Njemačka.
[71] Primjena odredbe o specifikaciji iz članka 37. stavka 4. Opće uredbe o zaštiti podataka.
[72] Usp. uvodnu izjavu 4. Opće uredbe o zaštiti podataka.
[73] https://ec.europa.eu/commission/presscorner/detail/hr/IP_19_2956
[74] Agencija Europske unije za temeljna prava (FRA) (2020.): Istraživanje o temeljnim pravima 2019. Zaštita podataka i tehnologija: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection

- više od petine ispitanika (23 %) u EU-u ne želi dijeliti osobne podatke (kao što su adresa, državljanstvo ili datum rođenja) s tijelima javne uprave, a 41 % ne želi dijeliti te podatke s privatnim poduzećima.

Pojedinci se sve više koriste svojim pravom na podnošenje pritužbi tijelima za zaštitu podataka, pojedinačno i udružnim tužbama[75]. Samo je nekoliko država članica dopustilo nevladinim organizacijama da pokrenu tužbe bez mandata, u skladu s mogućnošću koju pruža Opća uredba o zaštiti podataka. Očekuje se da će se donošenjem predložene direktive o udružnim tužbama za zaštitu kolektivnih interesa potrošača[76] ojačati okvir za udružne tužbe i u području zaštite podataka.

Pritužbe

Prema izvješću Odbora, ukupan broj pritužbi u razdoblju od svibnja 2018. do kraja studenoga 2019. iznosi oko 275 000[77]. Međutim, tu brojku treba uzeti s oprezom, s obzirom na to da definicija pritužbe nije jednaka za sva tijela. Apsolutni broj pritužbi koje su zaprimila tijela za zaštitu podataka[78] vrlo je različit među državama članicama. Najveći broj pritužbi zabilježen je u Njemačkoj (67 000), Nizozemskoj (37 000), Španjolskoj i Francuskoj (u svakoj po 18 000), Italiji (14 000), Poljskoj i Irskoj (u svakoj po 12 000). Dvije trećine nadležnih tijela izvijestile su da je broj pritužbi bio od 8 000 do 600. Najniži broj pritužbi zabilježen je u Estoniji i Belgiji (oko 500 u svakoj) te Malti i Islandu (manje od 200 u svakoj).

Broj pritužbi nije nužno povezan s veličinom populacije ili BDP-om, s obzirom na to da je, primjerice, u Njemačkoj podneseno gotovo dvostruko više pritužbi u nego u Nizozemskoj i četiri puta više nego u Španjolskoj i Francuskoj.

Povratne informacije skupine s više dionika pokazuju da su organizacije uvele niz mjera za lakše ostvarivanje prava ispitanika, uključujući provedbene postupke kojima se osigurava pojedinačno preispitivanje zahtjeva i odgovor voditelja obrade, uporabu nekoliko kanala (pošta, namjenska adresa e-pošte, internetska stranica itd.), ažurirane interne postupke i politike o pravodobnoj internoj obradi zahtjeva te osposobljavanje osoblja. Neka su poduzeća pokrenula digitalne portale dostupne putem internetskih stranica trgovačkog društva (ili intraneta trgovačkog društva za zaposlenike) kako bi se ispitanicima olakšalo ostvarivanje prava.

Međutim, potreban je daljnji napredak u sljedećim točkama:

- neki voditelji obrade podataka ne poštuju svoju obvezu da olakšaju ostvarivanje prava ispitanika[79]. Oni moraju osigurati učinkovitu kontaktnu točku kojoj ispitanici mogu objasniti svoje probleme. To može biti službenik za zaštitu podataka, čiji se podaci za kontakt moraju proaktivno pružati ispitaniku[80]. Mogućnosti kontaktiranja ne smiju biti ograničene na poruke e-pošte, već se ispitaniku mora omogućiti da se obrati voditelju obrade i drugim sredstvima,

[75] Članak 80. Opće uredbe o zaštiti podataka.
[76] COM(2018) 184 final – 2018/089 (COD)
[77] I jedno i drugo u člancima 77. i 80. Opće uredbe o zaštiti podataka.
[78] Vidjeti doprinos Odbora, stranice 31.–32.
[79] Članak 12. stavak 2. Opće uredbe o zaštiti podataka.
[80] Članak 13. stavak 1. točka (b) i članak 14. stavak 1. točka (b) Opće uredbe o zaštiti podataka.

- pojedinci se i dalje suočavaju s poteškoćama pri podnošenju zahtjeva za pristup svojim podacima, na primjer platformama, posrednicima podataka i poduzećima koja se bave tehnologijom oglašavanja,
- pravo na prenosivost podataka ne primjenjuje se u potpunosti. U Europskoj strategiji za podatke (dalje u tekstu „podatkovna strategija")[81], koju je Komisija donijela 19. veljače 2020., naglašena je potreba za olakšavanjem svih mogućih uporaba tog prava (npr. propisivanjem tehničkih sučelja i strojno čitljivih formata koji omogućuju prenosivost podataka u (gotovo) stvarnom vremenu). Subjekti napominju da ponekad dolazi do poteškoća pri pružanju podataka u strukturiranom, uobičajeno upotrebljavanom strojno čitljivom formatu (zbog nedostatka standarda). Samo organizacije u određenim sektorima, kao što su bankarstvo, telekomunikacije, vodomjeri i toplinska brojila, izvješćuju da su uvele potrebna sučelja[82]. Razvijeni su novi tehnološki alati kako bi se pojedincima olakšalo ostvarivanje njihovih prava na temelju Opće uredbe o zaštiti podataka, koja nisu ograničena na prenosivost podataka (npr. prostori za osobne podatke i usluge upravljanja osobnim informacijama),
- prava djece: nekoliko članova skupine s više dionika naglašava potrebu za pružanjem informacija djeci i činjenicu da mnoge organizacije zanemaruju činjenicu da bi se njihova obrada podataka mogla odnositi na djecu. Vijeće je naglasilo da bi se pri sastavljanju kodeksâ ponašanja posebna pozornost mogla posvetiti zaštiti djece. Zaštita djece također je u središtu pozornosti tijelâ za zaštitu podataka[83],
- pravo na informacije: neka trgovačka društva imaju vrlo legalistički pristup te uzimaju obavijesti o zaštiti podataka kao pravnu praksu, pri čemu su informacije prilično složene, teško razumljive ili nepotpune, dok se Općom uredbom o zaštiti podataka zahtijeva da sve informacije budu sažete i iznesene jasnim i jednostavnim jezikom[84]. Čini se da neka trgovačka društva ne poštuju preporuke Odbora, primjerice u pogledu navođenja naziva subjekata s kojima dijele podatke,
- nekoliko država članica uvelike je ograničilo prava ispitanika nacionalnim pravom, a neke čak i nadilaze okvir članka 23. Opće uredbe o zaštiti podataka,
- ostvarivanje prava pojedinaca ponekad je otežano praksama nekoliko velikih digitalnih aktera koje pojedincima otežavaju odabir postavki kojima se najviše štiti njihova privatnost (čime se krši zahtjev za tehničku i integriranu zaštitu podataka[85])[86].

---

81 https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

82 Vidjeti izvješće skupine s više dionika.

83 Vidjeti rezultate javnog savjetovanja o pravima djece na zaštitu podataka koje je provelo irsko tijelo za zaštitu podataka: https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Whose%20Rights%20Are%20They%20Anyway_Trends%20and%20Hightlights%20from%20Stream%201.pdf. Francusko tijelo za zaštitu podataka pokrenulo je javno savjetovanje u travnju 2020.: https://www.cnil.fr/fr/la-cnil-lance-une-consultation-publique-sur-les-droits-des-mineurs-dans-lenvironnement-numerique

84 Članak 12. stavak 1. Opće uredbe o zaštiti podataka.

85 Članak 25. Opće uredbe o zaštiti podataka.

Dionici željno iščekuju smjernice Odbora o pravima ispitanika.

5 MOGUĆNOSTI I IZAZOVI ZA ORGANIZACIJE, POSEBNO MALA I SREDNJA PODUZEĆA

Mogućnosti za organizacije

Općom uredbom o zaštiti podataka potiču se tržišno natjecanje i inovacije. Zajedno s Uredbom o slobodnom protoku neosobnih podataka[87], njome se osigurava slobodan protok podataka unutar EU-a i stvaraju jednaki uvjeti za poduzeća koja nemaju poslovni nastan u EU-u. Općom uredbom o zaštiti podataka stvara se usklađeni okvir za zaštitu osobnih podataka i osigurava se da sve sudionike na unutarnjem tržištu obvezuju jednaka pravila i da imaju jednake mogućnosti, bez obzira na to gdje se nalazi njihov poslovni nastan i gdje se odvija obrada. Tehnološka neutralnost Opće uredbe o zaštiti podataka omogućuje pružanje okvira za zaštitu podataka za nove tehnologije. Načelima tehničke i integrirane zaštite podataka potiču se inovativna rješenja koja od samog početka uključuju pitanja zaštite podataka i mogu smanjiti troškove usklađivanja s povezanim pravilima.

Nadalje, privatnost postaje važan parametar tržišnog natjecanja koji pojedinci sve više uzimaju u obzir pri odabiru usluga. Oni koji su informiraniji i osjetljiviji na pitanja zaštite podataka traže proizvode i usluge kojima se osigurava djelotvorna zaštita osobnih podataka. Provedbom prava na prenosivost podataka mogle bi se smanjiti prepreke za ulazak na tržište poduzeća koja nude inovativne usluge prilagođene zaštiti podataka. Potrebno je pratiti učinke moguće šire uporabe tog prava na tržište u različitim sektorima. Usklađenost s pravilima o zaštiti podataka i njihova transparentna primjena stvorit će povjerenje u uporabu osobnih podataka građana, a time i nove prilike za poduzeća.

Kao i svi propisi, pravila o zaštiti podataka uključuju povezane troškove usklađivanja za poduzeća. Međutim, prednosti i mogućnosti koje proizlaze iz većeg povjerenja u digitalne inovacije i društvene koristi koje proizlaze iz poštovanja temeljnog prava nadmašuju te troškove. Općom uredbom o zaštiti podataka osiguravaju se jednaki uvjeti za sve, a tijelima za zaštitu podataka daju se sredstva koja su im potrebna za djelotvornu provedbu pravila te se na taj način sprečava da poduzeća koja ne poštuju pravila iskorištavaju povjerenje koje su izgradili oni koji pravila poštuju.

Posebni izazovi za mala i srednja poduzeća (MSP-ove)

---

[86] Vidjeti izvješće Norveškog vijeća za zaštitu potrošača, *Deceived by Design* (Obmanuti dizajnom), u kojem su istaknuti „tamni uzorci", zadane postavke i druge značajke i tehnike koje poduzeća upotrebljavaju kako bi korisnike naveli na intruzivne opcije: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/
Vidjeti i istraživanje koje su u prosincu 2019. objavili Transatlantski dijalog potrošača i Heinrich-Böll-Stiftung Brussels European Union u kojem se analiziraju prakse triju velikih globalnih platformi: https://eu.boell.org/en/2019/12/11/privacy-eu-and-us-consumer-experiences-across-three-global-platforms

[87] Uredba (EU) 2018/1807 Europskog parlamenta i Vijeća od 14. studenoga 2018. o okviru za slobodan protok neosobnih podataka u Europskoj uniji – SL L 303, 28.11.2018., str. 59.–68.

Dionici, ali i Europski parlament, Vijeće i tijela za zaštitu podataka općenito smatraju da je primjena Opće uredbe o zaštiti podataka posebno zahtjevna za mikropoduzeća, mala i srednja poduzeća te male dobrovoljne i dobrotvorne organizacije.

U skladu s pristupom koji se temelji na riziku, ne bi bilo primjereno predvidjeti odstupanja na temelju veličine subjekata, jer njihova veličina sama po sebi nije pokazatelj rizika koje za pojedince može stvoriti obrada osobnih podataka koju oni provode. Pristupom koji se temelji na riziku postiže se fleksibilnost uz djelotvornu zaštitu. Njime se uzimaju u obzir potrebe MSP-ova čija osnovna djelatnost nije obrada podataka te se njihove obveze posebno prilagođavaju na temelju vjerojatnosti i ozbiljnosti rizika povezanih s vrstom obrade koju provode.[88]

Obrada malog opsega i niskog rizika ne bi se trebala tretirati na isti način kao visokorizična i česta obrada – neovisno o veličini trgovačkog društva koje obavlja obradu. Stoga bi, kako je Odbor zaključio, „u svakom slučaju trebalo zadržati pristup temeljen na riziku koji zakonodavac promiče u tekstu jer rizici za ispitanike ne ovise o veličini voditelja obrade”[89]. Tijela za zaštitu podataka trebala bi u potpunosti uzeti u obzir to načelo pri provedbi Opće uredbe o zaštiti podataka, po mogućnosti u okviru zajedničkog europskog pristupa, kako se ne bi stvarale prepreke jedinstvenom tržištu.

Tijela za zaštitu podataka razvila su nekoliko alata i naglasila svoju namjeru da ih dodatno poboljšaju. Neka su nadležna tijela pokrenula informativne kampanje i čak će održati besplatna „predavanja o Općoj uredbi o zaštiti podataka” za MSP-ove.

Primjeri smjernica i alata koje tijela za zaštitu podataka posebno pružaju MSP-ovima:

- objavljivanje informacija upućenih MSP-ovima,
- seminari za službenike za zaštitu podataka i događanja za MSP-ove koji ne moraju imenovati službenika za zaštitu podataka,
- interaktivni vodiči za pomoć MSP-ovima,
- dežurne telefonske linije za savjetovanje,
- predlošci za obradu ugovora i evidenciju o aktivnostima obrade.

Opis aktivnosti koje provode tijela za zaštitu podataka prikazan je u doprinosu Odbora[90].

Nekoliko mjera kojima se posebno podupiru MSP-ovi dobilo je financijska sredstva EU-a. Komisija je pružila financijsku potporu kroz tri vala bespovratnih sredstava u ukupnom iznosu od 5 milijuna EUR, pri čemu su posljednja dva vala namijenjena za potporu nacionalnim tijelima za zaštitu podataka u njihovim nastojanjima da dopru do pojedinaca i MSP-ova. Zbog toga je 2018. devet tijela za zaštitu podataka dobilo 2 milijuna EUR za aktivnosti u razdoblju 2018./2019. (Belgija, Bugarska, Danska,

[88] Članak 24. stavak 1. Opće uredbe o zaštiti podataka.
[89] Vidjeti doprinos Odbora, str. 35.
[90] Vidjeti doprinos Odbora, stranice 35.–45.

Mađarska, Litva, Latvija, Nizozemska, Slovenija i Island)[91], a 2019. su četiri tijela za zaštitu podataka dobila 1 milijun EUR za aktivnosti u 2020. (Belgija, Malta, Slovenija i Hrvatska u partnerstvu s Irskom)92. U 2020. dodijelit će se dodatni iznos od 1 milijun EUR.

Unatoč tim inicijativama, MSP-ovi i novoosnovana poduzeća često izvješćuju da imaju poteškoća s provedbom načela odgovornosti utvrđenog u Općoj uredbi o zaštiti podataka[93]. Posebno navode da ne dobivaju uvijek dovoljno smjernica i praktičnih savjeta od nacionalnih tijela za zaštitu podataka ili da je vrijeme potrebno za dobivanje smjernica i savjeta predugo. Bilo je i slučajeva u kojima nadležna tijela nisu bila voljna ulaziti u pravna pitanja. U takvim situacijama MSP-ovi se često obraćaju vanjskim savjetnicima i odvjetnicima kako bi mogli primijeniti načelo odgovornosti i pristup koji se temelji na riziku (uključujući zahtjeve u pogledu transparentnosti, evidencije o obradi i obavijesti o povredi podataka). To im može stvoriti i dodatne troškove.

