EUROPSKA
KOMISIJA

Bruxelles, 24.6.2020.
COM(2020) 264 final

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU

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

{SWD(2020) 115 final}

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU

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

1 PRAVILA O ZAŠTITI PODATAKA KAO JEDAN OD STUPOVA JAČANJA POLOŽAJA GRAĐANA I PRISTUPA EU-A DIGITALNOJ TRANZICIJI

Ovo je prvo izvješće o evaluaciji i preispitivanju Opće uredbe o zaštiti podataka[1], posebno o primjeni i funkcioniranju pravila o prijenosu osobnih podataka trećim zemljama i međunarodnim organizacijama te pravila o suradnji i konzistentnosti, u skladu s člankom 97. Opće uredbe o zaštiti podataka.

Opća uredba o zaštiti podataka, koja se primjenjuje od 25. svibnja 2018., u središtu je okvira EU-a[2] kojim se jamči temeljno pravo na zaštitu podataka, kako je utvrđeno u Povelji Europske unije o temeljnim pravima (članak 8.) i u Ugovorima (članak 16. Ugovora o funkcioniranju Europske unije, „UFEU"). Općom uredbom o zaštiti podataka ojačane su mjere za zaštitu podataka, pojedincima se pružaju dodatna i veća prava te se osigurava veća transparentnost i odgovornije ponašanje svih koji obrađuju osobne podatke obuhvaćene njezinim područjem primjene. Njome se neovisnim tijelima za zaštitu podataka dodjeljuju snažnije i usklađene provedbene ovlasti te se uspostavlja novi sustav upravljanja. Njome se stvaraju i jednaki uvjeti za sva poduzeća koja posluju na tržištu EU-a, bez obzira na to gdje imaju poslovni nastan, te se osigurava slobodan protok podataka unutar EU-a, čime se jača unutarnje tržište.

Opća uredba o zaštiti podataka važna je sastavnica antropocentričnog pristupa tehnologiji i putokaz za korištenje tehnologije u zelenoj i digitalnoj tranziciji, koja je važan element oblikovanja politika EU-a. To je nedavno istaknuto u Bijeloj knjizi o umjetnoj inteligenciji[3] i Komunikaciji o europskoj strategiji za podatke[4] (dalje u tekstu „podatkovna strategija") iz veljače 2020.

U gospodarstvu koje se sve više temelji na obradi podataka, uključujući osobne podatke, Opća uredba o zaštiti podataka ključan je instrument kojim se osigurava da pojedinci imaju bolji nadzor nad svojim osobnim podacima te da se ti podaci obrađuju u opravdane svrhe na zakonit, pravedan i transparentan način. Usto, Općom uredbom o zaštiti podataka pridonosi se poticanju inovacija dostojnih povjerenja, posebno zbog njezina pristupa koji se temelji na riziku i načela kao što su integrirana i zadana

---

[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] Nakon što je uključena u Sporazum o Europskom gospodarskom prostoru (EGP), Uredba se primjenjuje i na Norvešku, Island i Lihtenštajn.

[3] https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

[4] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_hr

privatnost. Komisija je predložila dopunu zakonodavnog okvira o zaštiti podataka i privatnosti[5] Uredbom o e-privatnosti[6], koja bi trebala zamijeniti postojeću Direktivu o e-privatnosti[7]. Suzakonodavci trenutačno razmatraju taj prijedlog te je vrlo važno osigurati njegovo brzo donošenje.

U okviru ključnih prioriteta Komisije „Europa spremna za digitalno doba”[8] i „europski zeleni plan”[9] mogu se razvijati nove inicijative da bi se građane potaknulo da preuzmu aktivniju ulogu u digitalnoj tranziciji i korištenju digitalnih alata kako bi se ostvario prelazak na klimatski neutralno društvo i održiviji razvoj. Općom uredbom o zaštiti podataka utvrđuje se okvir za te inicijative i osigurava se da su osmišljene tako da učinkovito jačaju položaj pojedinaca.

Podatkovnom strategijom[10] poziva se na stvaranje „jedinstvenoga europskog podatkovnog prostora”, istinskoga jedinstvenog tržišta za podatke, te deset sektorskih zajedničkih europskih podatkovnih prostora važnih za zelenu i digitalnu tranziciju[11]. Za ostvarenje tih prioriteta neophodni su jasan i provediv okvir za sigurnu razmjenu podataka i njihova veća dostupnost. U podatkovnoj strategiji Komisija je najavila i svoju namjeru da u budućem zakonodavstvu istraži kako omogućiti upotrebu podataka pohranjenih u javnim bazama podataka u svrhe znanstvenog istraživanja na način koji je u skladu s Općom uredbom o zaštiti podataka. Podatkovne prostore treba podupirati europska federacija oblaka koja pruža usluge obrade podataka i infrastrukture u oblaku u skladu s Općom uredbom o zaštiti podataka. Općom uredbom o zaštiti podataka osigurava se visoka razina zaštite osobnih podataka i središnja uloga pojedinaca u svim tim podatkovnim prostorima te se istodobno osigurava fleksibilnost potrebna za prihvaćanje različitih pristupa.

Potreba za osiguravanjem povjerenja i zahtjevi za zaštitom osobnih podataka zasigurno se ne javljaju samo u EU-u. Pojedinci diljem svijeta sve više cijene privatnost i sigurnost svojih podataka. Kao što je vidljivo iz nedavnoga globalnog istraživanja[12], smatraju da je to važan čimbenik koji utječe na njihove odluke o kupnji

---

[5] Taj zakonodavni okvir uključuje i Direktivu o zaštiti podataka za potrebe kaznenog progona (Direktiva 2016/680) i Uredbu o zaštiti podataka za institucije i tijela EU-a (Uredba 2018/1725).

[6] Prijedlog uredbe Europskog parlamenta i Vijeća o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ (Uredba o privatnosti i elektroničkim komunikacijama) – COM(2017) 10 final – 2017/0003(COD).

[7] 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.

[8] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_hr

[9] Komunikacija Komisije Europskom parlamentu, Europskom vijeću, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija: Europski zeleni plan – COM(2019) 640 final.

[10] Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija: Europska strategija za podatke – COM(2020) 66 final.

[11] Riječ je o sljedećih deset sektorskih zajedničkih europskih podatkovnih prostora: zdravstvo, industrijska proizvodnja, energetika, mobilnost, poljoprivreda, financijski podaci, javna uprava, zajednički europski podatkovni prostor za vještine u radu s podacima, podatkovni prostor za europski zeleni plan i europski oblak za otvorenu znanost.

[12] Vidjeti npr. Ciscovu studiju o privatnosti potrošača iz 2019. (https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf). Prema toj studiji, u kojoj je ispitano 2 600 potrošača diljem svijeta, znatan broj njih već je poduzeo mjere za zaštitu svoje privatnosti, primjerice promjenom poduzeća ili pružatelja usluga zbog njihovih politika postupanja s podacima ili prakse razmjene podataka.

i ponašanje na internetu. Sve veći broj poduzeća odgovorio je na tu potrebu za privatnošću, konkretno tako da su neka prava i zaštitne mjera predviđene Općom uredbom o zaštiti podataka dobrovoljno proširili na svoje kupce iz zemalja izvan EU-a. Mnoga poduzeća ističu i poštovanje osobnih podataka kao konkurentsku prednost i ono što privlači kupce na globalnom tržištu te nude inovativne proizvode i usluge s novim rješenjima za privatnost ili sigurnost podataka. Nadalje, povećana sposobnost dionika iz privatnog i javnog sektora da prikupljaju i obrađuju podatke u velikim količinama otvara važna i složena pitanja kojima se privatnost sve više stavlja u središte javne rasprave u različitim dijelovima svijeta.

Donošenje Opće uredbe o zaštiti podataka potaknulo je druge zemlje u mnogim regijama svijeta da razmotre žele li slijediti taj primjer. Riječ je o doista globalnom trendu, koji je primjetan od Čilea do Južne Koreje, od Brazila do Japana, od Kenije do Indije te od Kalifornije do Indonezije. Vodeći položaj EU-a u području zaštite podataka pokazuje da EU može postavljati globalne standarde za regulaciju digitalnog gospodarstva, a pozdravili su ga utjecajni pojedinci iz međunarodne zajednice, kao što je glavni tajnik UN-a António Guterres, koji je napomenuo da je Opća uredba o zaštiti podataka „primjer [...] koji je nadahnuo slične mjere drugdje" te je „potaknuo EU i njegove države članice da nastave voditi oblikovanje digitalnog doba i biti predvodnik u tehnološkim inovacijama i regulaciji"[13].

Trenutačna kriza uzrokovana pandemijom bolesti COVID-19 zorno pokazuje globalizaciju rasprave o privatnosti, i tijekom krize i u vrijeme kada svijet pokušava izaći iz nje. U EU-u je više država članica poduzelo hitne mjere u cilju zaštite javnog zdravlja. Općom uredbom o zaštiti podataka jasno se utvrđuje da se svakim ograničenjem mora poštovati bit temeljnih prava i sloboda te da ono mora biti nužna i proporcionalna mjera u demokratskom društvu poduzeta radi zaštite javnog interesa, kao što je javno zdravlje. Budući da se mjere za suzbijanje pandemije postupno ukidaju, donositelji odluka moraju se pozabaviti očekivanjima građana da im se ponude digitalna rješenja koja su pouzdana i kojima se poštuju prava na privatnost i zaštitu osobnih podataka.

U mnogim se zemljama ugrađene mjere zaštite privatnosti, kao što su dobrovoljna prijava korisnika, smanjenje količine podataka i njihova sigurnost te isključivanje geolociranja, smatraju neophodnima za osiguravanje pouzdanosti i društvene prihvaćenosti rješenja koja su temeljena na podacima i usmjerena na praćenje i ograničavanje širenja virusa, prilagodbu protumjera javne politike, pomoć pacijentima ili provedbu izlaznih strategija. Zakonodavni okvir o zaštiti podataka i privatnosti u EU-u[14] pokazao se dovoljno fleksibilnim alatom za razvoj praktičnih rješenja (npr. aplikacijâ za praćenje), a istodobno osigurava visoku razinu zaštite osobnih podataka. U tom je kontekstu Komisija 16. travnja 2020. objavila smjernice za zaštitu podataka u aplikacijama kojima se podupire suzbijanje pandemije[15].

---

[13] Obraćanje glavnog tajnika UN-a talijanskom Senatu 18. prosinca 2019. (dostupno na: https://www.un.org/press/en/2019/sgsm19916.doc.htm).

[14] Osim Opće uredbe o zaštiti podataka, taj okvir obuhvaća Direktivu o e-privatnosti (Direktiva 2002/58/EZ) kojom se, među ostalim, utvrđuju pravila o pristupu informacijama na terminalnoj opremi korisnika i njihovoj pohrani.

[15] Komunikacija Komisije: Smjernice za zaštitu podataka u aplikacijama kojima se podupire suzbijanje pandemije bolesti COVID-19 2020/C 124 I/01 – C/2020/2523 – SL C 124I, 17.4.2020., str. 1.–9. Dana 16. travnja 2020. države članice EU-a uz potporu Komisije razvile su paket instrumenata EU-a za

Zaštita osobnih podataka važna je i za sprečavanje manipuliranja odlukama građana, posebno mikrociljanja glasača na temelju nezakonite obrade osobnih podataka, te za izbjegavanje uplitanja u demokratske procese i očuvanje otvorene rasprave, pravednosti i transparentnosti koji su ključni za demokraciju. Zbog toga je u rujnu 2018. Komisija objavila svoje smjernice o primjeni prava Unije o zaštiti podataka u kontekstu izbora[16].

Pri evaluaciji i preispitivanju Komisija je uzela u obzir doprinose Vijeća[17], Europskog parlamenta[18], Europskog odbora za zaštitu podataka (dalje u tekstu „Odbor")[19] i pojedinih tijela za zaštitu podataka[20], stručne skupine s više dionika[21] i drugih dionika, među ostalim putem povratnih informacija o planu[22].

Općenito gledano, dvije godine nakon početka njezine primjene Opća uredba o zaštiti podataka uspješno je ispunila svoje ciljeve: jačanje zaštite prava pojedinca na zaštitu osobnih podataka i jamčenje slobodnog protoka osobnih podataka unutar EU-a[23]. Međutim, utvrđena su i brojna područja u kojima su moguća poboljšanja. Kao i većina dionika i tijela za zaštitu podataka, Komisija smatra da bi u ovoj fazi bilo prerano donositi konačne zaključke o primjeni Opće uredbe o zaštiti podataka. Vjerojatno će veće iskustvo u primjeni Uredbe u nadolazećim godinama pomoći pri rješavanju većine problema koje su utvrdile države članice i dionici. Unatoč tome, u ovom se izvješću naglašavaju izazovi na koje se dosad naišlo u primjeni Opće uredbe o zaštiti podataka te se utvrđuju mogući načini njihova rješavanja.

Bez obzira na to što se evaluacija prvenstveno bavi dvama pitanjima iz članka 97. stavka 2. Opće uredbe o zaštiti podataka, a to je međunarodni prijenos te mehanizmi suradnje i konzistentnosti, u evaluaciji i preispitivanju primjenjuje se širi pristup kako bi se riješila i pitanja koja su tijekom posljednje dvije godine postavili razni dionici.

2 GLAVNI ZAKLJUČCI

Provedba Opće uredbe o zaštiti podataka i funkcioniranje mehanizama suradnje i konzistentnosti

---

upotrebu mobilnih aplikacija za praćenje kontakata i upozoravanje kao odgovor na pandemiju koronavirusa. To je dio zajedničkoga koordiniranog pristupa za postupno ukidanje mjera ograničavanja. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

[16] Smjernice Komisije o primjeni prava Unije o zaštiti podataka u kontekstu izbora – Doprinos Europske komisije sastanku čelnika u Salzburgu 19.–20. rujna 2018. – COM(2018) 638 final.

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

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

[19] 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_en

[20] https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en

[21] Stručna skupina s više dionika za Uredbu koju je osnovala Komisija uključuje predstavnike civilnog društva i trgovačkih društava, pripadnike akademske zajednice i stručnjake: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537

[22] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Report-on-the-application-of-the-General-Data-Protection-Regulation/feedback?p_id=7669437

[23] Vidjeti, na primjer, stajalište i zaključke Vijeća te doprinos Odbora.