Posebno je pitanje evidentiranje aktivnosti obrade, koje MSP-ovi te mala udruženja smatraju velikim administrativnim opterećenjem. Izuzeće od te obveze iz članka 30. stavka 5. Opće uredbe o zaštiti podataka doista je vrlo ograničeno. Međutim, ne bi trebalo precjenjivati napore povezane s ispunjavanjem te obveze. Ako temeljna djelatnost MSP-ova ne uključuje obradu osobnih podataka, takva evidencija može biti jednostavna i neopterećujuća. Isto vrijedi i za dobrovoljna i druga udruženja. Takve pojednostavljene evidencije olakšale bi se primjenom obrazaca za evidenciju, što je već praksa nekih tijela za zaštitu podataka. U svakom slučaju, svatko tko obrađuje osobne podatke trebao bi imati pregled svoje obrade podataka, što je osnovni zahtjev načela odgovornosti.

Razvojem praktičnih alata na razini EU-a koji provodi Odbor, kao što su usklađeni obrasci za povrede podataka i pojednostavljena evidencija o aktivnostima obrade, može se pomoći MSP-ovima i malim udruženjima[94] čije glavne aktivnosti nisu usmjerene na obradu osobnih podataka da ispune svoje obveze.

Razna sektorska udruženja nastojala su jačati svijest i informirati svoje članove, primjerice putem konferencija i seminara, informiranjem poduzeća o dostupnim smjernicama ili razvijanjem usluge za pomoć pri zaštiti privatnosti za članove. Izvješćuju i o sve većem broju seminara, sastanaka i događanja o pitanjima povezanima s Općom uredbom o zaštiti podataka koje organiziraju skupine za strateško promišljanje i udruženja MSP-ova.

Kako bi se poboljšalo slobodno kretanje svih podataka unutar EU-a i uspostavila dosljedna primjena Opće uredbe o zaštiti podataka i Uredbe o slobodnom protoku neosobnih podataka, Komisija je izdala i praktične smjernice o pravilima kojima se

---

[91] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai- ag-2017.

[92] https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_hr

[93] Vidjeti izvješće skupine s više dionika.

[94] Vidjeti doprinos Vijeća.

uređuje obrada miješanih skupova podataka koji se sastoje od osobnih i neosobnih podataka, a posebno su usmjerene na MSP-ove[95].

Paketi instrumenata za poduzeća

Općom uredbom o zaštiti podataka predviđeni su instrumenti koji pomažu u dokazivanju usklađenosti, kao što su kodeksi ponašanja, mehanizmi certificiranja i standardne ugovorne klauzule.

- Kodeksi ponašanja

Odbor je objavio smjernice[96] za potporu „autorima kodeksa" kako bi im se olakšala izrada, izmjena ili proširenje kodeksa te pružile praktične upute i pomoć pri tumačenju. Osim toga, u tim se smjernicama razjašnjavaju postupci, odnosno utvrđuju minimalni kriteriji, za podnošenje, odobrenje i objavu kodeksâ i na nacionalnoj razini i na razini EU-a .

Dionici kodekse ponašanja smatraju vrlo korisnim instrumentima. Iako se mnogi kodeksi provode na nacionalnoj razini, trenutačno je u pripremi niz kodeksa ponašanja na razini EU-a (na primjer o mobilnim aplikacijama za zdravlje, zdravstvenim istraživanjima u području genomike, računalstvu u oblaku, izravnom marketingu, osiguranju, obradi putem usluga prevencije i savjetovanja za djecu)[97]. Subjekti smatraju da bi trebalo snažnije promicati kodekse ponašanja na razini EU-a jer se njima potiče dosljedna primjena Opće uredbe o zaštiti podataka u svim državama članicama.

Međutim, subjekti moraju uložiti vrijeme i sredstva za razvoj kodeksa ponašanja i uspostavu potrebnih neovisnih nadzornih tijela. Predstavnici MSP-ova naglašavaju važnost i korisnost kodeksa ponašanja prilagođenih njihovoj situaciji koji ne podrazumijevaju nerazmjerne troškove.

Stoga su poslovna udruženja u brojnim sektorima primijenila druge vrste alata za samoregulaciju, kao što su kodeksi dobre prakse ili smjernice. Iako takvi alati mogu pružiti korisne informacije, nisu ih odobrila tijela za zaštitu podataka i ne mogu poslužiti kao alat za dokazivanje usklađenosti s Općom uredbom o zaštiti podataka.

Vijeće naglašava da se u kodeksima ponašanja posebna pozornost mora posvetiti obradi podataka o djeci i zdravstvenih podataka. Komisija podržava kodeks(e) ponašanja kojima bi se uskladio pristup u području zdravlja i istraživanja te olakšala prekogranična obrada osobnih podataka[98]. Odbor je u postupku odobravanja nacrta akreditacijskih zahtjeva za tijela za praćenje sukladnosti s kodeksima ponašanja koje su predložila brojna tijela za zaštitu podataka[99]. Nakon što transnacionalni kodeksi ponašanja ili kodeksi ponašanja EU-a budu spremni za podnošenje tijelima za zaštitu podataka na odobrenje, o njima će raspravljati Odbor. Brzo uvođenje transnacionalnih

---

[95] Komunikacija Komisije Europskom parlamentu i Vijeću – Smjernice o Uredbi o okviru za slobodan protok neosobnih podataka u Europskoj uniji, COM(2019) 250 final.

[96] https://edpb.europa.eu/our-work-tools/our-documents/wytyczne/guidelines-12019-codes-conduct-and-monitoring-bodies-under_hr

[97] Vidjeti izvješće skupine s više dionika.

[98] Vidjeti mjere najavljene u Europskoj strategiji za podatke, str. 30.

[99] U skladu s člankom 41. stavkom 3. Opće uredbe o zaštiti podataka. Vidjeti mišljenja Europskog odbora za zaštitu podataka na: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_hr

kodeksa ponašanja posebno je važno za područja koja uključuju obradu znatnih količina podataka (npr. računalstvo u oblaku) ili osjetljivih podataka (npr. zdravlje/istraživanje).

- Certificiranje

Certificiranje može biti koristan instrument za dokazivanje usklađenosti s konkretnim zahtjevima Opće uredbe o zaštiti podataka. Njime se može povećati pravna sigurnost za poduzeća i promicati Opća uredba o zaštiti podataka na globalnoj razini.

Kako je istaknuto u studiji o certificiranju objavljenoj u travnju 2019.[100], cilj bi trebao biti olakšavanje primjene relevantnih programa. Razvoj programa certificiranja u EU-u poduprijet će se smjernicama Odbora o kriterijima certificiranja[101] i akreditaciji certifikacijskih tijela[102].

Sigurnost i tehnička zaštita podataka ključni su elementi koje treba uzeti u obzir u programima certificiranja u okviru Opće uredbe o zaštiti podataka i kojima bi koristio zajednički i ambiciozni pristup diljem EU-a. Komisija će nastaviti podupirati postojeće kontakte između Agencije Europske unije za kibersigurnost (ENISA), tijela za zaštitu podataka i Odbora.

U pogledu kibersigurnosti Komisija je nakon donošenja Akta o kibersigurnosti zatražila od ENISA-e da pripremi dva programa certificiranja, uključujući jedan program za usluge računalstva u oblaku[103]. Razmatraju se daljnji programi koji se odnose na kibersigurnost usluga i proizvoda za potrošače. Iako se ti programi certificiranja uspostavljeni na temelju Akta o kibersigurnosti ne odnose izričito na zaštitu podataka i privatnost, njima se doprinosi povećanju povjerenja potrošača u digitalne usluge i proizvode. Takvim programima mogu se pružiti dokazi o poštovanju načela integrirane sigurnosti, kao i o provedbi odgovarajućih tehničkih i organizacijskih mjera povezanih sa sigurnošću obrade osobnih podataka.

- Standardne ugovorne klauzule

Komisija radi na standardnim ugovornim klauzulama između voditeljâ obrade i izvršiteljâ obrade[104], među ostalim i s obzirom na modernizaciju standardnih ugovornih klauzula za međunarodne prijenose (vidjeti odjeljak 7.2.). Akt Unije, koji donosi Komisija, imat će obvezujući učinak na razini EU-a, čime će se osigurati potpuno usklađivanje i pravna sigurnost.

6 PRIMJENA OPĆE UREDBE O ZAŠTITI PODATAKA NA NOVE TEHNOLOGIJE

Tehnološki neutralan okvir otvoren za nove tehnologije

---

[100] https://ec.europa.eu/info/study-data-protection-certification-mechanisms_hr

[101] https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-12018-certification-and-identifying-certification_hr

[102] https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-42018-accreditation-certification-bodies-under_hr Nekoliko nadzornih tijela već je podnijelo svoje zahtjeve za akreditaciju EDPB-u, i za tijela za praćenje kodeksa ponašanja i za certifikacijska tijela. Pregled je dostupan na sljedećoj poveznici: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_hr

[103] https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe

[104] Članak 28. stavak 7. Opće uredbe o zaštiti podataka.

Opća uredba o zaštiti podataka tehnološki je neutralna, pruža povjerenje i temelji se na načelima[105]. Ta načela, uključujući zakonitu i transparentnu obradu, ograničavanje svrhe i smanjenje količine podataka, pružaju čvrstu osnovu za zaštitu osobnih podataka, neovisno o primijenjenim postupcima i tehnikama obrade.

Članovi skupine s više dionika izvješćuju da Opća uredba o zaštiti podataka općenito ima pozitivan učinak na razvoj novih tehnologija i pruža dobru osnovu za inovacije. Opća uredba o zaštiti podataka smatra se ključnim i fleksibilnim alatom za osiguravanje razvoja novih tehnologija u skladu s temeljnim pravima. Provedba njezinih temeljnih načela posebno je važna za intenzivnu obradu podataka. Pristupom temeljenim na riziku i tehnološki neutralnim pristupom Opće uredbe o zaštiti podataka osigurava se razina zaštite podataka koja je prikladna za rješavanje pitanja rizika obrade, među ostalim s pomoću tehnologija u nastajanju.

Dionici konkretno navode da se načelima ograničenja svrhe i daljnje usklađene obrade, smanjenja količine podataka, ograničenja pohrane, transparentnosti i odgovornosti te uvjetima zakonitog provođenja postupaka automatiziranog donošenja odluka[106] u velikoj mjeri rješavaju problemi povezani s uporabom umjetne inteligencije.

Pristup Opće uredbe o zaštiti podataka koji je otporan na promjene u budućnosti i koji se temelji na riziku primjenjivat će se i u mogućem budućem okviru za umjetnu inteligenciju i pri provedbi podatkovne strategije. Cilj je podatkovne strategije poticanje dostupnosti podataka i stvaranje zajedničkih europskih podatkovnih prostora uz potporu udruženih usluga infrastrukture u oblaku. Kad je riječ o osobnim podacima, Općom uredbom o zaštiti podataka osigurava se glavni pravni okvir unutar kojeg se djelotvorna rješenja mogu osmisliti na pojedinačnoj osnovi ovisno o prirodi i sadržaju svakog podatkovnog prostora.

Općom uredbom o zaštiti podataka povećana je informiranost o zaštiti osobnih podataka unutar i izvan EU-a te se poduzeća potiču da prilagode svoje prakse kako bi pri stvaranju inovacija uzela u obzir načela zaštite podataka. Međutim, organizacije civilnog društva napominju da, iako se čini da je učinak Opće uredbe o zaštiti podataka na razvoj novih tehnologija pozitivan, prakse velikih digitalnih aktera još nisu temeljito preusmjerene prema obradi koja više pogoduje privatnosti. Snažna i učinkovita provedba Opće uredbe o zaštiti podataka u pogledu velikih digitalnih platformi i integriranih poduzeća, među ostalim u područjima kao što su internetsko oglašavanje i mikrociljanje, ključan je element za zaštitu pojedinaca.

Komisija analizira šira pitanja povezana s ponašanjem velikih digitalnih aktera na tržištu u kontekstu paketa Akta o digitalnim uslugama[107]. Kad je riječ o istraživanju u području društvenih medija, Komisija podsjeća da se platforme društvenih medija ne mogu koristiti Općom uredbom o zaštiti podataka kao izgovorom za ograničavanje pristupa istraživača i provjeravatelja činjenica neosobnim podacima, kao što su statistički podaci o poslanim ciljanim oglasima i kategorijama ljudi kojima su poslani, kriteriji za osmišljavanje tog ciljanja, informacije o lažnim računima itd.

---

[105] Kako su podsjetili Vijeće, Europski parlament i Odbor u svojim doprinosima evaluaciji.

[106] Međutim, dionici primjećuju da neki automatizirani postupci donošenja odluka u kontekstu umjetne inteligencije nisu obuhvaćeni člankom 22. Opće uredbe o zaštiti podataka.

[107] https://ec.europa.eu/commission/presscorner/detail/hr/ip_20_962

Pristup iz Opće uredbe o zaštiti podataka koji je tehnološki neutralan i otporan na promjene u budućnosti testiran je tijekom pandemije bolesti COVID-19 i pokazao se uspješnim. Njegova pravila temeljena na načelima poduprla su razvoj alata za suzbijanje i praćenje širenja virusa.

Izazovi koje treba riješiti

Razvoj i primjena novih tehnologija ne dovode ta načela u pitanje. Izazovi leže u razjašnjavanju načina primjene dokazanih načela na uporabu određenih tehnologija kao što su umjetna inteligencija, lanac blokova, internet stvari, prepoznavanje lica ili kvantno računalstvo.

U tom su kontekstu Europski parlament i Vijeće naglasili potrebu za stalnim praćenjem kako bi se pojasnilo kako se Opća uredba o zaštiti podataka primjenjuje na nove tehnologije i velika tehnološka poduzeća. Osim toga, dionici upozoravaju da je za procjenu toga ispunjava li Opća uredba o zaštiti podataka svoju svrhu i dalje potrebno stalno praćenje.

Dionici iz industrije naglašavaju da je za inovacije potrebno da se Opća uredba o zaštiti podataka primjenjuje na način koji se temelji na načelima, u skladu s time kako je osmišljena, a ne na krut i formalan način. Smatraju da bi smjernice Odbora o načinu primjene načela, koncepata i pravila Opće uredbe o zaštiti podataka na nove tehnologije kao što su umjetna inteligencija, lanac blokova ili internet stvari, uzimajući u obzir pristup temeljen na riziku, pomogle u pružanju pojašnjenja i veće pravne sigurnosti. Takvi neobvezujući pravni instrumenti mogu pratiti primjenu Opće uredbe o zaštiti podataka na nove tehnologije jer pružaju veću pravnu sigurnost i mogu se revidirati u skladu s tehnološkim razvojem. Neki dionici napominju da bi mogle biti korisne i sektorske smjernice o načinu primjene Opće uredbe o zaštiti podataka na nove tehnologije.

Odbor je izjavio da će nastaviti razmatrati učinak tehnologija u nastajanju na zaštitu osobnih podataka.

Dionici naglašavaju i važnost toga da regulatorna tijela temeljito razumiju način na koji se tehnologija upotrebljava i da se uključe u dijalog s industrijom o razvoju tehnologija u nastajanju. Smatraju da bi „regulatorno sigurno testno okruženje” – kao sredstvo za dobivanje smjernica o primjeni pravila – moglo biti zanimljiva opcija za ispitivanje novih tehnologija te pomoći poduzećima u primjeni tehničke i integrirane zaštite podataka u novim tehnologijama.

Kad je riječ o daljnjem političkom djelovanju, dionici preporučuju da bi se svi budući prijedlozi politika o umjetnoj inteligenciji trebali temeljiti na postojećim pravnim okvirima i da bi trebali biti usklađeni s Općom uredbom o zaštiti podataka. Prije predlaganja novih preskriptivnih pravila trebalo bi pažljivo i na temelju relevantnih dokaza procijeniti moguća specifična pitanja.

U Bijeloj knjizi Komisije o umjetnoj inteligenciji iznesen je niz mogućnosti politika o kojima se tražilo mišljenje dionika do 14. lipnja 2020. U pogledu prepoznavanja lica, tehnologije koja može znatno utjecati na prava pojedinaca, u Bijeloj knjizi podsjeća se na postojeći zakonodavni okvir i otvorena je javna rasprava o posebnim okolnostima kojima bi se, ako postoje, mogla opravdati uporaba umjetne inteligencije za prepoznavanje lica i druge svrhe povezane s biometrijskom identifikacijom na daljinu na javnim mjestima te o zajedničkim zaštitnim mjerama.