Općom uredbom o zaštiti podataka uspostavljen je inovativni sustav upravljanja koji se temelji na neovisnim tijelima za zaštitu podataka u državama članicama i njihovoj suradnji u prekograničnim slučajevima i u okviru Europskog odbora za zaštitu podataka. Opće je stajalište da su tijela za zaštitu podataka uravnoteženo iskoristila svoje povećane korektivne ovlasti, kao što su upozorenja i opomene, novčane kazne i privremena ili konačna ograničenja obrade[24]. Komisija napominje da su nadležna tijela primjenjivala upravne novčane kazne u rasponu od nekoliko tisuća do nekoliko milijuna eura, ovisno o težini prekršaja. Druge sankcije, kao što je zabrana obrade, mogu imati jednak, ako ne i veći odvraćajući učinak od novčanih kazni. Krajnji je cilj Opće uredbe o zaštiti podataka promijeniti kulturu i ponašanje svih dionika u korist pojedinaca. Detaljnije informacije o načinu na koji tijela za zaštitu podataka primjenjuju korektivne ovlasti navedene su u priloženom radnom dokumentu službi Komisije.

Iako je još uvijek rano za temeljitu procjenu funkcioniranja novih mehanizama suradnje i konzistentnosti, tijela za zaštitu podataka razvila su suradnju s pomoću „jedinstvenog mehanizma"[25] i širokom upotrebom uzajamne pomoći[26]. Taj jedinstveni mehanizam, koji je ključno sredstvo unutarnjeg tržišta, upotrebljava se za odlučivanje o mnogim prekograničnim slučajevima[27]. U tijeku je donošenje važnih odluka s prekograničnom dimenzijom na koje će se primjenjivati jedinstveni mehanizam. Te odluke, koje često uključuju velika multinacionalna tehnološka poduzeća, imat će znatan utjecaj na prava pojedinaca u mnogim državama članicama.

Međutim, istinski zajednička europska kultura zaštite podataka među tijelima za zaštitu podataka i dalje se razvija. Tijela za zaštitu podataka još nisu u potpunosti iskoristila instrumente predviđene Općom uredbom o zaštiti podataka, kao što su zajedničke operacije koje bi mogle dovesti do zajedničkih istraga. Ponekad je pronalaženje zajedničkog pristupa značilo prelazak na najmanji zajednički nazivnik, zbog čega su propuštene mogućnosti za veću usklađenost[28].

Potrebno je poduzeti daljnje korake kako bi rješavanje prekograničnih predmeta bilo učinkovitije i usklađenije diljem EU-a, među ostalim s postupovnog stajališta, primjerice u pitanjima kao što su postupci rješavanja pritužbi, kriteriji dopuštenosti pritužbi, trajanje postupaka zbog različitih rokova ili nepostojanje rokova u nacionalnom upravnom postupovnom pravu, trenutak u postupku u kojem se odobrava pravo na saslušanje ili obavješćivanje i uključenost podnositelja pritužbi tijekom postupka. Pozdravlja se postupak razmatranja koji je Odbor pokrenuo u tom pogledu, a Komisija sudjeluje u tim raspravama[29].

[24] Vidjeti točku 2.1. radnog dokumenta službi Komisije.
[25] Ako poduzeće obavlja prekograničnu obradu podataka, nadležno tijelo za zaštitu podataka jest tijelo države članice u kojoj poduzeće ima glavni poslovni nastan.
[26] Vidjeti točku 2.2. radnog dokumenta službi Komisije.
[27] Od 25. svibnja 2018. do 31. prosinca 2019. na temelju postupaka u okviru jedinstvenog mehanizma podnesen je 141 nacrt odluka, od kojih je 79 rezultiralo konačnim odlukama.
[28] Primjerice, nacionalni popisi vrsta postupaka obrade za koje je potrebna procjena učinka na zaštitu podataka u skladu s člankom 35. Opće uredbe o zaštiti podataka mogli bi biti bolje usklađeni.
[29] Vidjeti točku 2.2. radnog dokumenta službi Komisije.

Aktivnosti i smjernice Odbora ključne su za dosljedan daljnji razvoj razmjena između Odbora i dionika[30]. Od kraja 2019. Odbor je donio 67 dokumenata, uključujući deset novih smjernica[31], te 43 mišljenja[32]. Dionici općenito pozdravljaju smjernice Odbora i traže dodatne smjernice u pogledu ključnih pojmova Opće uredbe o zaštiti podataka, ali i upućuju na nedosljednosti između nacionalnih smjernica i smjernica Odbora. Naglašavaju da im je potrebno više praktičnih savjeta, posebno konkretnijih primjera, te potrebu da tijela za zaštitu podataka raspolažu potrebnim ljudskim, tehničkim i financijskim resursima za učinkovito obavljanje svojih zadaća.

Komisija je dosljedno naglašavala obvezu država članica da osiguraju dostatne ljudske, financijske i tehničke resurse nacionalnim tijelima za zaštitu podataka[33]. Osoblje i proračuni većine tijela povećali su se između 2016. i 2019.[34], pri čemu se najviše povećao broj članova osoblja irskih, nizozemskih, islandskih, luksemburških i finskih nadležnih tijela. S obzirom na to da najveća tehnološka multinacionalna poduzeća imaju poslovni nastan u Irskoj i Luksemburgu, tijela za zaštitu podataka tih zemalja vodeća su tijela u mnogim važnim prekograničnim slučajevima i možda će im biti potrebna veća sredstva nego što se čini sudeći po njihovom broju stanovnika. Međutim, stanje među državama članicama i dalje je neujednačeno i općenito još nije zadovoljavajuće. Tijela za zaštitu podataka imaju ključnu ulogu u osiguravanju provedbe Opće uredbe o zaštiti podataka na nacionalnoj razini te učinkovitog funkcioniranja mehanizama suradnje i konzistentnosti unutar Odbora, osobito jedinstvenog mehanizma za prekogranične slučajeve. Stoga se države članice pozivaju da im osiguraju odgovarajuća sredstva u skladu s Općom uredbom o zaštiti podataka[35].

Usklađena su pravila, ali i dalje postoji određen stupanj fragmentacije i različiti pristupi

Komisija prati provedbu Opće uredbe o zaštiti podataka u nacionalnom zakonodavstvu. U vrijeme sastavljanja ovog izvješća sve su države članice osim Slovenije donijele novo zakonodavstvo ili prilagodile svoje nacionalne zakone o zaštiti podataka. Od Slovenije[36] je zatraženo da Komisiji dostavi pojašnjenja o dovršetku tog postupka[37].

---

[30] Osobito trgovačkih društava i predstavnika civilnog društva. Vidjeti točku 2.3. radnog dokumenta službi Komisije.

[31] Uz njih, radna skupina iz članka 29. već je prije početka primjene Uredbe donijela deset smjernica, koje je podržao Odbor. Odbor je donio i četiri dodatne smjernice između siječnja i kraja svibnja 2020. te ažurirao jednu postojeću smjernicu.

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

[33] 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.

[34] Broj članova osoblja nacionalnih tijela za zaštitu podataka u EGP-u u razdoblju od 2016. do 2019. ukupno se povećao za 42 %, a proračun za 49 %.

[35] Vidjeti točku 2.4. radnog dokumenta službi Komisije.

[36] Posljednji put u pismu povjerenika Reyndersa iz ožujka 2020.

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

Općom uredbom o zaštiti podataka predviđa se dosljedan pristup pravilima o zaštiti podataka diljem EU-a. Međutim, njome se od država članica zahtijeva da u nekim područjima donose zakone[38], a u drugima im se pruža mogućnost da dodatno preciziraju način provedbe Opće uredbe o zaštiti podataka[39]. Stoga još uvijek postoji određeni stupanj fragmentacije, što je prije svega posljedica raširene primjene neobaveznih odredaba o specifikacijama. Primjerice, među državama članicama postoje razlike u dobi za privolu djece u pogledu usluga informacijskog društva, što dovodi do nesigurnosti za djecu i njihove roditelje u pogledu primjene njihovih prava na zaštitu podataka na jedinstvenom tržištu. Ta fragmentacija dovodi i do izazova u prekograničnom poslovanju i inovacijama, posebno u pogledu novih tehnoloških dostignuća i rješenja u području kibersigurnosti. Kako bi unutarnje tržište učinkovito funkcioniralo i kako bi se izbjeglo nepotrebno opterećivanje poduzeća, važno je i da nacionalno zakonodavstvo ne prelazi granice utvrđene Općom uredbom o zaštiti podataka i da se njime ne uvode dodatni zahtjevi ako takve granice nisu utvrđene.

Poseban izazov za nacionalno zakonodavstvo jest usklađivanje prava na zaštitu osobnih podataka sa slobodom izražavanja i informiranja te postizanje odgovarajuće ravnoteže između tih prava. U nekim je nacionalnim zakonodavstvima prednost dana slobodi izražavanja, dok je u drugima prednost dana zaštiti osobnih podataka, a iznimke od provedbe pravila o zaštiti podataka dopuštene su samo u posebnim situacijama, primjerice ako je riječ o javnoj osobi. Naposljetku, neke države članice ostavljaju mogućnost da o odstupanju od određenih odredaba Opće uredbe o zaštiti podataka odlučuje zakonodavac i/ili da odluke ovise o pojedinačnom slučaju.

Komisija će nastaviti s procjenom nacionalnog zakonodavstva. Usklađivanje mora biti predviđeno zakonom, njime se mora poštovati bit tih temeljnih prava te mora biti proporcionalno i nužno[40]. Pravila o zaštiti podataka (kao i njihovo tumačenje i primjena) ne bi trebala utjecati na ostvarivanje slobode izražavanja i informiranja, primjerice stvaranjem odvraćajućeg učinka ili vršenjem pritiska na novinare da otkriju svoje izvore. Uravnoteženje tih dvaju prava u nacionalnim zakonima trebalo bi se temeljiti na sudskoj praksi Suda i Europskog suda za ljudska prava[41].

U zakonodavstvu država članica postoje različiti pristupi provedbi odstupanja od opće zabrane obrade posebnih kategorija osobnih podataka u pogledu razine specifikacije i zaštitnih mjera, među ostalim u zdravstvene i istraživačke svrhe. Kako bi riješila to pitanje, Komisija najprije utvrđuje različite pristupe država članica[42], a zatim će poduprijeti donošenje kodeksâ ponašanja koji bi doprinijeli dosljednijem pristupu u tom području i olakšali prekograničnu obradu osobnih podataka[43]. Osim toga, buduće smjernice Odbora o uporabi osobnih podataka u području znanstvenih istraživanja doprinijet će usklađenom pristupu. Komisija će Odboru dati svoj doprinos, osobito u pogledu istraživanja u području zdravlja, među ostalim u obliku konkretnih pitanja i analize konkretnih scenarija koje je primila od istraživačke zajednice.

---

[38] Vidjeti točku 3.1. radnog dokumenta službi Komisije.
[39] Vidjeti točku 3.2. radnog dokumenta službi Komisije.
[40] Članak 52. stavak 1. Povelje.
[41] Vidjeti točku 3.1. radnog dokumenta službi Komisije: Usklađivanje prava na zaštitu osobnih podataka i slobode izražavanja i informiranja.
[42] Komisija je pokrenula studiju „Procjena pravila država članica o zdravstvenim podacima u svjetlu Opće uredbe o zaštiti podataka”, Chafea/2018/Health/03, posebni ugovor br. 2019 70 01.
[43] Vidjeti mjere najavljene u Europskoj strategiji za podatke, str. 30.

Jačanje položaja pojedinaca kako bi kontrolirali svoje podatke

Prema istraživanju o temeljnim pravima[44], 69 % stanovništva EU-a starijeg od 16 godina čulo je za Opću uredbu o zaštiti podataka, a 71 % upoznato je sa svojim nacionalnim tijelom za zaštitu podataka.

Pojedinci su sve bolje upoznati sa svojim pravima: pravom na pristup svojim osobnim podacima, pravom na njihov ispravak, brisanje i prenosivost, pravom prigovora na obradu te pravom na veću transparentnost. Općom uredbom o zaštiti podataka ojačana su postupovna prava, uključujući pravo na podnošenje pritužbe tijelu za zaštitu podataka, među ostalim i putem udružnih tužbi, te pravo na sudsku zaštitu. Pojedinci se sve više koriste tim pravima, ali treba olakšati njihovo ostvarivanje i potpunu provedbu. Razmatranjima koja vodi Odbor pojasnit će se i dodatno olakšati ostvarivanje prava pojedinaca, dok se očekuje da će predložena Direktiva o udružnim tužbama[45], nakon što bude donesena, omogućiti pojedincima pokretanje kolektivnih tužbi u svim državama članicama i smanjiti troškove prekograničnih postupaka.

Pravo na prenosivost podataka ima jasan potencijal, koji još nije u potpunosti iskorišten, da se pojedinci stave u središte podatkovnog gospodarstva tako što će im se omogućiti promjena pružatelja usluga, kombiniranje različitih usluga, upotreba drugih inovativnih usluga i odabir usluga koje najviše pogoduju zaštiti podataka. Time će se neizravno poticati tržišno natjecanje i podupirati inovacije. Iskorištavanje tog potencijala jedan je od prioriteta Komisije, posebno s obzirom na to da, uz sve veću uporabu uređaja priključenih na „internet stvari", sve više podataka generiraju potrošači koji bi se mogli suočiti s nepoštenim praksama i ovisnosti o pružatelju. Prenosivost bi mogla donijeti bolje zdravlje i veću dobrobit, smanjeni ekološki otisak te pristup javnim i privatnim uslugama, veću produktivnost u proizvodnji te veću kvalitetu i sigurnost proizvoda.

U podatkovnoj strategiji naglašena je potreba za rješavanjem poteškoća kao što je nedostatak standarda za pružanje podataka u strojno čitljivom formatu kako bi se bolje iskoristilo pravo na prenosivost podataka, koje je trenutačno ograničeno na tek nekoliko sektora (npr. bankarstvo i telekomunikacije). To bi se moglo postići ponajprije osmišljavanjem odgovarajućih alata, standardiziranog formata i sučeljâ[46]. Ta bi se povećana uporaba mogla postići i propisivanjem tehničkih sučelja i strojno čitljivih formata koji omogućuju prenosivost podataka u stvarnom vremenu. Povećanim ostvarivanjem prava na prenosivost mogao bi se, među ostalim, pojednostavniti način na koji pojedinci mogu dopustiti uporabu svojih podataka za javno dobro (primjerice za istraživanja u zdravstvenom sektoru) ako to žele učiniti („podatkovni altruizam"). Tijekom pripreme akta o digitalnim uslugama[47] Komisija će u širem smislu istražiti ulogu podataka i praksi povezanih s podacima u platformskom ekosustavu.

---

[44] 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

[45] Očekuje se da će se predloženom Direktivom o udružnim tužbama za zaštitu kolektivnih interesa potrošača (COM(2018) 184 final – 2018/089 (COD)), nakon njezina donošenja, ojačati okvir za udružne tužbe i u području zaštite podataka.

[46] Ti alati mogu uključivati alate za upravljanje privolom i aplikacije za upravljanje osobnim informacijama.