7 MEĐUNARODNI PRIJENOSI I GLOBALNA SURADNJA

7.1 Privatnost: globalno pitanje

Potreba za zaštitom osobnih podataka ne poznaje granice jer pojedinci diljem svijeta sve više njeguju i vrednuju privatnost i sigurnost svojih podataka.

Istodobno, važnost protoka podataka za pojedince, vlade, poduzeća i, općenitije, društvo u cjelini, neizbježna je činjenica u našem povezanom svijetu. Protok podataka čini sastavni dio trgovine, suradnje javnih tijela i društvenih interakcija. U situaciji pandemije bolesti COVID-19 vrlo je očito da su prijenos i razmjena osobnih podataka neophodni za mnoge važne aktivnosti, uključujući kontinuitet djelovanja vlade i poslovanja (jer omogućuju rad na daljinu i druga rješenja koja se uvelike oslanjaju na informacijske i komunikacijske tehnologije), suradnju u znanstvenim istraživanjima u području dijagnostike, liječenja i cjepiva te borbu protiv novih oblika kiberkriminaliteta kao što su internetske prijevare kojima se nude krivotvoreni lijekovi za koje se tvrdi da sprečavaju ili liječe bolest COVID-19.

U tom kontekstu zaštita privatnosti i olakšavanje protoka podataka moraju ići ruku pod ruku i više nego ikad prije. Zahvaljujući svojem režimu zaštite podataka u kojem se otvorenost prema međunarodnim prijenosima kombinira s visokom razinom zaštite pojedinaca EU može promicati siguran i pouzdan protok podataka. Opća uredba o zaštiti podataka već je sada referentna točka na međunarodnoj razini i zbog nje mnoge zemlje diljem svijeta razmatraju uvođenje modernih pravila o privatnosti.

Riječ je o istinski globalnom trendu koji je prisutan, primjerice, od Čilea do Južne Koreje, od Brazila do Japana, od Kenije do Indije, od Tunisa do Indonezije te od Kalifornije do Tajvana. Ta su kretanja iznimna ne samo s kvantitativnog nego i s kvalitativnog stajališta: mnogi zakoni o privatnosti koji su nedavno doneseni ili su u postupku donošenja temelje se na osnovnom skupu zajedničkih zaštitnih mjera, prava i provedbenih mehanizama koje dijeli EU. U svijetu koji je prečesto obilježen različitim, ako ne i proturječnim regulatornim pristupima, trend globalnog usklađivanja predstavlja vrlo pozitivno kretanje koje donosi nove mogućnosti za povećanje zaštite pojedinaca u Europi, a istodobno olakšava protok podataka i smanjuje transakcijske troškove za poslovne subjekte.

Kako bi iskoristila te mogućnosti i provela strategiju utvrđenu u Komunikaciji iz 2017. „Razmjena i zaštita osobnih podataka u globaliziranom svijetu”[108], Komisija je znatno pojačala svoj rad na međunarodnoj dimenziji privatnosti te pritom u potpunosti iskoristila raspoloživ „paket instrumenata” za prijenos, kako je objašnjeno u nastavku. To je uključivalo aktivnu suradnju s ključnim partnerima kako bi se postigao „zaključak o primjerenosti” te su se ostvarili važni rezultati, kao što je stvaranje najvećega svjetskog područja slobodnog i sigurnog protoka podataka između EU-a i Japana.

Osim što je radila na primjerenosti, Komisija je blisko surađivala s tijelima za zaštitu podataka unutar Odbora, kao i s drugim dionicima, kako bi iskoristila puni potencijal

[108] Komunikacija Komisije Europskom parlamentu i Vijeću „Razmjena i zaštita osobnih podataka u globaliziranom svijetu”, 10.1.2017. (COM(2017) 7 final).

fleksibilnih pravila za međunarodne prijenose iz Opće uredbe o zaštiti podataka. To se odnosi na modernizaciju instrumenata kao što su standardne ugovorne klauzule, razvoj programa certificiranja, kodeksâ ponašanja ili administrativnih dogovora za razmjenu podataka među javnim tijelima, kao i pojašnjenje ključnih pojmova povezanih s, primjerice, teritorijalnim područjem primjene pravila EU-a o zaštiti podataka ili uporabom takozvanih „odstupanja" u prijenosu osobnih podataka.

Naposljetku, Komisija je pojačala dijalog u nizu bilateralnih, regionalnih i multilateralnih foruma kako bi potaknula globalnu kulturu poštovanja privatnosti i razvila elemente usklađenosti među različitim sustavima privatnosti. Komisija bi u svojim naporima mogla računati na aktivnu potporu Europske službe za vanjsko djelovanje i mreže delegacija EU-a u trećim zemljama te misija u međunarodnim organizacijama. Time se osigurala i usklađenost i veća komplementarnost različitih aspekata vanjske dimenzije politika EU-a – od trgovine do novog partnerstva Afrike i EU-a.

7.2 Paket instrumenata za prijenos iz Opće uredbe o zaštiti podataka

Budući da se sve više privatnih i javnih subjekata oslanja na međunarodni protok podataka u okviru svojih rutinskih aktivnosti, postoji sve veća potreba za fleksibilnim instrumentima koji se mogu prilagoditi različitim sektorima, poslovnim modelima i situacijama prijenosa. Uzimajući u obzir te potrebe, Općom uredbom o zaštiti podataka nudi se modernizirani paket instrumenata kojim se olakšava prijenos osobnih podataka iz EU-a u treću zemlju ili međunarodnu organizaciju, a istodobno se osigurava da se na te podatke i dalje primjenjuje visoka razinu zaštite. Taj kontinuitet zaštite važan je s obzirom na to da se u današnjem svijetu podaci lako kreću preko granica, a zaštita zajamčena Općom uredbom o zaštiti podataka bila bi nepotpuna ako bi bila ograničena na obradu unutar EU-a.

U poglavlju V. Opće uredbe o zaštiti podataka zakonodavac je potvrdio strukturu pravila o prijenosu koja su već postojala na temelju Direktive 95/46: prijenosi podataka mogu se obavljati ako je Komisija donijela zaključak o primjerenosti u odnosu na treću zemlju ili međunarodnu organizaciju ili, ako nije, ako je voditelj obrade ili izvršitelj obrade u EU-u („izvoznik podataka") predvidio odgovarajuće zaštitne mjere, na primjer s pomoću ugovora s primateljem („uvoznik podataka"). Osim toga, zakonski razlozi za prijenose (takozvana odstupanja) i dalje su dostupni za posebne situacije za koje je zakonodavac odlučio da se radi ravnoteže interesa prijenos podataka omogućuje pod određenim uvjetima. Istodobno, reformom su postojeća pravila pojašnjena i pojednostavljena; na primjer propisani su detaljni uvjeti za donošenje zaključka o primjerenosti ili obvezujućih korporativnih pravila, zahtjevi za odobrenje ograničeni su na vrlo mali broj posebnih slučajeva i potpuno su ukinuti zahtjevi za obavješćivanje. Usto, uvedeni su novi alati za prijenos kao što su kodeksi ponašanja ili programi certificiranja te su proširene mogućnosti za uporabu postojećih instrumenata (npr. standardnih ugovornih klauzula).

Današnje digitalno gospodarstvo omogućuje stranim subjektima da (na daljinu, ali) izravno sudjeluju na unutarnjem tržištu EU-a i da se natječu za europske potrošače i njihove osobne podatke. Ondje gdje se ponuda robe ili usluga ili praćenje ponašanja posebno odnosi na Europljane, trebali bi poštovati pravo EU-a na isti način kao i subjekti iz EU-a. To se odražava u članku 3. Opće uredbe o zaštiti podataka, kojim se izravna primjenjivost pravila EU-a o zaštiti podataka proširuje na određene postupke

obrade voditelja obrade i izvršitelja obrade izvan EU-a. Time se jamče potrebne zaštitne mjere, a i jednaki uvjeti za sva poduzeća koja posluju na tržištu EU-a.

Široki doseg Opće uredbe o zaštiti podataka jedan je od razloga zbog kojih se njezini učinci osjećaju i u drugim dijelovima svijeta. Stoga su detaljne smjernice o teritorijalnom području primjene Opće uredbe o zaštiti podataka, koje je Odbor izdao nakon sveobuhvatnog javnog savjetovanja, važne kako bi se stranim subjektima pomoglo, među ostalim pružanjem konkretnih primjera, da utvrde podliježu li aktivnosti obrade izravno njezinim zaštitnim mjerama i koje su to aktivnosti[109].

Međutim, proširenje područja primjene prava EU-a o zaštiti podataka samo po sebi nije dovoljno da bi se zajamčilo njegovo poštovanje u praksi. Kao što je istaknulo i Vijeće[110], važno je osigurati usklađenost stranih subjekata i učinkovitu provedbu u odnosu na njih. U tom bi pogledu ključnu ulogu trebalo imati imenovanje predstavnika u EU-u (članak 27. stavci 1. i 2. Opće uredbe o zaštiti podataka) kojem se mogu obratiti pojedinci i nadzorna tijela, uz odgovorno trgovačko društvo koje djeluje iz inozemstva[111] ili umjesto njega. Taj pristup, koji se sve više primjenjuje i u drugim kontekstima[112], trebalo bi snažnije provoditi kako bi se poslala jasna poruka da nepostojanje poslovnog nastana u EU-u ne oslobađa strane subjekte njihovih odgovornosti prema Općoj uredbi o zaštiti podataka. Ako ti subjekti ne ispune svoju obvezu imenovanja predstavnika[113], nadzorna tijela trebala bi iskoristiti sve instrumente provedbe iz članka 58. Opće uredbe o zaštiti podataka (npr. javna upozorenja, privremene ili konačne zabrane obrade u EU-u, provedbu u odnosu na zajedničke voditelje obrade s poslovnim nastanom u EU-u).

Naposljetku, vrlo je važno da Odbor dovrši svoj rad na daljnjem pojašnjenju odnosa između članka 3. o izravnoj primjeni Opće uredbe o zaštiti podataka i pravila o međunarodnim prijenosima iz poglavlja V.[114]

Odluke o primjerenosti

Informacije koje su dostavili dionici potvrđuju da su odluke o primjerenosti i dalje ključan instrument kojim subjekti iz EU-a mogu na siguran način prenositi osobne

---

[109] EDPB, Smjernice 2/2018 o teritorijalnom području primjene Opće uredbe o zaštiti podataka, 12.11.2019. Smjernice se odnose na nekoliko pitanja iznesenih tijekom javnog savjetovanja, kao što je primjerice tumačenje kriterija za usmjeravanje i praćenje.

[110] Vidjeti Stajalište Vijeća i zaključke, točke 34., 35. i 38.

[111] Vidjeti članak 27. stavak 4. i uvodnu izjavu 80. Opće uredbe o zaštiti podataka („U slučaju da voditelj obrade ili izvršitelj obrade krši pravila, imenovani bi predstavnik trebao podlijegati postupku izvršavanja zakonodavstva”).

[112] Prijedlog Direktive Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila za imenovanje pravnih zastupnika za potrebe prikupljanja dokaza u kaznenim postupcima (COM(2018) 226 final), članak 3.; Prijedlog uredbe Europskog parlamenta i Vijeća o sprečavanju širenja terorističkih sadržaja na internetu (COM(2018) 640 final), članak 16. stavci 2. i 3.

[113] Prema jednom podnesku u okviru javnog savjetovanja, jedno od glavnih pitanja koje treba riješiti „je učinkovita provedba i stvarne posljedice za one koji su odlučili zanemariti taj zahtjev [...] Potrebno je posebno imati na umu da se time poduzeća s poslovnim nastanom u Uniji stavljaju u konkurentski nepovoljan položaj u odnosu na poduzeća koja ne poštuju zahtjeve s poslovnim nastanom izvan Unije koja trguju u Uniji.” Vidjeti „Poslovni partneri EU-a”, podnesak od 29. travnja 2020.

[114] To je istaknuto u nekoliko podnesaka u okviru javnog savjetovanja, primjerice u pogledu prijenosa osobnih podataka primateljima izvan EU-a koji su obuhvaćeni Općom uredbom o zaštiti podataka.

podatke trećim zemljama[115]. Takve odluke su najsveobuhvatnije, najjednostavnije i najisplativije rješenje za prijenose podataka jer se izjednačavaju s prijenosima unutar EU-a, čime se osigurava siguran i slobodan protok osobnih podataka bez dodatnih uvjeta ili potrebe za odobrenjem. Stoga se odlukama o primjerenosti otvaraju komercijalni kanali za subjekte iz EU-a i olakšava suradnja među javnim tijelima, dok se istodobno osigurava povlašteni pristup jedinstvenom tržištu EU-a. Oslanjajući se na praksu iz Direktive iz 1995., Općom uredbom o zaštiti podataka izričito se omogućuje utvrđivanje primjerenosti s obzirom na određeno državno područje neke treće zemlje ili određeni sektor ili industriju u trećoj zemlji (takozvana „djelomična" primjerenost).

Opća uredba o zaštiti podataka temelji se na iskustvu stečenom tijekom proteklih godina i na pojašnjenjima koja je pružio Sud utvrđivanjem detaljnog kataloga elemenata koje Komisija mora uzeti u obzir u svojoj procjeni. Standard primjerenosti zahtijeva razinu zaštite koja je usporediva s onom koja je osigurana u EU-u (ili joj je „bitno ekvivalentna")[116]. To uključuje sveobuhvatnu procjenu sustava treće zemlje u cjelini, uključujući sadržaj mjera zaštite privatnosti, njihovu djelotvornu primjenu i provedbu, kao i pravila o pristupu javnih tijela osobnim podacima, posebno za potrebe kaznenog progona i nacionalne sigurnosti[117].

To se odražava i u smjernicama koje je donijela nekadašnja Radna skupina iz članka 29. (i koje je potvrdio Odbor), posebno u takozvanom „referentnom dokumentu o primjerenosti", kojim se dodatno pojašnjavaju elementi koje Komisija mora uzeti u obzir pri provedbi procjene primjerenosti, među ostalim pružanjem pregleda „ključnih jamstava" za pristup javnih tijela osobnim podacima[118]. Potonje se posebno temelji na sudskoj praksi Europskog suda za ljudska prava. Iako standard „načelne istovjetnosti" ne uključuje ponavljanje pravila Unije od riječi do riječi („presliku"), s obzirom na to da se načini osiguravanja usporedive razine zaštite mogu razlikovati među različitim sustavima privatnosti, često odražavajući različite pravne tradicije, ipak zahtijeva visoku razinu zaštite.

Taj je standard opravdan činjenicom da se odlukom o primjerenosti u osnovi na treću zemlju proširuju koristi od jedinstvenog tržišta u smislu slobodnog protoka podataka. Međutim, to znači i da će ponekad postojati relevantne razlike između razine zaštite osigurane u predmetnoj trećoj zemlji u usporedbi s Općom uredbom o zaštiti podataka. Te razlike treba premostiti, primjerice pregovorima o dodatnim zaštitnim mjerama. Takve zaštitne mjere trebalo bi smatrati pozitivnima jer se njima dodatno jača zaštita dostupna pojedincima u EU-u. Komisija se usto slaže s Odborom da je

---

[115] Stajalište Vijeća i zaključci, točka 17.; doprinos Odbora, str. 5.–6. U više podnesaka u okviru javnog savjetovanja, uključujući podneske brojnih poslovnih udruženja (kao što su *Association française des entreprises privées* (Francuska udruga velikih poduzeća), Digitalna Europa, Globalni savez za podatke/Savez za softver (BSA), Udruženje za računalnu i komunikacijsku industriju (CCIA) ili Gospodarska komora SAD-a) pozivalo se na intenzivniji rad na zaključcima o primjerenosti, posebno s važnim trgovinskim partnerima.

[116] Presuda Suda Europske unije od 6. listopada 2015. u predmetu C-362/14, *Maximillian Schrems* protiv *Data Protection Commissioner* (*Schrems*), točke 73., 74. i 96. Vidjeti i uvodnu izjavu 104. Opće uredbe o zaštiti podataka koja se odnosi na standard načelne istovjetnosti.

[117] Članak 45. stavak 2. i uvodna izjava 104. Opće uredbe o zaštiti podataka. Vidjeti i *Schrems*, točke 75. i 91–91.