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

Prilike i izazovi za organizacije, posebice mala i srednja poduzeća

U okviru Opće uredbe o zaštiti podataka, zajedno s Uredbom o slobodnom protoku neosobnih podataka[48], potiču se tržišno natjecanje i inovacije, osigurava se slobodan protok podataka unutar EU-a i stvaraju se jednaki uvjeti za poduzeća s poslovnim nastanom izvan EU-a[49]. Pravo na prenosivost i činjenica da sve veći broj pojedinaca traži rješenja koja više pogoduju privatnosti mogu dovesti do smanjenja prepreka za ulazak poduzeća na tržište i otvaranja mogućnosti za rast koji se temelji na povjerenju i inovacijama. Neki dionici navode da primjena Opće uredbe o zaštiti podataka predstavlja izazov posebno za mala i srednja poduzeća (MSP-ove). U skladu s pristupom koji se temelji na riziku, ne bi bilo primjereno predvidjeti odstupanja na temelju veličine subjekta jer njihova veličina nije sama po sebi pokazatelj rizika za pojedince koji može proizaći iz obrade osobnih podataka koju ono provodi. Više tijela za zaštitu podataka pružilo je MSP-ovima koji se bave obradom podataka niskog rizika praktične alate kojima se olakšava primjena Opće uredbe o zaštiti podataka. Takve bi aktivnosti trebalo pojačati i proširiti, po mogućnosti u okviru zajedničkog europskog pristupa kako se ne bi stvarale prepreke jedinstvenom tržištu.

Tijela za zaštitu podataka pokrenula su niz aktivnosti kako bi pomogla MSP-ovima da ispune zahtjeve iz Opće uredbe o zaštiti podataka; primjerice, osigurala su predloške za ugovore o obradi podataka i evidencije o aktivnostima obrade, organizirale seminare i uvele telefonske linije za savjetovanje. Neke od tih inicijativa financirale su se sredstvima EU-a[50]. Trebalo bi razmotriti i druge aktivnosti kojima bi se olakšala primjena Opće uredbe o zaštiti podataka za MSP-ove.

Kako bi im se pomoglo dokazati da ispunjavaju zahtjeve, svim je vrstama poduzeća i organizacija dan na raspolaganje paket instrumenata na temelju Opće uredbe o zaštiti podataka, kao što su kodeksi ponašanja, mehanizmi certificiranja i standardna ugovorna klauzula. Taj bi paket instrumenata trebalo u potpunosti iskoristiti. MSP-ovi su posebno naglasili važnost i korisnost kodeksâ ponašanja koji su prilagođeni njihovoj situaciji i koji ne podrazumijevaju nerazmjerne troškove. Kad je riječ o programima certificiranja, sigurnost (uključujući kibersigurnost) i integrirana zaštita podataka ključni su elementi koje treba uzeti u obzir u okviru Opće uredbe o zaštiti podataka i koji bi imali koristi od zajedničkog i ambicioznog pristupa diljem EU-a. Komisija trenutačno radi na standardnim ugovornim klauzulama između voditeljâ obrade i izvršiteljâ obrade[51], koje će se temeljiti na tekućem radu na modernizaciji standardnih ugovornih klauzula za međunarodne prijenose[52].

---

[48] 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.

[49] Vidjeti točku 5. radnog dokumenta službi Komisije. Vidjeti i COM(2019) 250 final Smjernice o Uredbi o okviru za slobodan protok neosobnih informacija u Europskoj uniji, gdje se objašnjavaju pravila kojima se uređuje obrada miješanih skupova podataka koji se sastoje od osobnih i neosobnih podataka, čineći to praktičnim za poduzeća, uključujući MSP-ove.

[50] 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 te malih i srednjih poduzeća: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en. Još milijun EUR dodijelit će se 2020.

[51] U skladu s člankom 28. Opće uredbe o zaštiti podataka.

[52] U skladu s člankom 46. Opće uredbe o zaštiti podataka.

Primjena Opće uredbe o zaštiti podataka na nove tehnologije

Budući da je osmišljena tako da bude tehnološki neutralna, Opća uredba o zaštiti podataka temelji se na načelima i stoga obuhvaća nove tehnologije tijekom njihova razvoja.

Smatra se ključnim i fleksibilnim instrumentom kojim se osigurava da razvoj novih tehnologija bude u skladu s temeljnim pravima. Zakonodavni okvir o zaštiti podataka i privatnosti pokazao se važnim i fleksibilnim tijekom krize uzrokovane bolešću COVID-19, posebno u pogledu osmišljavanja aplikacija za praćenje i drugih tehnoloških rješenja za borbu protiv pandemije. Budući izazovi nalaze se u razjašnjavanju načina primjene dokazanih načela na konkretne tehnologije kao što su umjetna inteligencija, lanac blokova, internet stvari ili prepoznavanje lica, koje zahtijevaju stalno praćenje. Primjerice, Bijelom knjigom Komisije o umjetnoj inteligenciji[53] otvorena je javna rasprava o posebnim okolnostima, ako postoje, kojima bi se mogla opravdati upotreba umjetne inteligencije za biometrijsku identifikaciju na daljinu (kao što je prepoznavanje lica) na javnim mjestima te o zajedničkim zaštitnim mjerama. U tom bi pogledu tijela za zaštitu podataka trebala biti spremna od početka pratiti procese nastanka tehničkih rješenja.

Nadalje, 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, neophodna je za zaštitu pojedinaca.

Razvoj modernog paketa instrumenata za međunarodni prijenos podataka

Općom uredbom o zaštiti podataka nudi se modernizirani paket instrumenata za olakšavanje prijenosa osobnih podataka iz EU-a u treću zemlju ili međunarodnu organizaciju, a istodobno se osigurava da se na te podatke i dalje primjenjuje visoka razina zaštite. U posljednje dvije godine Komisija intenzivnije radi na iskorištavanju punog potencijala instrumenata dostupnih u okviru Opće uredbe o zaštiti podataka.

Primjerice, surađuje s ključnim partnerima u cilju donošenja „odluke o primjerenosti". Učinak je takve odluke omogućiti siguran i slobodan protok osobnih podataka u dotičnu treću zemlju, a da pritom izvoznik podataka ne mora pružiti dodatne zaštitne mjere ili ishoditi odobrenje. Konkretno, uzajamnim odlukama o primjerenosti između EU-a i Japana, koje su stupile na snagu u veljači 2019., stvoreno je najveće područje slobodnog i sigurnog protoka podataka na svijetu. Usto, postupak procjene primjerenosti s Republikom Korejom u kasnoj je fazi, a u tijeku su i preliminarni pregovori s drugim važnim partnerima u Aziji i Latinskoj Americi.

Primjerenost igra i važnu ulogu u kontekstu budućeg odnosa s Ujedinjenom Kraljevinom, pod uvjetom da su ispunjeni svi primjenjivi uvjeti. Ona omogućuje trgovinu, uključujući digitalnu trgovinu, te je ključni preduvjet za blisku i ambicioznu suradnju u području kaznenog progona i sigurnosti. Nadalje, visok stupanj konvergencije u zaštiti podataka važan je element za osiguravanje ravnopravnih uvjeta za dva tako blisko povezana gospodarstva. U skladu s političkom izjavom o budućem odnosu između EU-a i Ujedinjene Kraljevine, Komisija trenutačno provodi

[53] Bijela knjiga o umjetnoj inteligenciji – Europski pristup izvrsnosti i povjerenju, COM(2020) 65 final.

procjenu primjerenosti na temelju Opće uredbe o zaštiti podataka i Direktive o zaštiti podataka za potrebe kaznenog progona[54].

U okviru prve evaluacije Opće uredbe o zaštiti podataka Komisija je dužna preispitati i odluke o primjerenosti koje su donesene na temelju prijašnjih pravila[55]. Službe Komisije sudjelovale su u intenzivnom dijalogu sa svakom od jedanaest predmetnih trećih zemalja i državnih područja[56] kako bi procijenile kako su se njihovi sustavi za zaštitu podataka razvijali od donošenja odluke o primjerenosti te ispunjavaju li standarde utvrđene u Općoj uredbi o zaštiti podataka. Potreba da se osigura kontinuitet takvih odluka, kao ključnog instrumenta za trgovinu i međunarodnu suradnju, jedan je od čimbenika zbog kojih je nekoliko tih zemalja i područja moderniziralo i ojačalo svoje zakone o privatnosti. S nekima od tih zemalja i državnih područja raspravlja se o dodatnim zaštitnim mjerama kako bi se riješile relevantne razlike u području zaštite. Međutim, s obzirom na to da presuda Suda koja će se donijeti 16. srpnja može sadržavati pojašnjenja koja bi mogla biti relevantna za određene elemente standarda primjerenosti, Komisija će zasebno izvijestiti o evaluaciji postojećih odluka o primjerenosti nakon što Sud donese presudu u tom predmetu[57].

Osim na primjerenosti, Komisija radi na sveobuhvatnoj modernizaciji standardnih ugovornih klauzula kako bi ih ažurirala s obzirom na nove zahtjeve uvedene Općom uredbom o zaštiti podataka. Cilj je da one bolje odražavaju stvarnu problematiku postupaka obrade u modernom digitalnom gospodarstvu i da se razmotri moguća potreba da se, među ostalim s obzirom na očekivanu presudu Suda, dodatno pojasne određene zaštitne mjere[58]. Te klauzule predstavljaju daleko najrašireniji mehanizam za prijenos podataka, pri čemu se na njih oslanjaju tisuće poduzeća iz EU-a kako bi svojim klijentima, dobavljačima, partnerima i zaposlenicima pružile širok raspon usluga.

Odbor je imao aktivnu ulogu i u razvoju međunarodnih aspekata Opće uredbe o zaštiti podataka. To uključuje ažuriranje smjernica o postojećim mehanizmima prijenosa, kao što su obvezujuća korporativna pravila i takozvana „odstupanja”, te razvoj pravne infrastrukture za upotrebu novih instrumenata uvedenih Općom uredbom o zaštiti podataka, tj. kodeksâ ponašanja i certificiranja.

Kako bi se dionicima omogućilo da u potpunosti iskoriste paket instrumenata za prijenos iz Opće uredbe o zaštiti podataka, Odbor mora još intenzivnije raditi na različitim mehanizmima prijenosa, među ostalim još i više pojednostavniti postupak

---

[54] Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP, SL L 119, 4.5.2016., str. 89.–131.

[55] Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, SL L 281, 23.11.1995., str. 31.–50.

[56] Te su zemlje i državna područja: Andora, Argentina, Kanada, Farski otoci, Guernsey, Jersey, Otok Man, Izrael, Novi Zeland, Švicarska i Urugvaj.

[57] Vidjeti predmet C-311/18, Data Protection Commissioner protiv Facebook Ireland Limited, Maximilliana Schremsa („Schrems II”), koji se odnosi na zahtjev za prethodnu odluku o takozvanim standardnim ugovornim klauzulama. Međutim, Sud može dodatno pojasniti određene elemente standarda primjerenosti.

[58] Vidjeti predmet Schrems II.

odobravanja obvezujućih korporativnih pravila, dovršiti smjernice o kodeksima ponašanja i certificiranju kao instrumentima za prijenose te pojasniti međudjelovanje pravila o međunarodnim prijenosima podataka (poglavlje V.) s teritorijalnim područjem primjene Opće uredbe o zaštiti podataka (članak 3.).

Još jedan važan aspekt međunarodne dimenzije pravila EU-a o zaštiti podataka jest prošireno teritorijalno područje primjene Opće uredbe o zaštiti podataka, koje obuhvaća i aktivnosti obrade stranih subjekata aktivnih na tržištu EU-a. Kako bi se osigurala učinkovita usklađenost s Općom uredbom o zaštiti podataka i istinski jednaki uvjeti, ključno je da se to proširenje na odgovarajući način odrazi u mjerama izvršenja tijela za zaštitu podataka. Te bi mjere posebno trebale uključivati, prema potrebi, predstavnika voditelja obrade ili izvršitelja obrade u EU-u, kojem se moguće obratiti kao i poduzeću sa sjedištem izvan EU-a ili umjesto njega. Taj bi se pristup trebao snažnije primjenjivati kako bi se poslala jasna poruka da nepostojanje poslovnog nastana u EU-u ne oslobađa strane poslovne subjekte od odgovornosti koju imaju na temelju Opće uredbe o zaštiti podataka.

Promicanje konvergencije i međunarodne suradnje u području zaštite podataka

Opća uredba o zaštiti podataka već je sada ključna referentna točka na međunarodnoj razini i zbog nje mnoge zemlje diljem svijeta razmatraju uvođenje modernih pravila o privatnosti. Taj trend prema globalnoj konvergenciji vrlo je pozitivan jer se zbog njega stvaraju nove mogućnosti za bolju zaštitu pojedinaca u EU-u pri prijenosu njihovih podataka u inozemstvo, dok se istodobno olakšava protok podataka.

Nadovezujući se na taj trend, Komisija je pojačala dijalog u nizu bilateralnih, regionalnih i multilateralnih foruma kako bi potaknula globalnu kulturu poštovanja privatnosti i stvaranje elemenata konvergencije među različitim sustavima privatnosti. Komisija se u svojim naporima oslanjala i nastavit će računati na aktivnu potporu Europske službe za vanjsko djelovanje i mreže delegacija EU-a u trećim zemljama i misija u međunarodnim organizacijama. To je omogućilo i veću dosljednost i komplementarnost različitih aspekata vanjske dimenzije politika EU-a – od trgovine do novog partnerstva EU-a i Afrike. Skupine G20 i G7 također su nedavno uvidjele da zaštita podataka pridonosi većem povjerenju u digitalno gospodarstvo i protok podataka, osobito putem ideje „slobodnog protoka podataka uz puno povjerenje" koju je izvorno predložio Japan tijekom predsjedanja skupinom G20[59]. U podatkovnoj strategiji ističe se namjera Komisije da nastavi promicati razmjenu podataka s pouzdanim partnerima te da se pritom bori protiv zlouporaba kao što je nerazmjeran pristup (stranih) javnih tijela osobnim podacima.

Uz promicanje konvergencije standarda zaštite podataka na međunarodnoj razini kako bi se olakšao protok podataka, a time i trgovina, Komisija je odlučna i u borbi protiv digitalnog protekcionizma, kako je nedavno istaknuto u podatkovnoj strategiji.[60] U tu je svrhu razvila posebne odredbe o protoku podataka i zaštiti podataka u trgovinskim

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

[60] Podatkovna strategija, str. 23.

sporazumima[61] koje sustavno navodi u bilateralnim – posljednji put s Australijom, Novim Zelandom i Ujedinjenom Kraljevinom – i multilateralnim pregovorima, primjerice u aktualnim pregovorima WTO-a o e-trgovini[62]. Tim se horizontalnim odredbama isključuju neopravdana ograničenja, kao što su prisilna lokalizacija podataka, te se čuva regulatorna autonomija stranaka u pogledu poštovanja temeljnog prava na zaštitu podataka.

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, pa i malih i srednjih poduzeća, u okolnostima sve veće digitalizacije gospodarstva.