[118] *Adequacy Referential* (Referentni dokument o primjerenosti), WP 254 rev. 01, 6. veljače 2018. (dostupno na: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).

važno stalno pratiti njihovu primjenu u praksi, kao i učinkovitu provedbu koju obavljaju tijela za zaštitu podataka iz trećih zemalja[119].

U Općoj uredbi o zaštiti podataka pojašnjava se da su odluke o primjerenosti „živući instrumenti" koje bi trebalo stalno pratiti i periodično preispitivati[120]. U skladu s tim zahtjevima, Komisija redovito razmjenjuje mišljenja s relevantnim tijelima kako bi proaktivno pratila nova kretanja. Primjerice, nakon donošenje odluke o europsko-američkom sustavu zaštite privatnosti 2016.[121] Komisija je s predstavnicima Odbora provela tri godišnja preispitivanja kako bi ocijenila sve aspekte funkcioniranja okvira[122]. Ta su se preispitivanja temeljila na informacijama dobivenima od tijela SAD-a te na informacijama dobivenima od drugih dionika, kao što su tijela za zaštitu podataka EU-a, civilno društvo i trgovinska udruženja. Njima se omogućilo poboljšanje praktičnog funkcioniranja različitih elemenata okvira. U širem smislu, godišnja preispitivanja doprinijela su uspostavljanju opsežnijeg dijaloga s vladom SAD-a o privatnosti općenito, a posebno o ograničenjima i zaštitnim mjerama u pogledu nacionalne sigurnosti.

U okviru svoje prve evaluacije Opće uredbe o zaštiti podataka Komisija je dužna preispitati i odluke o primjerenosti donesene u skladu s Direktivom iz 1995.[123] Službe Komisije sudjelovale su u intenzivnom dijalogu sa svakom od 11 predmetnih zemalja i područja kako bi ocijenile kako su se njihovi sustavi zaštite osobnih podataka razvili od donošenja odluke o primjerenosti te ispunjavaju li standarde utvrđene Općom uredbom o zaštiti podataka. Potreba da se osigura kontinuitet takvih odluka, s obzirom na to da su ključan instrument za trgovinu i međunarodnu suradnju, jedan je od čimbenika zbog kojih je nekoliko tih zemalja i područja moderniziralo i ojačalo svoje

---

[119] Doprinos Odbora, str. 5.–6.

[120] Člankom 45. stavcima 4. i 5. Opće uredbe o zaštiti podataka od Komisije se zahtijeva da kontinuirano prati kretanja u trećim zemljama i da redovito, najmanje svake četiri godine, preispituje zaključak o primjerenosti. Njima se Komisiji daje i ovlast za stavljanje izvan snage, izmjenu ili suspenziju odluke o primjerenosti ako utvrdi da dotična zemlja ili međunarodna organizacija više ne osigurava odgovarajuću razinu zaštite. Člankom 97. stavkom 2. točkom (a) Opće uredbe o zaštiti podataka od Komisije se nadalje zahtijeva da Europskom parlamentu i Vijeću do 2020. podnese izvješće o evaluaciji. Vidjeti i presudu Suda Europske unije od 6. listopada 2015. u predmetu C-362/14, *Maximillian Schrems* protiv *Data Protection Commissioner*, točka 76.

[121] Provedbena odluka Komisije (EU) 2016/1250 od 12. srpnja 2016. o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti u skladu s Direktivom 95/46/EZ Ta odluka o primjerenosti poseban je slučaj koji se, u nedostatku općeg zakonodavstva o zaštiti podataka u SAD-u, oslanja na obveze koje su preuzela trgovačka društva sudionici (koje se izvršavaju u skladu sa zakonodavstvom SAD-a) kako bi se primijenio standard zaštite podataka utvrđen tim dogovorom. Nadalje, europsko-američki sustav zaštite privatnosti temelji se na posebnim izjavama i jamstvima vlade SAD-a u pogledu pristupa u svrhu nacionalne sigurnosti kojima se podupire zaključak o primjerenosti.

[122] Preispitivanja su provedena 2017. (Izvješće Komisije Europskom parlamentu i Vijeću o prvom godišnjem preispitivanju funkcioniranja europsko-američkog sustava zaštite privatnosti, (COM(2017) 611 final), 2018. (Izvješće Komisije Europskom parlamentu i Vijeću o drugom godišnjem preispitivanju funkcioniranja europsko-američkog sustava zaštite privatnosti, (COM(2018) 860 final) i 2019. (Izvješće Komisije Europskom parlamentu i Vijeću o trećem godišnjem preispitivanju funkcioniranja europsko-američkog sustava zaštite privatnosti, (COM(2019) 495 final).

[123] Te postojeće odluke o primjerenosti odnose se na zemlje koje su blisko povezane s Europskom unijom i njezinim državama članicama (Švicarska, Andora, Farski Otoci, Guernsey, Jersey, Otok Man), važne trgovinske partnere (npr. Argentina, Kanada, Izrael) i zemlje koje su imale pionirsku ulogu u razvoju zakona o zaštiti podataka u svojoj regiji (Novi Zeland, Urugvaj).

zakone o privatnosti. To je svakako dobrodošao razvoj događaja. S nekima od tih zemalja i državnih područja raspravlja se o dodatnim zaštitnim mjerama kako bi se riješile relevantne razlike u zaštiti.

Međutim, s obzirom na to da Sud u presudi koja se očekuje 16. srpnja može pružiti pojašnjenja koja bi mogla biti relevantna za određene elemente standarda primjerenosti, Komisija će zasebno izvijestiti o evaluaciji navedenih 11 odluka o primjerenosti nakon što Sud donese presudu u tom predmetu[124].

Provedbom strategije utvrđene u Komunikaciji iz 2017. „Razmjena i zaštita osobnih podataka u globaliziranom svijetu" Komisija se uključila i u nove dijaloge o primjerenosti[125]. Tako su već ostvareni znatni rezultati u koje su uključeni glavni partneri EU-a. U siječnju 2019. Komisija je donijela odluku o primjerenosti za Japan, koja se temelji na visokom stupnju konvergencije, među ostalim putem konkretnih zaštitnih mjera, primjerice u području daljnjih prijenosa te uspostavom mehanizma za istraživanje i rješavanje pritužbi pojedinaca u vezi s pristupom vlade osobnim podacima za potrebe kaznenog progona i nacionalne sigurnosti.

Kao prvi zaključak o primjerenosti donesen na temelju Opće uredbe o zaštiti podataka, okvir dogovoren s Japanom koristan je presedan za buduće odluke[126]. To uključuje i činjenicu da je Japan uzvratio zaključkom o primjerenosti za EU. Ti zaključci o uzajamnoj primjerenosti zajedno čine najveće područje sigurnog i slobodnog protoka osobnih podataka na svijetu, čime se nadopunjuje Sporazum o gospodarskom partnerstvu između EU-a i Japana. Sporazumom se zapravo svake godine podupire trgovina robom u iznosu od približno 124 milijarde EUR i trgovina uslugama u iznosu od 42,5 milijardi EUR.

Postupak procjene primjerenosti s Južnom Korejom također je u poodmakloj fazi. Važan je rezultat toga nedavna zakonodavna reforma Južne Koreje koja je dovela do uspostave neovisnog tijela za zaštitu podataka s velikim provedbenim ovlastima. To pokazuje kako dijalog o primjerenosti može doprinijeti većoj usklađenosti između pravila o zaštiti podataka EU-a i pravila strane zemlje.

124 Predmet C-311/18, *Data Protection Commissioner* protiv *Facebook Ireland Limited, Maximillian Schrems* („Schrems II"), odnosi se na zahtjev za prethodnu odluku o takozvanim standardnim ugovornim klauzulama. Međutim, Sud može dodatno pojasniti određene elemente standarda primjerenosti. Rasprava u ovom predmetu održana je 9. srpnja 2019., a presuda je najavljena za 16. srpnja 2020.

125 Vidjeti *supra* bilješku 109. Komisija je objasnila da će se pri procjeni s kojim bi trećim zemljama trebalo nastaviti dijalog o primjerenosti u obzir uzeti sljedeći kriteriji: i. opseg (stvarnih ili potencijalnih) trgovinskih odnosa EU-a s trećom zemljom, uključujući postojanje sporazuma o slobodnoj trgovini ili tekućih pregovora; ii. opseg protoka osobnih podataka iz EU-a koji odražava zemljopisne i/ili kulturne veze; iii. pionirska uloga zemlje u području privatnosti i zaštite podataka koja bi mogla poslužiti kao primjer drugim zemljama u njezinoj regiji i iv. sveukupni politički odnos s tom zemljom, posebno u pogledu promicanja zajedničkih vrijednosti i ciljeva na međunarodnoj razini.

126 Europski parlament, Rezolucija od 13. prosinca 2018. o primjerenosti zaštite osobnih podataka koju pruža Japan (2018/2979 (RSP)), točka 27.; doprinos Odbora, str. 5.–6.

Komisija se u potpunosti slaže s dionicima da bi trebalo pojačati dijalog s odabranim trećim zemljama s obzirom na moguće nove zaključke o primjerenosti[127]. Aktivno istražuje tu mogućnost s drugim važnim partnerima u Aziji, Latinskoj Americi i susjedstvu na temelju trenutačnog trenda prema uzlaznoj globalnoj konvergenciji standarda zaštite podataka. Na primjer, sveobuhvatno zakonodavstvo o zaštiti privatnosti doneseno je ili se nalazi u naprednoj fazi zakonodavnog postupka u Latinskoj Americi (Brazil, Čile), a do obećavajućih pomaka došlo je u Aziji (npr. u Indiji, Indoneziji, Maleziji, Šri Lanki, Tajvanu i Tajlandu), Africi (npr. u Etiopiji i Keniji) te u europskom istočnom i južnom susjedstvu (npr. u Gruziji i Tunisu). Gdje je god moguće, Komisija će raditi na donošenju sveobuhvatnih odluka o primjerenosti koje obuhvaćaju i privatni i javni sektor[128].

Nadalje, Općom uredbom o zaštiti podataka uvedena je i mogućnost da Komisija donese zaključke o primjerenosti za međunarodne organizacije. U vrijeme kada neke međunarodne organizacije uvode sveobuhvatna pravila, kao i mehanizme koji omogućuju neovisan nadzor i pravnu zaštitu, kako bi modernizirala svoje sustave zaštite podataka, ta bi se mogućnost prvi put mogla istražiti.

Primjerenost igra i važnu ulogu u kontekstu odnosa s Ujedinjenom Kraljevinom nakon Brexita, pod uvjetom da su ispunjeni svi primjenjivi uvjeti. Ona omogućuje trgovinu, uključujući digitalnu trgovinu, te je važan preduvjet za blisku i ambicioznu suradnju u području kaznenog progona i sigurnosti[129]. Nadalje, s obzirom na važnost protoka podataka s Ujedinjenom Kraljevinom i njezinu blizinu tržištu EU-a, visok stupanj konvergencije pravila o zaštiti podataka u Ujedinjenoj Kraljevini i Uniji važan je element za osiguravanje ravnopravnih uvjeta. U skladu s Političkom izjavom o budućem odnosu EU-a i Ujedinjene Kraljevine, Komisija trenutačno provodi procjenu primjerenosti u skladu s Općom uredbom o zaštiti podataka i Direktivom o zaštiti pojedinaca u vezi s obradom osobnih podataka za potrebe kaznenog progona[130]. S obzirom na autonomnu i jednostranu prirodu procjene primjerenosti, ti pregovori slijede zaseban put u odnosu na pregovore o sporazumu o budućem odnosu između EU-a i Ujedinjene Kraljevine.

Naposljetku, Komisija pozdravlja činjenicu da druge zemlje uspostavljaju mehanizme za prijenos podataka koji su slični zaključku o primjerenosti. Pritom su EU i zemlje za koje je Komisija donijela odluku o primjerenosti često priznate kao sigurna odredišta

[127] Vidjeti npr. Rezoluciju Europskog parlamenta od 12. prosinca 2017. „Ususret strategiji digitalne trgovine" (2017/2065(INI)), točke 8. i 9.; Stajalište Vijeća i zaključci o primjeni Opće uredbe o zaštiti podataka (GDPR), 19.12.2019. (14994/1/19), točka 17.; Doprinos Odbora, str. 5.

[128] Kako je zatražilo i Vijeće, vidjeti Stajalište Vijeća i zaključke o primjeni Opće uredbe o zaštiti podataka (GDPR), 19.12.2019. (14994/1/19), točke 17. i 40. Međutim, to zahtijeva ispunjavanje uvjeta za zaključak o primjerenosti u pogledu prijenosa podataka javnim tijelima, među ostalim u vezi s neovisnim nadzorom.

[129] Vidjeti pregovaračke smjernice priložene Odluci Vijeća o odobravanju otvaranja pregovora s Ujedinjenom Kraljevinom Velike Britanije i Sjeverne Irske o novom sporazumu o partnerstvu (ST 5870/20 ADD 1 REV 3), točke 13. i 118.

[130] Vidjeti revidirani tekst političke izjave kojom se uspostavlja okvir za buduće odnose između Europske unije i Ujedinjene Kraljevine, kako je dogovoreno na razini pregovarača 17. listopada 2019., točke od 8. do 10. (dostupno na: https://ec.europa.eu/commission/sites/beta-political/files/revised_political_declaration.pdf).

za prijenose[131]. Sve veći broj zemalja koje imaju koristi od odluka EU-a o primjerenosti, s jedne strane, i taj oblik priznavanja od strane drugih zemalja, s druge strane, mogli bi dovesti do stvaranja mreže zemalja u kojima se podaci mogu kretati slobodno i sigurno. Komisija to smatra dobrodošlim razvojem događaja kojim će se dodatno povećati koristi od odluke o primjerenosti za treće zemlje i doprinijeti globalnoj konvergenciji. Ta vrsta sinergija također može doprinijeti razvoju okvira za siguran i slobodan protok podataka, primjerice u kontekstu inicijative o „slobodnom protoku podataka uz puno povjerenje" (vidjeti u nastavku).

Odgovarajuće zaštitne mjere

Općom uredbom o zaštiti podataka predviđen je niz drugih instrumenata prijenosa koji nadilaze sveobuhvatno rješenje zaključka o primjerenosti. Fleksibilnost tog „paketa instrumenata" prikazana je u članku 46. Opće uredbe o zaštiti podataka, kojim se uređuju prijenosi podataka na temelju „odgovarajućih zaštitnih mjera", uključujući provediva prava ispitanika i učinkovitu sudsku zaštitu. Kako bi se zajamčile odgovarajuće zaštitne mjere, dostupni su različiti instrumenti radi zadovoljavanja potreba komercijalnih subjekata i javnih tijela povezanih s prijenosom.

- Standardne ugovorne klauzule (SUK-ovi)

Prva skupina tih instrumenata odnosi se na ugovorne alate koji mogu biti prilagođene *ad hoc* klauzule o zaštiti podataka koje su dogovorili izvoznik podataka iz EU-a i uvoznik podataka izvan EU-a koje je odobrilo nadležno tijelo za zaštitu podataka (članak 46. stavak 3. točka (a) Opće uredbe o zaštiti podataka) ili ogledne klauzule koje je prethodno odobrila Komisija (članak 46. stavak 2. točke (c) i (d) Opće uredbe o zaštiti podataka[132]). Najvažniji su od tih instrumenata takozvane standardne ugovorne klauzule (SUK-ovi), tj. modeli klauzula o zaštiti podataka koje izvoznik podataka i uvoznik podataka dobrovoljno mogu uključiti u svoje ugovorne aranžmane (npr. ugovor o pružanju usluga kojim se zahtijeva prijenos osobnih podataka) i kojima se utvrđuju zahtjevi povezani s odgovarajućim zaštitnim mjerama.

SUK-ovi su daleko najčešće upotrebljavani mehanizam za prijenos podataka[133]. Tisuće poduzeća iz EU-a oslanjaju se na SUK-ove kako bi svojim klijentima, dobavljačima, partnerima i zaposlenicima pružile širok raspon usluga, uključujući usluge koje su ključne za funkcioniranje gospodarstva. Njihova široka uporaba upućuje na to da su vrlo korisni poduzećima u nastojanjima da se usklade, a posebno su korisni poduzećima koja nemaju resurse za pregovaranje o pojedinačnim ugovorima sa svakim od svojih komercijalnih partnera. Zahvaljujući normizaciji i prethodnom odobrenju, SUK-ovima se poduzećima osigurava alat koji je jednostavan

[131] Na primjer, Argentina, Kolumbija, Izrael, Švicarska ili Urugvaj.

[132] Standardne ugovorne klauzule (SUK-ovi) za međunarodne prijenose uvijek zahtijevaju odobrenje Komisije, ali ih može pripremiti bilo sama Komisija bilo nacionalno tijelo za zaštitu podataka. Svi postojeći SUK-ovi pripadaju prvoj kategoriji.

[133] Prema Godišnjem izvješću o upravljanju privatnošću IAPP-EY 2019, „najpopularniji od tih alata [za prijenos] – u odnosu na proteklu godinu – nesumnjivo su standardne ugovorne klauzule: u ovogodišnjem istraživanju 88 % ispitanika navelo je SUK-ove kao glavnu metodu za izvanteritorijalne prijenose podataka, nakon čega slijedi usklađenost sa sporazumom o europsko-američkom sustavu zaštite privatnosti (60 %). Kad je riječ o ispitanicima koji prenose podatke iz EU-a u Ujedinjenu Kraljevinu (52 %), 91 % navodi da za potrebe usklađenosti prijenosa podataka nakon Brexita namjerava primjenjivati SUK-ove."

za primjenu i s pomoću kojeg mogu ispuniti zahtjeve u pogledu zaštite podataka u kontekstu prijenosa.

Postojeći skupovi SUK-ova[134] doneseni su i odobreni na temelju Direktive iz 1995. Ti SUK-ovi ostaju na snazi dok ih se prema potrebi ne izmijeni, zamijeni ili stavi izvan snage odlukom Komisije (članak 46. stavak 5. Opće uredbe o zaštiti podataka). Općom uredbom o zaštiti podataka proširuju se mogućnosti uporabe SUK-ova unutar EU-a i za međunarodne prijenose. Komisija surađuje s dionicima kako bi iskoristila te mogućnosti i ažurirala postojeće klauzule[135]. Kako bi se osiguralo da buduće oblikovanje SUK-ova bude svrsishodno, Komisija je prikupljala povratne informacije o iskustvima dionika sa SUK-ovima preko „Skupine s više dionika za Opću uredbu o zaštiti podataka" i putem posebne radionice održane u rujnu 2019., ali i s pomoću višestrukih kontakata s poduzećima koja se koriste SUK-ovima i organizacijama civilnog društva. Odbor ažurira i niz smjernica koje bi mogle biti relevantne za preispitivanje SUK-ova, na primjer o pojmovima voditelja obrade i izvršitelja obrade.

Službe Komisije trenutačno rade na reviziji SUK-ova na temelju primljenih povratnih informacija. U tom je kontekstu utvrđeno nekoliko područja u kojima su potrebna poboljšanja, posebno u pogledu sljedećih aspekata:

1. ažuriranje SUK-ova s obzirom na nove zahtjeve uvedene Općom uredbom o zaštiti podataka, kao što su oni koji se odnose na odnos voditelja obrade i izvršitelja obrade u skladu s člankom 28. Opće uredbe o zaštiti podataka (posebno u vezi s obvezama izvršitelja obrade) te obveze uvoznika podataka u pogledu transparentnosti (kad je riječ o potrebnim informacijama koje treba pružiti ispitaniku) itd.;
2. rješavanje niza scenarija prijenosa koji nisu obuhvaćeni trenutačnim SUK-ovima, kao što je prijenos podataka od izvršitelja obrade iz EU-a do (pod)izvršitelja obrade izvan EU-a, ali i, na primjer, situacije u kojima se voditelj obrade nalazi izvan EU-a[136];
3. bolje odražavanje stvarnih postupaka obrade u modernom digitalnom gospodarstvu, u kojem takve operacije često uključuju više uvoznika i izvoznika podataka, duge i često složene lance obrade, promjenjive poslovne odnose, itd. Kako bi se riješile takve situacije, neka su od razmatranih rješenja, na primjer,

[134] Komisija trenutačno donosi tri skupa standardnih ugovornih klauzula za prijenos osobnih podataka trećim zemljama: dva za prijenose od voditelja obrade iz EGP-a do voditelja obrade izvan EGP-a i jedan za prijenose od voditelja obrade iz EGP-a do izvršitelja obrade izvan EGP-a. Izmijenjeni su 2016. u skladu s presudom Suda u predmetu *Schrems I* (C-362/14) kako bi se uklonila sva ograničenja za nadležna nadzorna tijela u izvršavanju njihovih ovlasti nadzora prijenosa podataka. Vidjeti: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_hr

[135] Vidjeti i Doprinos Odbora, str. 6.–7. Isto tako, Vijeće je pozvalo Komisiju „da ih [SUK-ove] u dogledno vrijeme preispita i izmijeni kako bi se u obzir uzele potrebe voditeljâ i izvršiteljâ obrade". Vidjeti Stajalište Vijeća i zaključke.

[136] Nekoliko podnesaka tijekom javnog savjetovanja sadržavalo je komentare povezane s tim posljednjim scenarijem, u kojima se više puta izražavala zabrinutost da bi se zahtijevanjem da izvršitelji obrade iz EU-a osiguraju odgovarajuće zaštitne mjere u odnosu s voditeljima obrade izvan EU-a izvršitelje obrade iz EU-a stavilo u konkurentski nepovoljan položaj u odnosu na strane izvršitelje obrade koji nude slične usluge.

mogućnost da se potpisivanje SUK-ova osigura većem broju stranaka ili pristupanje novih stranaka tijekom trajanja ugovora.

Pri rješavanju tih pitanja Komisija razmatra i načine kako trenutačnu „arhitekturu" SUK-ova učiniti pristupačnijom korisnicima, na primjer tako da se višestruki skupovi SUK-ova zamijene jedinstvenim sveobuhvatnim dokumentom. Izazov koji se pritom javlja je postići dobru ravnotežu između potrebe za jasnoćom i određenim stupnjem standardizacije s jedne strane i potrebne fleksibilnosti kojom će se omogućiti da klauzule koristi više subjekata s različitim zahtjevima, u različitim kontekstima i za različite vrste prijenosa, s druge strane.

Još je jedan važan aspekt koji treba razmotriti moguća potreba da se, s obzirom na trenutačne postupke pred Sudom[137], dodatno pojasne zaštitne mjere u pogledu pristupa stranih javnih tijela podacima prenesenima na temelju SUK-ova, posebno u svrhu nacionalne sigurnosti. To može uključivati zahtjev da uvoznik ili izvoznik podataka, ili i uvoznik i izvoznik podataka, poduzmu mjere i pojasne ulogu tijela za zaštitu podataka u tom kontekstu. Iako je revizija SUK-ova dobro uznapredovala, potrebno je pričekati presudu Suda koja će odražavati moguće dodatne zahtjeve u revidiranim klauzulama prije nego što se nacrt odluke o novom skupu SUK-ova može podnijeti Odboru na mišljenje i predložiti njegovo donošenje u „postupku komitologije"[138].

Komisija je istodobno u kontaktu s međunarodnim partnerima koji razvijaju slične alate[139]. Tim bi se dijalogom, kojim se omogućuje razmjena iskustava i najboljih primjera iz prakse, moglo znatno doprinijeti daljnjem razvoju konvergencije „na terenu" i tako olakšati usklađenost s pravilima o prekograničnom prijenosu poduzećima koja posluju u različitim regijama svijeta.

- Obvezujuća korporativna pravila

Još su jedan važan instrument takozvana obvezujuća korporativna pravila. To su pravno obvezujuće politike i dogovori koji se primjenjuju na članove korporativne grupe, uključujući njihove zaposlenike (članak 46. stavak 2. točka (b) i članak 47. Opće uredbe o zaštiti podataka). Uporabom obvezujućih korporativnih pravila omogućuje se slobodno kretanje osobnih podataka među različitim članovima grupe diljem svijeta, pri čemu više ne postoji potreba za ugovornim odnosima između svakog korporativnog subjekta, a istodobno se osigurava usklađenost s visokom razinom zaštite osobnih podataka koja je jednaka u cijeloj grupi. Ta su pravila posebno dobro rješenje za složene i velike korporativne grupe te za blisku suradnju

[137] Vidjeti predmet *Schrems II*.

[138] U skladu s člankom 46. stavkom 2. točkom (c) Opće uredbe o zaštiti podataka, standardne ugovorne klauzule moraju se donijeti postupkom ispitivanja utvrđenim člankom 5. Uredbe (EU) br. 182/2011 Europskog parlamenta i Vijeća od 16. veljače 2011. o utvrđivanju pravila i općih načela u vezi s mehanizmima nadzora država članica nad izvršavanjem provedbenih ovlasti Komisije – SL L 55, 28.2.2011., str. 13.–18. To posebno uključuje pozitivnu odluku odbora sastavljenog od predstavnika država članica.

[139] Primjerice, to uključuje aktivnosti koje trenutačno provode države članice ASEAN-a kako bi se razvili „modeli ugovornih klauzula ASEAN-a". Vidjeti ASEAN, Ključni pristupi za mehanizam prekograničnog protoka podataka ASEAN-a (dostupno na: https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf).

među poduzećima koja razmjenjuju podatke u više jurisdikcija. Za razliku od Direktive iz 1995., u skladu s Općom uredbom o zaštiti podataka, obvezujuća korporativna pravila može primjenjivati skupina poduzeća koja se bave zajedničkom gospodarskom djelatnošću, ali ne pripadaju istoj korporativnoj grupi.

U pogledu postupka, obvezujuća korporativna pravila moraju odobriti nadležna tijela za zaštitu podataka na temelju neobvezujućeg mišljenja Odbora[140]. Kako bi vodio taj postupak, Odbor je preispitao referentne podatke o obvezujućim korporativnim pravilima (kojima se utvrđuju materijalni standardi) za voditelje obrade[141] i izvršitelje obrade[142] s obzirom na Opću uredbu o zaštiti podataka te nastavlja ažurirati te dokumente na temelju praktičnog iskustva koje su stekla nadzorna tijela. Donio je i razne smjernice kako bi pomogao podnositeljima zahtjeva i pojednostavio postupak podnošenja zahtjeva i odobravanja obvezujućih korporativnih pravila[143]. Prema informacijama Odbora, trenutačno se više od 40 obvezujućih korporativnih pravila nalazi u pripremi za odobrenje, a očekuje se da će polovina biti odobrena do kraja 2020.[144] Važno je da tijela za zaštitu podataka nastave raditi na daljnjem pojednostavnjenju postupka odobravanja jer dionici često navode da je trajanje takvih postupaka praktična prepreka široj uporabi obvezujućih korporativnih pravila.

Naposljetku, kada je posebno riječ o obvezujućim korporativnim pravilima koja je odobrilo tijelo za zaštitu podataka Ujedinjene Kraljevine – Ured povjerenika za informiranje – trgovačka društva moći će ih i dalje upotrebljavati kao valjani mehanizam prijenosa u skladu s Općom uredbom o zaštiti podataka nakon isteka prijelaznog razdoblja na temelju Sporazuma o povlačenju između EU-a i Ujedinjene Kraljevine, ali samo ako se izmijene tako da se svaka veza s pravnim poretkom Ujedinjene Kraljevine zamijeni odgovarajućim upućivanjima na korporativne subjekte i nadležna tijela unutar EU-a. Odobrenje svih novih obvezujućih korporativnih pravila trebalo bi zatražiti od jednog od nadzornih tijela u EU-u.

- Mehanizmi certificiranja i kodeksi ponašanja

Osim modernizacije i proširenja primjene već postojećih alata za prijenos, Općom uredbom o zaštiti podataka uvedeni su i novi instrumenti, čime se proširuju mogućnosti za međunarodne prijenose. To pod određenim uvjetima uključuje uporabu odobrenih kodeksa ponašanja i mehanizama certificiranja (kao što su pečati ili oznake privatnosti) kako bi se osigurale odgovarajuće zaštitne mjere. To su alati koji se primjenjuju „odozdo prema gore" i koji omogućuju prilagođena rješenja, kao mehanizam opće odgovornosti (vidjeti članke od 40. do 42. Opće uredbe o zaštiti podataka), posebno kad je riječ o međunarodnim prijenosima podataka, koji odražavaju, primjerice, posebna obilježja i potrebe određenog sektora ili industrije ili određenih tokova podataka. Kodeksima ponašanja mogu se usklađivati obveze i rizici

---

[140] Pregled dosadašnjih mišljenja Europskog odbora za zaštitu podataka dostupan je na: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_hr.

[141] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109.

[142] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110.

[143] Ti su dokumenti doneseni (donijela ih je nekadašnja Radna skupina iz članka 29.) nakon stupanja na snagu Opće uredbe o zaštiti podataka, ali prije isteka prijelaznog razdoblja. Vidjeti WP263 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056); WP264 (https://edpb.europa.eu/sites/edpb/files/files/file2/wp264_art29_wp_bcr-c_application_form.pdf); WP265 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623848).

[144] Doprinos Odbora, str. 7.

pa oni mogu biti vrlo koristan i troškovno učinkovit način na koji mala i srednja poduzeća mogu ispuniti svoje obveze iz Opće uredbe o zaštiti podataka.

Kad je riječ o mehanizmima certificiranja, iako je Odbor donio smjernice kojima se potiče njihova uporaba u EU-u, njegov rad na razvoju kriterija za odobravanje mehanizama certificiranja kao alatâ za međunarodni prijenos još nije dovršen. Isto vrijedi i za kodekse ponašanja, a Odbor trenutačno radi na smjernicama za njihovu uporabu kao alata za prijenose.

Budući da je subjektima važno osigurati širok raspon instrumenata prijenosa prilagođenih njihovim potrebama i da je mehanizmima certificiranja posebno svojstven potencijal za olakšavanje prijenosa podataka uz istodobno osiguravanje visoke razine zaštite podataka, Komisija poziva Odbor da što prije dovrši svoje smjernice u tom pogledu. To se odnosi i na materijalne aspekte (kriterije) i na postupovne aspekte (odobrenje, praćenje itd.). Dionici su izrazili velik interes za te mehanizme prijenosa i trebali bi moći u potpunosti iskoristiti paket instrumenata Opće uredbe o zaštiti podataka. Smjernicama Odbora doprinijelo bi se i promicanju modela EU-a za zaštitu podataka na globalnoj razini te bi se potaknula konvergencija, s obzirom na to da se drugi sustavi zaštite privatnosti koriste sličnim instrumentima.

Iz trenutačnih napora u pogledu normizacije u području privatnosti mogu se izvući vrijedne pouke na europskoj i međunarodnoj razini. Zanimljiv je primjer nedavno objavljena međunarodna norma ISO 27701[145] čiji je cilj pomoći poduzećima da ispune zahtjeve u pogledu privatnosti i upravljaju rizicima povezanima s obradom osobnih podataka kroz primjenu „sustavâ za upravljanje informacijama o privatnosti”. Iako certificiranje u skladu s normom kao takvo ne ispunjava zahtjeve iz članaka 42. i 43. Opće uredbe o zaštiti podataka, primjenom sustavâ za upravljanje informacijama o privatnosti može se doprinijeti odgovornosti, među ostalim u kontekstu međunarodnih prijenosa podataka.

- Međunarodni sporazumi i administrativni dogovori

Općom uredbom o zaštiti podataka omogućuje se i osiguravanje odgovarajućih zaštitnih mjera za prijenose podataka između tijela javne vlasti ili javnih tijela na temelju međunarodnih sporazuma (članak 46. stavak 2. točka (a)) ili administrativnih dogovora (članak 46. stavak 3. točka (b)). Iako oba instrumenta moraju jamčiti isti ishod u smislu zaštitnih mjera, uključujući provediva prava ispitanika i učinkovitu sudsku zaštitu, razlikuju se u pogledu pravne prirode i postupka donošenja.