Isto tako, važno je da poduzeća koja posluju na europskom tržištu i prime opravdan zahtjev za dijeljenje podataka u svrhu kaznenog progona te podatke mogu podijeliti bez rizika od sukoba zakona i potpuno poštujući temeljna prava EU-a. Da bi se poboljšali takvi prijenosi podataka, Komisija se obvezuje razviti odgovarajuće pravne okvire sa svojim međunarodnim partnerima kako bi se izbjegao sukob zakona i poticala djelotvorna suradnja, konkretno tako da osigura potrebne mjere za zaštitu podataka, te time doprinijeti učinkovitijoj borbi protiv kriminala.

Naposljetku, u vrijeme kada problemi povezani s poštovanjem privatnosti ili incidenti u području sigurnosti podataka mogu istodobno utjecati na velik broj pojedinaca u više jurisdikcija, trebalo bi dodatno ojačati suradnju „na terenu" između europskih i međunarodnih regulatornih tijela. To konkretno zahtijeva razvoj odgovarajućih pravnih instrumenata za bliskije oblike suradnje i uzajamne pomoći, među ostalim tako da se dopusti nužna razmjena informacija u kontekstu istraga. U tom duhu Komisija osniva i „Akademiju za zaštitu podataka", platformu na kojoj bi EU i strana tijela za zaštitu podataka razmjenjivali znanja, iskustva i najbolju praksu kako bi olakšali i podržali suradnju među tijelima za provedbu zaštite privatnosti.

3 DALJNJI KORACI

Kako bi se ostvario puni potencijal Opće uredbe o zaštiti podataka, važno je uspostaviti usklađeni pristup i zajedničku europsku kulturu zaštite podataka te poticati učinkovitije i usklađenije rješavanje prekograničnih slučajeva. To očekuju pojedinci i poduzeća te je to jedan od najvažnijih ciljeva reforme pravila EU-a o zaštiti podataka. Jednako je važno osigurati da se svi instrumenti dostupni u Općoj uredbi o zaštiti podataka u potpunosti upotrebljavaju, a time i da ih učinkovito primjenjuju pojedinci i poduzeća.

Komisija će nastaviti s bilateralnim razmjenama s državama članicama o provedbi Opće uredbe o zaštiti podataka te će, prema potrebi, nastaviti upotrebljavati sve

[61] Vidjeti tekst horizontalnih odredaba za prekogranični prijenos podataka i zaštitu osobnih podataka (u trgovinskim sporazumima i sporazumima o ulaganjima EU-a): https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf

[62] Osamdeset i četiri članice WTO-a sada sudjeluju u plurilateralnim pregovorima o e-trgovini, slijedom inicijative za zajedničku izjavu koju su ministri donijeli 25. siječnja 2019. u Davosu. U okviru tog postupka EU je 3. svibnja 2019. podnio prijedlog teksta o budućim pravilima i obvezama u području e-trgovine. Prijedlog sadrži horizontalne odredbe o protoku podataka i zaštiti osobnih podataka: https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf

raspoložive instrumente kako bi potaknula države članice da poštuju svoje obveze na temelju Opće uredbe o zaštiti podataka.

S obzirom na procjenu nacionalnog zakonodavstva koja je u tijeku, kratko razdoblje koje je proteklo od početka primjene Opće uredbe o zaštiti podataka u kojem su se stekla praktična iskustva i činjenicu da se sektorsko zakonodavstvo u mnogim državama članicama još uvijek revidira, još je prerano za donošenje konačnih zaključaka o postojećoj razini fragmentacije. U pogledu mogućeg sukoba zakona zbog provedbe odredaba o specifikacijama u državama članicama, najprije je potrebno bolje razumjeti posljedice za voditelje i izvršitelje obrade podataka[63].

Prilikom daljnjeg postupanja u vezi s tim pitanjima u dosljednom tumačenju pravila o zaštiti podataka pomaže relevantna sudska praksa nacionalnih sudova i Suda. Nacionalni sudovi nedavno su donijeli presude kojima se poništavaju odredbe nacionalnih zakona koje odstupaju od Opće uredbe o zaštiti podataka[64].

Na međunarodnoj razini Komisija će i dalje promicati konvergenciju pravila o zaštiti podataka kako bi se osigurao siguran protok podataka. To uključuje različite oblike „prethodnog" rada, na primjer u okviru tekućih reformi za nove ili ažurirane zakone o zaštiti podataka, ili zagovaranje koncepta „slobodnog protoka podataka uz puno povjerenje" na multilateralnim forumima. Obuhvaća i razne dijaloge o primjerenosti te modernizaciju i proširenje našeg paketa instrumenata za prijenos ažuriranjem standardnih ugovornih klauzula i postavljanjem temelja za mehanizme certificiranja. Taj rad uključuje i međunarodne pregovore, primjerice u području prekograničnog pristupa elektroničkim dokazima, kako bi se osiguralo da će se kod prijenosa podataka poštovati odgovarajuće mjere zaštite podataka. Naposljetku, pokretanjem pregovora o međunarodnoj suradnji i uzajamnoj pomoći među tijelima za provedbu zaštite podataka Komisija će nastojati primijeniti konvergenciju u praksi.

Na temelju evaluacije primjene Opće uredbe o zaštiti podataka, od svibnja 2018. utvrđeno je da su za potporu njezinoj primjeni potrebne mjere navedene u nastavku. Komisija će pratiti njihovu provedbu i s obzirom na predstojeće izvješće o evaluaciji 2024.

Provedba i dopuna pravnog okvira

Države članice trebale bi:

- dovršiti usklađivanje svojih sektorskih zakona s Općom uredbom o zaštiti podataka;
- razmotriti mogućnost ograničavanja uporabe odredaba o specifikacijama koje bi mogle uzrokovati fragmentaciju i ugroziti slobodan protok podataka unutar EU-a;
- ocijeniti nalazi li se nacionalno pravo kojim se provodi Opća uredba o zaštiti podataka u svim okolnostima unutar granica predviđenih zakonodavstvom država članica.

[63] Usp. stajalište Vijeća i zaključke o primjeni Opće uredbe o zaštiti podataka.
[64] Primjerice u Njemačkoj i Španjolskoj, a u Austriji su se uklonili nedostaci u nacionalnom zakonodavstvu.

Komisija će učiniti sljedeće:

- ostvariti bilateralne razmjene s državama članicama o usklađenosti nacionalnih zakona s Općom uredbom o zaštiti podataka, među ostalim o neovisnosti i resursima nacionalnih tijela za zaštitu podataka; upotrijebiti sve instrumente koji su joj na raspolaganju, uključujući postupke zbog povrede, kako bi osiguralo da države članice poštuju Opću uredbu o zaštiti podataka;
- podupirati daljnje razmjene mišljenja i nacionalne prakse među državama članicama o pitanjima koja se trebaju dodatno specificirati na nacionalnoj razini kako bi se smanjila fragmentacija jedinstvenog tržišta, kao što je obrada osobnih podataka povezanih sa zdravljem i istraživanjima, ili pitanjima kod kojih treba potražiti ravnotežu s drugim pravima, poput slobode izražavanja;
- podupirati dosljednu primjenu okvira za zaštitu podataka u odnosu na nove tehnologije kako bi se pružila potpora inovacijama i tehnološkom razvoju;
- aktivirati stručnu skupinu država članica za Opću uredbu o zaštiti podataka (osnovanu tijekom prijelazne faze prije početka primjene te uredbe) kako bi se olakšale rasprave i razmjena iskustava među državama članicama i s Komisijom;
- istražiti bi li, s obzirom na daljnje iskustvo i relevantnu sudsku praksu, bilo primjereno predložiti moguće buduće ciljane izmjene određenih odredaba Opće uredbe o zaštiti podataka, posebno u pogledu evidencije o obradi koju provode MSP-ovi čija glavna djelatnost nije obrada osobnih podataka (nizak rizik)[65] i mogućeg usklađivanja dobi za privolu djece u vezi s uslugama informacijskog društva.