Za razliku od međunarodnih sporazuma kojima se stvaraju obvezujuće obveze na temelju međunarodnog prava, administrativni dogovori (npr. u obliku memoranduma o razumijevanju) obično nisu obvezujući i stoga zahtijevaju prethodno odobrenje nadležnog tijela za zaštitu podataka (vidjeti i uvodnu izjavu 108. Opće uredbe o zaštiti podataka). Jedan rani primjer odnosi se na administrativni dogovor za prijenos osobnih podataka između financijskih nadzornih tijela unutar EGP-a i izvan EGP-a koja surađuju u okviru Međunarodne organizacije nadzornih tijela za vrijednosne

[145] Popis posebnih zahtjeva koji čine ovu normu ISO dostupan je na: https://www.iso.org/standard/71670.html.

papire (IOSCO), o čemu je Odbor dao svoje mišljenje[146] početkom 2019. Od tada je Odbor dodatno razvio svoje tumačenje „minimalnih zaštitnih mjera" koje međunarodni sporazumi (o suradnji) i administrativni dogovori između tijela javne vlasti ili javnih tijela (uključujući međunarodne organizacije) moraju osigurati u skladu sa zahtjevima iz članka 46. Opće uredbe o zaštiti podataka. Odbor je 18. siječnja 2020. donio nacrt smjernica[147], čime je odgovorio na zahtjev država članica za dodatnim pojašnjenjima i smjernicama o tome što se može smatrati odgovarajućim zaštitnim mjerama za prijenose između tijela javne vlasti[148]. Odbor snažno preporučuje da se tijela javne vlasti koriste ovim smjernicama kao referentnom točkom za pregovore s trećim stranama[149].

Smjernice pokazuju fleksibilnost u oblikovanju takvih instrumenata, uključujući važne aspekte kao što su nadzor[150] i pravna zaštita[151]. Time bi se javnim tijelima trebalo omogućiti da prevladaju poteškoće u, primjerice, osiguravanju provedivih prava ispitanika putem neobvezujućih dogovora. Važan je element takvih dogovora stalno praćenje koje provodi nadležno tijelo za zaštitu podataka, uz potporu zahtjeva za informacije i vođenje evidencije, te suspenzija protoka podataka ako se u praksi više ne mogu osigurati odgovarajuće zaštitne mjere.

Odstupanja

---

[146] Europski odbor za zaštitu podataka, Mišljenje 4/2019 o Nacrtu administrativnog dogovora za prijenos osobnih podataka između financijskih nadzornih tijela Europskoga gospodarskog prostora (EGP) i financijskih nadzornih tijela izvan EGP-a, 12.2.2019.

[147] Europski odbor za zaštitu podataka, Smjernice 2/2020 o članku 46. stavku 2. točki (a) i članku 46. stavku 3. točki (b) Uredbe 2016/679 za prijenose osobnih podataka između tijela javne vlasti i javnih tijela EGP-a i izvan EGP-a (nacrt je dostupan na: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_hr). Prema mišljenju Odbora, „[n]adležno [nadzorno tijelo] temeljit će svoje ispitivanje na općim preporukama navedenima u ovim smjernicama, ali može zatražiti i više jamstava ovisno o konkretnom slučaju". Odbor je podnio taj nacrt smjernica na javno savjetovanje koje je završilo 18. svibnja 2020.

[148] Stajalište Vijeća i zaključci, točka 20.

[149] Istodobno, Odbor pojašnjava da se tijela javne vlasti i dalje „mogu osloniti na druge relevantne instrumente kojima se osiguravaju odgovarajuće zaštitne mjere u skladu s člankom 46. Opće uredbe o zaštiti podataka". U pogledu odabira instrumenta, Odbor naglašava da bi trebalo „pažljivo procijeniti je li potrebno koristiti se pravno neobvezujućim administrativnim dogovorima kako bi se osigurale zaštitne mjere u javnom sektoru, s obzirom na svrhu obrade i prirodu podataka o kojima je riječ. Ako prava na zaštitu podataka i pravna zaštita pojedinaca iz EGP-a nisu predviđeni domaćim pravom treće zemlje, prednost bi trebalo dati sklapanju pravno obvezujućeg sporazuma. Bez obzira na vrstu donesenog instrumenta, postojeće mjere moraju biti učinkovite kako bi se osigurala odgovarajuća provedba, izvršenje i nadzor" (točka 67.).

[150] To može uključivati, na primjer, kombiniranje unutarnjih provjera (s obvezom obavješćivanja druge strane o svakom slučaju neusklađenosti s neovisnim nadzorom s pomoću vanjskih ili barem funkcionalno autonomnih mehanizama), kao i mogućnost da javno tijelo koje obavlja prijenos suspendira ili prekine prijenos.

[151] To može uključivati, primjerice, kvazisudske, obvezujuće mehanizme (npr. arbitražu) ili alternativne mehanizme rješavanja sporova, u kombinaciji s mogućnošću da tijelo javne vlasti koje obavlja prijenos suspendira ili prekine prijenos osobnih podataka ako stranke ne uspiju mirnim putem riješiti spor, uz obvezu javnog tijela koje prima podatke da vrati ili izbriše osobne podatke. Pri odabiru alternativnih mehanizama pravne zaštite u obvezujućim i provedivim instrumentima Odbor preporučuje da se prije sklapanja tih instrumenata zatraži savjet nadležnoga nadzornog tijela jer ne postoji mogućnost osiguravanja učinkovite sudske zaštite.

Naposljetku, Općom uredbom o zaštiti podataka pojašnjava se uporaba takozvanih „odstupanja”. To su posebni razlozi za prijenos podataka (npr. izričita privola[152], izvršenje ugovora ili važni razlozi od javnog interesa) koji su priznati zakonom i na koje se subjekti mogu osloniti u nedostatku drugih alata za prijenos i pod određenim uvjetima.

Kako bi se pojasnila uporaba takvih zakonskih razloga, Odbor je izdao posebne smjernice[153] i dao tumačenje članka 49. u nizu slučajeva s obzirom na posebne scenarije prijenosa[154]. Zbog njihove iznimne prirode Odbor smatra da se odstupanja moraju tumačiti usko, od slučaja do slučaja. Unatoč njihovu strogom tumačenju, ti razlozi obuhvaćaju brojne scenarije prijenosa. To posebno uključuje prijenose podataka tijela javne vlasti i privatnih subjekata koji su potrebni iz „važnih razloga od javnog interesa”, primjerice između tijela nadležnih za tržišno natjecanje, među financijskim, poreznim ili carinskim tijelima, među službama nadležnim za pitanja socijalne sigurnosti ili za javno zdravlje (na primjer u slučaju praćenja kontakata kod zaraznih bolesti ili kako bi se spriječio doping u sportu)[155]. Drugo je područje prekogranična suradnja u svrhu kaznenog progona, posebno u pogledu teških kaznenih djela[156].

Odbor je pojasnio da, iako relevantni javni interes mora biti priznat u pravu EU-a ili države članice, on se može uspostaviti i na temelju „međunarodnog sporazuma ili konvencije kojom se priznaje određeni cilj i predviđa međunarodna suradnja na postizanju tog cilja [čije postojanje] može biti pokazatelj u procjeni postojanja javnog interesa u skladu s člankom 49. stavkom 1. točkom (d) pod uvjetom da su EU ili države članice stranke tog sporazuma ili konvencije”[157].

Odluke stranih sudova ili tijela: nisu osnova za prijenose

---

[152] Riječ je o promjeni u odnosu na Direktivu 95/46 kojom se zahtijevala samo „nedvosmislena” suglasnost. Osim toga, primjenjuju se opći zahtjevi za privolu u skladu s člankom 4. stavkom 11. Opće uredbe o zaštiti podataka.

[153] Europski odbor za zaštitu podataka, Smjernice 2/2018 o odstupanjima iz članka 49. Uredbe 2016/679, 25.5.2018. (dostupno na: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_hr.pdf).

[154] To uključuje, na primjer, međunarodne prijenose zdravstvenih podataka u svrhu istraživanja u kontekstu izbijanja bolesti COVID-19. Vidjeti Smjernice Odbora 03/2020 o obradi podataka koji se odnose na zdravlje u svrhu znanstvenog istraživanja u kontekstu izbijanja bolesti COVID-19, 21.4.2020. (dostupno na: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_hr.pdf).

[155] Vidjeti uvodnu izjavu 112.

[156] Vidjeti podnesak Europske komisije u ime Europske unije kao nepristranog *amicus curiae* u predmetu *US v. Microsoft*, str. 15.: „U pravu Unije i pravu država članica općenito se prepoznaje važnost borbe protiv teških kaznenih djela, a time i važnost kaznenog progona te međunarodne suradnje u tom pogledu, kao cilja od općeg interesa. [...] člankom 83. UFEU-a utvrđeno je nekoliko područja kriminala koja su posebno teška i imaju prekograničnu dimenziju, kao što je nezakonita trgovina drogom.” (dostupno na: https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf).

[157] EDPB, Smjernice o odstupanjima (*supra* bilješka 153), str. 10. Odbor je dodatno pojasnio da, iako se prijenosi podataka na temelju odstupanja zbog javnog interesa ne smiju odvijati „u velikim razmjerima” ili „sustavno”, već „ih treba ograničiti na posebne situacije, a […] osigurati da prijenos ispunjava zahtjeve stroge provjere nužnosti”, ne postoji zahtjev da oni budu „povremeni”.

Osim što se utvrđuju razlozi za prijenos podataka, u poglavlju V. Opće uredbe o zaštiti podataka u članku 48. pojašnjava se i da nalozi sudova i odluke upravnih tijela izvan EU-a *sami po sebi* ne pružaju takve razloge, osim ako su priznati ili izvršivi na temelju međunarodnog sporazuma (npr. ugovora o uzajamnoj pravnoj pomoći). Svako otkrivanje podataka tijela kojem je upućen zahtjev u EU-u stranom sudu ili tijelu kao odgovor na takav nalog ili odluku predstavlja međunarodni prijenos podataka koji se mora temeljiti na jednom od navedenih instrumenata prijenosa.[158]

Opća uredba o zaštiti podataka ne predstavlja „statut o blokiranju" i njome će se, pod određenim uvjetima, dopustiti prijenos kao odgovor na odgovarajući zahtjev za provedbu zakona iz treće zemlje. Važno je da bi se upravo pravom EU-a trebalo utvrditi je li to slučaj i na temelju kojih se zaštitnih mjera mogu provesti takvi prijenosi.

Komisija je objasnila funkcioniranje članka 48. Opće uredbe o zaštiti podataka, uključujući moguće oslanjanje na odstupanje zbog javnog interesa, u kontekstu naloga za dostavljanje (naloga) stranog tijela kaznenog progona u predmetu *Microsoft* pred američkim Vrhovnim sudom[159]. Komisija je u svojem podnesku naglasila interes EU-a da osigura da se suradnja u području izvršavanja zakonodavstva odvija „unutar pravnog okvira kojim se izbjegavaju sukobi zakona i koji se temelji na [...] poštovanju temeljnih interesa obiju strana u pogledu privatnosti i provedbe zakona"[160]. Konkretno, „iz perspektive međunarodnog javnog prava, kada tijelo javne vlasti od trgovačkog društva s poslovnim nastanom u njegovoj nadležnosti zahtijeva dostavljanje elektroničkih podataka pohranjenih na poslužitelju u stranoj jurisdikciji, primjenjuju se načela teritorijalnosti i priznavanja u skladu s međunarodnim javnim pravom"[161].

To se odražava i u Komisijinu prijedlogu Uredbe o europskom nalogu za dostavljanje i europskom nalogu za čuvanje elektroničkih dokaza u kaznenim stvarima[162], koji

[158] To je jasno iz teksta članka 48. Opće uredbe o zaštiti podataka („ne dovodeći u pitanje druge razloge za prijenos u skladu s ovim poglavljem") i prateće uvodne izjave 115. („[p]rijenosi bi se smjeli dopustiti samo ako su ispunjeni uvjeti ove Uredbe za prijenos u treće zemlje. Ovo može, među ostalim, biti slučaj kada je otkrivanje nužno iz važnih razloga javnog interesa priznatog pravom Unije ili pravom države članice koje se primjenjuje na voditelja obrade."). Priznaje ga i EDPB, vidjeti Smjernice o odstupanjima (*supra* bilješka 153), str. 5. Kao i za sve postupke obrade, moraju se poštovati i druge zaštitne mjere iz Uredbe (npr. da se podaci prenose u određenu svrhu, da su relevantni, ograničeni na ono što je nužno za potrebe zahtjeva itd.).

[159] Podnesak *Microsoft* (*supra* bilješka 156). Kako je Komisija objasnila, Općom uredbom o zaštiti podataka ugovori o uzajamnoj pravnoj pomoći postaju „opcija kojoj se daje prednost" kad je riječ o prijenosima, jer se takvim ugovorima „predviđa prikupljanje dokaza uz privolu i utjelovljuje pažljivo dogovorena ravnoteža između interesa različitih država kojoj je cilj ublažiti moguće sukobe nadležnosti". Vidjeti i Smjernice o odstupanjima EDPB-a (*supra* bilješka 153), str. 5. („Ako postoji međunarodni sporazum, primjerice ugovor o uzajamnoj pravnoj pomoći, poduzeća iz EU-a načelno bi trebala odbiti izravni zahtjev i tijelo treće zemlje koje ga je podnijelo uputiti na postojeći ugovor o uzajamnoj pravnoj pomoći ili sporazum.").

[160] Podnesak *Microsoft* (*supra* bilješka 156), str. 4.

[161] Podnesak *Microsoft* (*supra* bilješka 156), str. 6.

[162] Europska komisija, Prijedlog uredbe Europskog parlamenta i Vijeća o europskom nalogu za dostavljanje i europskom nalogu za čuvanje elektroničkih dokaza u kaznenim stvarima, 17.4.2018. (COM(2018) 225 final). Vijeće je 7. prosinca 2018. usvojilo opći pristup o prijedlogu uredbe (dostupno na: https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-eevidence-council-agrees-its-position/#). Vidjeti i Mišljenje 7/19 Europskog nadzornika za zaštitu podataka o prijedlozima u vezi s europskim nalozima za dostavljanje i

sadržava posebnu „odredbu o priznavanju" kojom se omogućuje ulaganje prigovora na nalog za dostavljanje ako bi udovoljavanje tom nalogu bilo u suprotnosti sa zakonima treće zemlje kojima se zabranjuje otkrivanje, posebno na temelju činjenice da je to potrebno za zaštitu temeljnih prava dotičnih pojedinaca[163].

Osiguravanje priznavanja važno je s obzirom na to da kazneni progon, kad je riječ o kriminalu, a posebno kiberkriminalitetu, sve češće ima prekograničnu dimenziju te se stoga često javljaju pitanja nadležnosti i stvaraju mogući sukobi zakona[164]. Očekivano, najbolji način rješavanja tih pitanja jest primjena međunarodnih sporazuma kojima se predviđaju potrebna ograničenja i zaštitne mjere za prekogranični pristup osobnim podacima, među ostalim tako da tijelo koje podnosi zahtjev osigura visoku razinu zaštite podataka.

Komisija, djelujući u ime EU-a, trenutačno sudjeluje u multilateralnim pregovorima o Drugom dodatnom protokolu uz Konvenciju Vijeća Europe o kibernetičkom kriminalu („Budimpeštanska konvencija o kiberkriminalitetu"), čiji je cilj poboljšanje postojećih pravila za dobivanje prekograničnog pristupa elektroničkim dokazima u kaznenim istragama uz istodobno osiguravanje odgovarajućih mjera za zaštitu podataka u okviru Protokola[165]. Usto, započeli su bilateralni pregovori o sporazumu između EU-a i Sjedinjenih Američkih Država o prekograničnom pristupu elektroničkim dokazima za potrebe pravosudne suradnje u kaznenim stvarima[166]. Komisija računa na potporu Europskog parlamenta i Vijeća te na smjernice Odbora tijekom tih pregovora.

čuvanje elektroničkih dokaza u kaznenim stvarima (dostupno na: https://edps.europa.eu/data-protection/ourwork/publications/opinions/electronic-evidence-criminal-matters_en).

163 U obrazloženju, str. 21., jasno je navedeno da je, osim osiguravanja priznavanja u pogledu suverenih interesa trećih zemalja, zaštite dotičnog pojedinca i izbjegavanja sukoba zakona za pružatelje usluga, važna motivacija za odredbu o priznavanju i uzajamnost, tj. osiguravanje poštovanja pravila EU-a, uključujući zaštitu osobnih podataka (članak 48. Opće uredbe o zaštiti podataka). Vidjeti i Izjavu Radne skupine iz članka 29. od 29. studenoga 2017., „Zaštita podataka i aspekti privatnosti prekograničnog pristupa elektroničkim dokazima" (Izjava Radne skupine iz članka 29.) (dostupno na: file:///C:/Users/ralfs/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20171207_e-Evidence_Statement_FINALpdf%20 (1).pdf), str. 9.

164 Vidjeti i Izjavu Radne skupine iz članka 29. (*supra* bilješka 163), str. 6.

165 Vidjeti Preporuku za odluku Vijeća o odobrenju sudjelovanja u pregovorima o Drugom dodatnom protokolu uz Konvenciju Vijeća Europe o kibernetičkom kriminalu (CETS br. 185), 5.2.2019. (COM(2019) 71 final). Vidjeti i Mišljenje 3/2019 Europskog nadzornika za zaštitu podataka o sudjelovanju u pregovorima u pogledu Drugog dodatnog protokola uz Konvenciju o kibernetičkom kriminalu donesenu u Budimpešti, 2.4.2019. (dostupno na: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_budapest_convention_en.pdf); EDPB, Doprinos savjetovanju o nacrtu drugog dodatnog protokola uz Konvenciju Vijeća Europe o kibernetičkom kriminalu („Budimpeštanska konvencija o kiberkriminalitetu"), 13.11.2019. (dostupno na: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf).

166 Vidjeti Preporuku za odluku Vijeća o odobravanju otvaranja pregovora u cilju sklapanja sporazuma između Europske unije i Sjedinjenih Američkih Država o prekograničnom pristupu elektroničkim dokazima za potrebe pravosudne suradnje u kaznenim stvarima, 5.2.2019. (COM(2019) 70 final). Vidjeti i Mišljenje 2/2019 Europskog nadzornika za zaštitu podataka o pregovaračkom mandatu za sporazum između EU-a i SAD-a o prekograničnom pristupu elektroničkim dokazima (dostupno na: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e-evidence_en.pdf).

Općenito, važno je osigurati da, kada se trgovačka društva aktivna na europskom tržištu pozivaju, na temelju legitimnog zahtjeva, na dijeljenje podataka za potrebe kaznenog progona, to mogu činiti bez sukoba zakona i uz puno poštovanje temeljnih prava EU-a. Kako bi se poboljšali takvi prijenosi, Komisija sa svojim međunarodnim partnerima predano radi na razvoju odgovarajućih pravnih okvira kako bi se izbjegli sukobi zakona i poduprli učinkoviti oblici suradnje, posebno osiguravanjem potrebnih mjera za zaštitu podataka, čime bi se doprinijelo učinkovitijoj borbi protiv kriminala.

7.3 Međunarodna suradnja u području zaštite podataka

Poticanje konvergencije između različitih sustava privatnosti znači i uzajamno učenje kroz razmjenu znanja, iskustva i najboljih praksi. Takve su razmjene ključne za rješavanje novih izazova, koji su sve češće globalne prirode i opsega. Zbog toga je Komisija pojačala dijalog o zaštiti i protoku podataka sa širokim rasponom dionika i u okviru različitih foruma, i to na bilateralnoj, regionalnoj i multilateralnoj razini.

Bilateralna dimenzija

Nakon donošenja Opće uredbe o zaštiti podataka, sve je veći interes za iskustvo EU-a u oblikovanju, dogovaranju i provedbi modernih pravila o privatnosti. Dijalog sa zemljama koje prolaze slične procese odvija se na nekoliko načina.

Službe Komisije dostavile su podneske na brojna javna savjetovanja u pogledu zakonodavstva u području privatnosti koja su organizirale strane vlade, na primjer u SAD-u[167], Indiji[168], Maleziji i Etiopiji. U nekim trećim zemljama službe Komisije imale su čast svjedočiti pred nadležnim parlamentarnim tijelima, primjerice u Brazilu[169], Čileu[170], Ekvadoru i Tunisu[171].

---

[167] Vidjeti podnesak Glavne uprave za pravosuđe i zaštitu potrošača od 9. studenoga 2018. kao odgovor na zahtjev za primjedbe javnosti o predloženom pristupu privatnosti potrošača [predmet br. 180821780-8780-01] američke Nacionalne uprave za telekomunikacije i informacije (dostupno na: https://ec.europa.eu/info/sites/info/files/european_commission_submission_on_a_proposed_approach_to_consumer_privacy.pdf).

[168] Vidjeti podnesak Glavne uprave za pravosuđe i zaštitu potrošača od 19. studenoga 2018. o nacrtu indijskog zakona o zaštiti osobnih podataka iz 2018. Ministarstvu elektronike i informacijske tehnologije (dostupno na: https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en).

[169] Vidjeti plenarnu sjednicu brazilskog Senata od 17. travnja 2018. (https://www25.senado.leg.br/web/atividade/sessao-plenaria/-/pauta/23384), sjednicu Zajedničkog odbora o MP 869/2018 brazilskog Kongresa od 10. travnja 2019. (https://www12.senado.leg.br/ecidadania/visualizacaoaudiencia?id=15392) i sjednicu Posebnog odbora brazilskog Zastupničkog doma od 26. studenoga 2019. (https://www.camara.leg.br/noticias/616579-comissao-discutira-protecao-de-dados-no-ambito-das-constituicoes-de-outros-paises/).

[170] Vidjeti sjednice od 29. svibnja 2018. (https://senado.cl/appsenado/index.php?mo=comisiones&ac=asistencia_sesion&idcomision=186&idsesion=12513&idpunto=15909&sesion=29/05/2018&listado=1), 24. travnja 2019. (https://www.senado.cl/appsenado/index.php?mo=comisiones&ac=sesiones_celebradas&idcomision=186&tipo=3&legi=485&ano=2019&desde=0&hasta=0&idsesion=13603&idpunto=17283&listado=2), Odbor za ustavna, zakonodavna i pravosudna pitanja čileanskog Senata.

[171] Vidjeti sastanak Odbora za prava, slobode i vanjske odnose tuniske Skupštine narodnih predstavnika od 2. studenoga 2018. (https://www.facebook.com/1515094915436499/posts/2264094487203201/).

Nadalje, u kontekstu tekućih reformi zakona o zaštiti podataka održani su posebni sastanci s predstavnicima vlade ili parlamentarnim izaslanstvima iz mnogih regija svijeta (npr. Gruzije, Kenije, Tajvana, Tajlanda i Maroka). To je uključivalo organizaciju seminara i studijskih posjeta, primjerice s predstavnicima indonezijske vlade i izaslanstvom zaposlenika američkog Kongresa. Time su dobivene mogućnosti za pojašnjenje važnih pojmova Opće uredbe o zaštiti podataka, poboljšanje uzajamnog razumijevanja pitanja privatnosti i prikazivanje načina na koji konvergencija može osigurati visoku razinu zaštite prava pojedinaca, trgovine i suradnje. U nekim je slučajevima omogućeno i ukazivanje na određene pogrešne predodžbe o zaštiti podataka koje mogu dovesti do uvođenja protekcionističkih mjera kao što su zahtjevi za prisilnu lokalizaciju.

Od donošenja Opće uredbe o zaštiti podataka Komisija surađuje i s nekoliko međunarodnih organizacija, među ostalim zbog važnosti razmjene podataka s tim organizacijama u nizu područja politika. Konkretno, uspostavljen je poseban dijalog s Ujedinjenim narodima u cilju olakšavanja rasprave sa svim uključenim dionicima kako bi se osigurao nesmetan prijenos podataka i nastavila konvergencija među predmetnim sustavima zaštite podataka. U okviru tog dijaloga Komisija će blisko surađivati s Odborom kako bi dodatno pojasnila na koji način javni i privatni subjekti iz EU-a mogu ispuniti svoje obveze iz Opće uredbe o zaštiti podataka pri razmjeni podataka s međunarodnim organizacijama poput UN-a.

Komisija je spremna nastaviti dijeliti iskustva stečena u procesu reforme sa zainteresiranim zemljama i međunarodnim organizacijama, a i sama je na taj način učila od drugih sustava prilikom izrade vlastitog prijedloga novih pravila EU-a o zaštiti podataka. Ta vrsta dijaloga korisna je i za EU i njegove partnere jer omogućuje bolje razumijevanje okruženja privatnosti koje se brzo razvija i razmjenu mišljenja o novim pravnim i tehnološkim rješenjima.

U tom duhu Komisija uspostavlja „Akademiju za zaštitu podataka” kako bi se potaknula razmjena između europskih regulatornih tijela i regulatornih tijela trećih zemalja te tako poboljšala suradnja „na terenu”.

Osim toga, potrebno je razviti odgovarajuće pravne instrumente za bliže oblike suradnje i uzajamne pomoći, među ostalim omogućavanjem potrebne razmjene informacija u kontekstu istraga. Komisija će stoga iskoristiti ovlasti koje su joj u tom području dodijeljene člankom 50. Opće uredbe o zaštiti podataka i zatražiti odobrenje za otvaranje pregovora o sklapanju sporazuma o suradnji u području izvršavanja zakonodavstva s relevantnim trećim zemljama. U tom će kontekstu uzeti u obzir i stajališta Odbora o tome kojim bi zemljama trebalo dati prednost s obzirom na količinu prijenosa podataka, ulogu i ovlasti tijela koja provode zaštitu privatnosti u trećoj zemlji te potrebu za suradnjom u području izvršavanja zakonodavstva kako bi se riješili slučajevi od zajedničkog interesa.

Multilateralna dimenzija

Osim u bilateralnim razmjenama, Komisija aktivno sudjeluje i u nizu multilateralnih foruma za promicanje zajedničkih vrijednosti i izgradnju konvergencije na regionalnoj i globalnoj razini.

Sve univerzalnije članstvo Konvencije Vijeća Europe br. 108, jedinoga pravno obvezujućeg multilateralnog instrumenta u području zaštite osobnih podataka, jasan je pokazatelj tog trenda prema (uzlaznoj) konvergenciji[172]. Konvenciju, koja je otvorena i za države koje nisu članice Vijeća Europe, već je ratificiralo 55 zemalja, uključujući niz afričkih i latinoameričkih država[173]. Komisija je znatno doprinijela uspješnom ishodu pregovora o modernizaciji Konvencije[174] i osigurala da u njoj odražavaju ista načela kao ona sadržana u pravilima EU-a o zaštiti podataka. Većina država članica EU-a do sada je potpisala Protokol o izmjeni, iako se još uvijek čekaju potpisi Danske, Malte i Rumunjske. Do sada su samo četiri države članice (Bugarska, Hrvatska, Litva i Poljska) ratificirale Protokol o izmjeni. Komisija poziva preostale tri države članice da potpišu moderniziranu Konvenciju, a sve države članice da je brzo ratificiraju kako bi se omogućilo njezino stupanje na snagu u bliskoj budućnosti[175]. Osim toga, nastavit će proaktivno poticati pristupanje trećih zemalja.

O protoku i zaštiti podataka nedavno se raspravljalo i u okviru skupina G20 i G7. Globalni su čelnici 2019. prvi put podržali ideju da se zaštitom podataka doprinosi povjerenju u digitalno gospodarstvo i olakšava protok podataka. Uz aktivnu potporu Komisije[176], čelnici su podržali koncept „slobodnog protoka podataka uz puno povjerenje" (DFFT), koji je izvorno predložio Japan u Izjavi skupine G20 iz Osake[177] i na sastanku na vrhu skupine G7 u Biarritzu[178]. Taj se pristup odražava i u Komunikaciji Komisije iz 2020. pod nazivom „Europska strategija za podatke"[179], u

---

[172] Važno je napomenuti da modernizirana Konvencija nije samo ugovor kojim se utvrđuju stroge mjere za zaštitu podataka, već se njome stvara i mreža nadzornih tijela s alatima za suradnju u provedbi te, uz Odbor Konvencije, forum za rasprave, razmjenu najboljih praksi i razvoj međunarodnih standarda.

[173] Vidjeti cjeloviti popis članova: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures. Zemlje Afrike uključuju Cabo Verde, Mauricijus, Maroko, Senegal i Tunis, a zemlje Latinske Amerike Argentinu, Meksiko i Urugvaj. Burkina Faso pozvana je da se pridruži Konvenciji.

[174] Vidjeti tekst modernizirane Konvencije: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

[175] U skladu sa svojom Odlukom o Protokolu o izmjeni od 18. svibnja 2018., Odbor ministara „pozvao je države članice i druge stranke Konvencije da bez odgode poduzmu potrebne mjere kako bi se omogućilo stupanje na snagu Protokola u roku od tri godine od njegova otvaranja za potpisivanje i da pokrenu odmah, ali u svakom slučaju najkasnije godinu dana nakon datuma otvaranja Protokola za potpisivanje, postupak ratifikacije u skladu s njihovim nacionalnim pravom..." Također je „naložio svojim zamjenicima da svake dvije godine, a prvi put godinu dana nakon datuma otvaranja Protokola za potpisivanje, ispitaju ukupan napredak prema ratifikaciji na temelju informacija koje će svaka država članica i druge stranke Konvencije dostaviti glavnom tajniku najkasnije mjesec dana prije takvog ispitivanja". Vidjeti: https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016808a3c9f.

[176] Na margini sastanka na vrhu EU-a i Japana održanog u travnju 2019. predsjednik Juncker izrazio je potporu japanskoj inicijativi o „slobodnom protoku podataka uz puno povjerenje" i pokretanju inicijative „Osaka Track" te je obvezao Komisiju da „preuzme aktivnu ulogu u objema inicijativama".

[177] Vidjeti tekst Izjave čelnika i čelnica skupine G20 iz Osake: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf

[178] Vidjeti tekst Strategije skupine G7 iz Biarritza za otvorenu, slobodnu i sigurnu digitalnu transformaciju: https://www.elysee.fr/admin/upload/default/0001/05/62a9221e66987d4e0d6ffcb058f3d2c649fc6d9d.pdf

Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija, Europska strategija za podatke, 19.2.2020. (COM(2020) 66 final)

kojoj se ističe njezina namjera da nastavi promicati razmjenu podataka s pouzdanim partnerima te da se pritom bori protiv zlouporaba kao što je nerazmjeran pristup (stranih) javnih tijela podacima.

Pritom će se EU moći osloniti i na niz alata u različitim područjima politika kojima se sve više uzima u obzir učinak na privatnost: primjerice, prvi okvir EU-a za provjeru stranih ulaganja, koji će se u potpunosti početi primjenjivati u listopadu 2020., daje EU-u i njegovim državama članicama mogućnost provjere investicijskih transakcija koje utječu na „pristup osjetljivim informacijama, uključujući osobne podatke, ili mogućnost kontroliranja takvih informacija" ako utječu na sigurnost ili javni poredak[180].

Komisija surađuje sa zemljama istomišljenicama u nekoliko drugih multilateralnih foruma kako bi promicala svoje vrijednosti i standarde. Važan je forum nedavno osnovana Radna skupina OECD-a za upravljanje podacima i privatnost (DGP), koja provodi niz važnih inicijativa povezanih sa zaštitom, razmjenom i prijenosom podataka. To uključuje evaluaciju Smjernica OECD-a o privatnosti iz 2013. Nadalje, Komisija je dala aktivan doprinos Preporuci Vijeća OECD-a o umjetnoj inteligenciji[181] i osigurala da se u konačnom tekstu odražava antropocentrični pristup EU-a, što znači da primjena umjetne inteligencije mora biti u skladu s temeljnim pravima, a posebno sa zaštitom podataka. Važno je napomenuti da se Preporukom o umjetnoj inteligenciji, koja je naknadno uključena u načela umjetne inteligencije skupine G20 priložene Izjavi čelnika i čelnica skupine G20 iz Osake[182], utvrđuju načela transparentnosti i objašnjivosti kako bi se „osobama na koje sustav umjetne inteligencije negativno utječe omogućilo osporavanje njegova ishoda na temelju jednostavnih i lako razumljivih informacija o čimbenicima i logici koja je poslužila kao osnova za predviđanje, preporuku ili odluku", čime se vjerno odražavaju načela Opće uredbe o zaštiti podataka u pogledu donošenja automatiziranih odluka[183].

Komisija također pojačava dijalog s regionalnim organizacijama i mrežama koje sve više imaju središnju ulogu u oblikovanju zajedničkih standarda zaštite podataka[184], promicanju razmjene najboljih praksi i poticanju suradnje među provedbenim tijelima. To se posebno odnosi na Udruženje država jugoistočne Azije (ASEAN), među ostalim u kontekstu njegova trenutačnog rada na instrumentima za prijenos podataka, Afričku uniju, Azijsko-pacifički forum za zaštitu privatnosti (APPA) i Iberoameričku mrežu za zaštitu podataka, što je sve pokrenulo važne inicijative u tom području i osiguralo forume za plodonosan dijalog između regulatornih tijela iz područja privatnosti i drugih dionika.

(https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf), str. 23.–24.

[180] Članak 4. stavak 1. točka (d) Uredbe (EU) 2019/452 Europskog parlamenta i Vijeća od 19. ožujka 2019. o uspostavi okvira za provjeru izravnih stranih ulaganja u Uniji (SL L 79I, 21.3.2019.).

[181] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[182] Ministarska izjava skupine G20 o trgovini i digitalnom gospodarstvu: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

[183] Vidjeti članak 13. stavak 2. točku (f), članak 14. stavak 2. točku (g) te članak 22. Opće uredbe o zaštiti podataka.

[184] Vidjeti primjerice Konvenciju o kibernetičkoj sigurnosti i zaštiti osobnih podataka („Konvencija iz Malaba") Afričke unije i Standarde za zaštitu podataka za iberoameričke države, koje je razvila Iberoamerička mreža za zaštitu podataka.

Afrika je primjer komplementarnosti između nacionalne, regionalne i globalne dimenzije privatnosti. Zahvaljujući digitalnim tehnologijama, afrički se kontinent brzo i iz korijena mijenja. To bi moglo ubrzati postizanje ciljeva održivog razvoja poticanjem gospodarskog rasta, ublažavanjem siromaštva i poboljšanjem života ljudi. Uspostava modernog okvira za zaštitu podataka kojim se privlače ulaganja i potiče razvoj konkurentnog poslovanja te istodobno doprinosi poštovanju ljudskih prava, demokracije i vladavine prava ključan je element te preobrazbe. Usklađivanjem pravila o zaštiti podataka diljem Afrike omogućila bi se integracija digitalnog tržišta, dok bi se usklađivanjem s globalnim standardima olakšala razmjena podataka s EU-om. Te su različite dimenzije zaštite podataka međusobno povezane i uzajamno se nadopunjuju.

Danas postoji sve veći interes za zaštitu podataka u mnogim afričkim zemljama, a broj afričkih zemalja koje su donijele ili su u postupku donošenja modernih pravila o zaštiti podataka i ratificirale su Konvenciju br. 108[185] ili Konvenciju iz Malaba[186] nastavlja rasti[187]. No regulatorni je okvir na afričkom kontinentu i dalje vrlo neujednačen i rascjepkan. Mnoge zemlje još uvijek nude tek malen broj mjera za zaštitu podataka ili ih uopće ne nude. Mjere kojima se ograničava protok podataka i dalje su široko rasprostranjene i ometaju razvoj regionalnog digitalnog gospodarstva.

Kako bi se iskoristile prednosti usklađenih pravila o zaštiti podataka za obje strane, Komisija će surađivati sa svojim afričkim partnerima bilateralno i u regionalnim forumima[188]. To se nadovezuje na rad Radne skupine EU-a i Afričke unije (AU) za digitalno gospodarstvo u kontekstu Partnerstva za digitalno gospodarstvo Nove Afrike i Europe[189]. U svrhu promicanja takvih ciljeva područje primjene instrumenta za partnerstvo Komisije „Poboljšana zaštita podataka i protok podataka" prošireno je i na Afriku. Projekt će se pokrenuti radi potpore afričkim zemljama koje namjeravaju razviti moderne okvire za zaštitu podataka ili žele ojačati kapacitete svojih regulatornih tijela osposobljavanjem, dijeljenjem znanja i razmjenom najboljih praksi.

---

[185] Konvencija Vijeća Europe za zaštitu osoba glede automatizirane obrade osobnih podataka: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=DW5jevqD

[186] Konvencija Afričke unije o kibersigurnosti i zaštiti osobnih podataka: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection. Osim toga, nekoliko regionalnih gospodarskih zajednica razvilo je pravila o zaštiti podataka, primjerice Gospodarska zajednica zapadnoafričkih država (ECOWAS) i Južnoafrička razvojna zajednica (SADC). Vidjeti: http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf i http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data%20protection.pdf.

[188] Među ostalim, kroz Političku i regulatornu inicijativu za digitalnu Afriku (PRIDA), informacije vidjeti na: https://www.africa-eu-partnership.org/en/projects/policy-and-regulation-initiative-digital-africa-prida.

[189] Vidjeti Zajedničku komunikaciju Europske komisije i Visokog predstavnika za vanjske poslove i sigurnosnu politiku „Put prema sveobuhvatnoj strategiji s Afrikom" (dostupno na: https://ec.europa.eu/international-partnerships/system/files/communication-eu-africa-strategy-join-2020-4-final_en.pdf); Radna skupina za digitalno gospodarstvo, Novo partnerstvo Afrike i Europe za digitalno gospodarstvo: Prema bržem ostvarenju ciljeva održivog razvoja (dostupno na: https://www.africa-eu-partnership.org/sites/default/files/documents/finaldetfreportpdf.pdf).

Naposljetku, Komisija promiče konvergenciju standarda zaštite podataka na međunarodnoj razini radi olakšavanja protoka podataka, a time i trgovine, ali je i odlučna u borbi protiv digitalnog protekcionizma, kako je nedavno istaknuto u podatkovnoj strategiji[190]. U tu je svrhu razvila posebne odredbe o protoku podataka i zaštiti podataka u trgovinskim sporazumima koje sustavno navodi u bilateralnim – posljednji put s Australijom, Novim Zelandom i Ujedinjenom Kraljevinom – i multilateralnim pregovorima, primjerice aktualnim pregovorima WTO-a o e-trgovini. Tim se horizontalnim odredbama isključuju neopravdana ograničenja, kao što su zahtjevi za prisilnu lokalizaciju podataka, a čuva se regulatorna autonomija stranaka u pogledu poštovanja temeljnog prava na zaštitu podataka.

Iako se dijalozi o zaštiti podataka i trgovinski pregovori moraju odvijati zasebno, mogu se međusobno nadopunjavati. Zapravo je konvergencija, utemeljena na visokim standardima i poduprta djelotvornom provedbom, najsnažniji temelj za razmjenu osobnih podataka, što naši međunarodni partneri sve više prepoznaju. S obzirom na to da trgovačka društva sve više posluju prekogranično i daju prednost sličnim pravilima u svim svojim poslovnim operacijama diljem svijeta, takva konvergencija pomaže u stvaranju okruženja pogodnog za izravna ulaganja, olakšavanju trgovine i poboljšanju povjerenja među trgovinskim partnerima. Stoga bi trebalo dodatno istražiti sinergije između instrumenata za zaštitu trgovine i podataka kako bi se osigurao slobodan i siguran međunarodni protok podataka, koji je neophodan za poslovanje, konkurentnost i rast europskih poduzeća, uključujući MSP-ove, u okolnostima sve veće digitalizacije gospodarstva.

[190] https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf, str. 23.

Prilog I. – Odredbe o fakultativnim specifikacijama prema nacionalnom zakonodavstvu

Predmet	Područje primjene	Članci Opće uredbe o zaštiti podataka
Specifikacije za pravne obveze i javne zadaće	Prilagodba primjene odredbi s obzirom na obradu radi poštovanja pravne obveze ili javne zadaće, među ostalim za posebne situacije obrade iz poglavlja IX.	Članak 6. stavci 2. i 3.
Dobna granica za privolu u odnosu na usluge informacijskog društva	Utvrđivanje najniže dobi između 13 i 16 godina	Članak 8. stavak 1.
Obrada posebnih kategorija podataka	Zadržavanje ili uvođenje dodatnih uvjeta, uključujući ograničenja s obzirom na obradu genetskih podataka, biometrijskih podataka ili podataka koji se odnose na zdravlje	Članak 9. stavak 4.
Odstupanje od zahtjeva u pogledu informacija	Dobivanje ili otkrivanje podataka koje je izrijekom propisano zakonom ili za čuvanje profesionalne tajne koje je uređeno zakonom	Članak 14. stavak 5. točke (c) i (d)
Automatizirano pojedinačno donošenje odluka	Odobrenje za automatizirano donošenje odluka koje odstupa od opće zabrane	Članak 22. stavak 2. točka (b)
Ograničenja prava ispitanika	Ograničenja iz članaka od 12. do 22., članka 34. i odgovarajućih odredbi članka 5., kada je to nužno i razmjerno kako bi se zaštitili iscrpno navedeni važni ciljevi	Članak 23. stavak 1.
Zahtjev za savjetovanje i odobrenje	Obveza voditeljâ obrade da se savjetuju s tijelom za zaštitu podataka ili od njega dobiju odobrenje za obradu u vezi sa zadaćom od javnog interesa	Članak 36. stavak 5.
Imenovanje službenika za zaštitu podataka u dodatnim slučajevima	Imenovanje službenika za zaštitu podataka u slučajevima koji nisu navedeni u članku 37. stavku 1.	Članak 37. stavak 4.
Ograničenja prijenosa	Ograničenje prijenosa određenih kategorija osobnih podataka	Članak 49. stavak 5.
Samostalne pritužbe i sudski postupci organizacija	Davanje ovlasti organizacijama za zaštitu privatnosti za podnošenje pritužbi i pokretanje sudskih postupaka neovisno o mandatu ispitanikâ	Članak 80. stavak 2.

Pristup službenim dokumentima	Usklađivanje javnog pristupa službenim dokumentima s pravom na zaštitu osobnih podataka	Članak 86.
Obrada nacionalnog identifikacijskog broja	Posebni uvjeti za obradu nacionalnog identifikacijskog broja	Članak 87.
Obrada u kontekstu zaposlenja	Preciznija pravila za obradu osobnih podataka zaposlenika	Članak 88.
Odstupanja vezano za obradu u svrhe arhiviranja u javnom interesu, u svrhe istraživanja ili statističke svrhe	Odstupanja od određenih prava ispitanika ako je vjerojatno da će se takvim pravima onemogućiti ili ozbiljno ugroziti postizanje posebnih svrha	Članak 89. stavci 2. i 3.
Usklađivanje zaštite podataka s obvezama tajnosti	Posebna pravila o istražnim ovlastima tijela za zaštitu podataka u odnosu na voditelje obrade ili izvršitelje obrade koji podliježu obvezi čuvanja profesionalne tajne	Članak 90.

PRILOG II. – Pregled resursa tijela za zaštitu podataka

U tablici u nastavku prikazan je pregled resursa (osoblja i proračunskih sredstava) tijela za zaštitu podataka po državama članicama EU-a/EGP-a[191].

Prilikom uspoređivanja podataka među državama članicama važno je imati na umu da se nadležnim tijelima mogu dodijeliti zadaće koje nadilaze one iz Opće uredbe o zaštiti podataka te da se te zadaće mogu razlikovati među državama članicama. Broj članova osoblja koje zapošljavaju nadležna tijela na milijun stanovnika i iznos proračunskih sredstava nadležnih tijela u odnosu na milijun eura BDP-a navedeni su samo kao dodatni elementi usporedbe među državama članicama slične veličine i ne bi ih trebalo razmatrati izvan konteksta. Pri procjeni resursa određenog tijela trebalo bi zajedno uzeti u obzir apsolutne brojke, omjere i razvoj tijekom proteklih godina.

	OSOBLJE (ekvivalenti punoga radnog vremena)					PRORAČUNSKA SREDSTVA (EUR)				
Države članice EU-a/EGP-a	**2019.**	**Prognoza za 2020.**	**% rasta u razdoblju 2016.–2019.**	**% rasta 2016.–2020. (prognoza)**	**Osoblje na milijun stanovnika (2019.)**	**2019.**	**Prognoza za 2020.**	**% rasta u razdoblju 2016.–2019.**	**% rasta 2016.–2020. (prognoza)**	**Proračunska sredstva na milijun EUR BDP-a (2019.)**
Austrija	34	34	48 %	48 %	3,8	2 282 000	2 282 000	29 %	29 %	5,7
Belgija	59	65	9 %	20 %	5,2	8 197 400	8 962 200	1 %	10 %	17,3
Bugarska	60	60	–14 %	–14 %	8,6	1 446 956	1 446 956	24 %	24 %	23,8
Hrvatska	39	60	39 %	114 %	9,6	1 157 300	1 405 000	57 %	91 %	21,5
Cipar	24	22	n. p.	n. p.	27,4	503 855	n. p.	114 %	n. p.	23,0
Češka	101	109	0 %	8 %	9,5	6 541 288	6 720 533	10 %	13 %	29,7
Danska	66	63	106 %	97 %	11,4	5 610 128	5 623 114	101 %	101 %	18,0
Estonija	16	18	–11 %	0 %	12,1	750 331	750 331	7 %	7 %	26,8
Finska	45	55	114 %	162 %	8,2	3 500 000	4 500 000	94 %	150 %	14,6
Francuska	215	225	9 %	14 %	3,2	18 506 734	20 143 889	–2 %	7 %	7,7
Njemačka	888	1002	52 %	72 %	10,7	76 599 800	85 837 500	48 %	66 %	22,3
Grčka	33	46	–15 %	18 %	3,1	2 849 000	3 101 000	38 %	50 %	15,2
Mađarska	104	117	42 %	60 %	10,6	3 505 152	4 437 576	102 %	155 %	24,4
Island	17	17	143 %	143 %	47,6	2 272 490	2 294 104	167 %	170 %	105,2
Irska	140	176	169 %	238 %	28,5	15 200 000	16 900 000	223 %	260 %	43,8
Italija	170	170	40 %	40 %	2,8	29 127 273	30 127 273	46 %	51 %	16,3
Latvija	19	31	–10 %	48 %	9,9	640 998	1 218 978	4 %	98 %	21,0
Litva	46	52	–8 %	4 %	16,5	1 482 000	1 581 000	40 %	49 %	30,6
Luksemburg	43	48	126 %	153 %	70,0	5 442 416	6 691 563	165 %	226 %	85,7
Malta	13	15	30 %	50 %	26,3	480 000	550 000	41 %	62 %	36,3
Nizozemska	179	188	145 %	158 %	10,4	18 600 000	18 600 000	130 %	130 %	22,9
Norveška	49	58	2 %	21 %	9,2	5 708 950	6 580 660	27 %	46 %	15,9
Poljska	238	260	54 %	68 %	6,3	7 506 345	9 413 381	66 %	108 %	14,2
Portugal	25	27	–4 %	4 %	2,4	2 152 000	2 385 000	67 %	86 %	10,1
Rumunjska	39	47	–3 %	18 %	2,0	1 103 388	1 304 813	3 %	22 %	4,9
Slovačka	49	51	20 %	24 %	9,0	1 731 419	1 859 514	47 %	58 %	18,4
Slovenija	47	49	42 %	48 %	22,6	2 242 236	2 266 485	68 %	70 %	46,7
Španjolska	170	220	13 %	47 %	3,6	15 187 680	16 500 000	8 %	17 %	12,2
Švedska	87	87	81 %	81 %	8,5	8 800 000	10 300 000	96 %	129 %	18,5
UKUPNO	**2 966**	**3 372**	**42 %**	**62 %**	**6,6**	**249 127 139**	**273 782 870**	**49 %**	**64 %**	**17,4**

Izvor neobrađenih podataka: doprinos Odbora. Izračuni Komisije.

[191] Osim Lihtenštajna.