Ostvarivanje punog potencijala novog sustava upravljanja

Odbor i tijela za zaštitu podataka pozivaju se da:

- postignu učinkovite dogovore među tijelima za zaštitu podataka o funkcioniranju mehanizama suradnje i konzistentnosti, među ostalim o postupovnim aspektima, oslanjajući se na stručnost svojih članova i jačajući sudjelovanje tajništva Odbora;
- podupiru usklađivanje u primjeni i provedbi Opće uredbe o zaštiti podataka upotrebom svih sredstava koja su im na raspolaganju, među ostalim tako da dodatno pojasne ključne pojmove Opće uredbe o zaštiti podataka i osiguraju da su nacionalne smjernice u potpunosti u skladu sa smjernicama koje je donio Odbor;
- potiču upotrebu svih instrumenata predviđenih Općom uredbom o zaštiti podataka kako bi se osigurala njezina dosljedna primjena;
- jačaju suradnju među tijelima za zaštitu podataka, primjerice provođenjem zajedničkih istraga.

Komisija će učiniti sljedeće:

[65] Članak 30. stavak 5. Opće uredbe o zaštiti podataka.

- nastaviti pomno pratiti djelotvornu i potpunu neovisnost nacionalnih tijela za zaštitu podataka;
- poticati suradnju među regulatornim tijelima (posebno u područjima kao što su tržišno natjecanje, elektroničke komunikacije, sigurnost mrežnih i informacijskih sustava i politika zaštite potrošača);
- podržati, u okviru Odbora, razmatranje postupaka koje primjenjuju nacionalna tijela za zaštitu podataka kako bi se poboljšala suradnja u prekograničnim slučajevima.

Države članice trebaju:

- dodijeliti dostatna sredstva tijelima za zaštitu podatka kako bi ona mogla izvršavati svoje zadaće.

Potpora dionicima

Odbor i tijela za zaštitu podataka pozivaju se da:

- donesu daljnje smjernice koje će biti praktične i lako razumljive te kojima će se pružiti jasni odgovori i izbjeći nejasnoće u pogledu pitanja povezanih s primjenom Opće uredbe o zaštiti podataka, primjerice u pogledu obrade podataka djece i prava ispitanika, uključujući ostvarivanje prava na pristup i prava na brisanje, uz savjetovanje s dionicima u postupku;
- preispitaju smjernice kada su potrebna dodatna pojašnjenja s obzirom na iskustvo i razvoj događaja, među ostalim u sudskoj praksi Suda;
- razviju praktične alate, kao što su usklađeni obrasci za povrede podataka i pojednostavljene evidencije o aktivnostima obrade, kako bi se MSP-ovima koji se bave obradom podataka niskog rizika pomoglo da ispune svoje obveze.

Komisija će učiniti sljedeće:

- osigurati standardne ugovorne klauzule, kako za međunarodne prijenose tako i za odnos između voditelja obrade i izvršitelja obrade;
- osigurati alate za pojašnjavanje/podupiranje primjene pravila o zaštiti podataka na djecu[66];
- u skladu s podatkovnom strategijom istražiti praktične načine za olakšavanje većeg iskorištavanja prava pojedinaca na prenosivost, primjerice tako da im se omogući veća kontrola nad time tko može pristupiti strojno generiranim podacima i koristiti se njima;
- putem suradnje između Agencije Europske unije za kibersigurnost, tijela za zaštitu podataka i Odbora podržati standardizaciju/certifikaciju, posebice u pogledu aspekata kibersigurnosti;

[66] Projekt Komisije o alatima za utvrđivanje dobi – pilot-projekt za dokazivanje interoperabilne tehničke infrastrukture za zaštitu djece, uključujući provjeru dobi i suglasnost roditelja. Očekuje se da će se time poduprijeti provedba mehanizama za zaštitu djece na temelju postojećega zakonodavstva EU-a koje je relevantno za zaštitu djece na internetu.

- prema potrebi, iskoristiti svoje pravo da od Odbora zatraži pripremu smjernica i mišljenja o posebnim pitanjima koja su važna za dionike;
- pružiti smjernice, prema potrebi, uz potpuno poštovanje uloge Odbora;
- osigurati financijsku potporu za djelatnosti tijela za zaštitu podataka kojima se MSP-ovima olakšava provedba obveza iz Opće uredbe o zaštiti podataka, posebice za praktične smjernice i digitalne alate koje mogu koristiti i druge države članice.

Poticanje inovacija

Komisija će učiniti sljedeće:

- pratiti primjenu Opće uredbe o zaštiti podataka na nove tehnologije, uzimajući u obzir i moguće buduće inicijative u području umjetne inteligencije i u okviru podatkovne strategije;
- poticati, među ostalim i pružanjem financijske potpore, izradu kodeksâ ponašanja EU-a u području zdravlja i istraživanja;
- pomno pratiti razvoj i upotrebu aplikacija u kontekstu pandemije bolesti COVID-19.

Odbor se poziva da:

- izradi smjernice o primjeni Opće uredbe o zaštiti podataka u području znanstvenih istraživanja, umjetne inteligencije, lanca blokova i drugih mogućih tehnoloških dostignuća;
- preispita smjernice kada su potrebna dodatna pojašnjenja s obzirom na tehnološki razvoj.

Daljnji razvoj instrumenata za prijenos podataka

Komisija će učiniti sljedeće:

- nastaviti dijaloge o primjerenosti sa zainteresiranim trećim zemljama, u skladu sa strategijom utvrđenom u njezinoj Komunikaciji iz 2017. „Razmjena i zaštita osobnih podataka u globaliziranom svijetu”, pri čemu će, gdje je to moguće, obuhvatiti prijenose podataka tijelima kaznenog progona (u skladu s Direktivom o zaštiti podataka za potrebe kaznenog progona) i drugim javnim tijelima; to uključuje što skorije dovršenje postupka procjene primjerenosti s Republikom Korejom;
- dovršiti evaluaciju postojećih odluka o primjerenosti i o tome izvijestiti Europski parlament i Vijeće;
- dovršiti rad na modernizaciji standardnih ugovornih klauzula u cilju njihova ažuriranja s obzirom na Opću uredbu o zaštiti podataka, pri čemu će obuhvatiti sve relevantne scenarije prijenosa i bolje uzeti u obzir moderne poslovne prakse.

Odbor se poziva da:

- dodatno pojasni međudjelovanje pravila o međunarodnim prijenosima podataka (poglavlje V.) i teritorijalnog područja primjene Opće uredbe o zaštiti podataka (članak 3.);
- osigura djelotvorno izvršenje u odnosu na subjekte s poslovnim nastanom u trećim zemljama koji su obuhvaćeni teritorijalnim područjem primjene Opće uredbe o zaštiti podataka, među ostalim u pogledu imenovanja predstavnika ako je to primjenjivo (članak 27.);
- pojednostavni procjenu i eventualno odobravanje obvezujućih korporativnih pravila kako bi se ubrzao postupak;
- dovrši rad na arhitekturi, postupcima i kriterijima procjene za kodekse ponašanja i mehanizme certificiranja kao instrumente za prijenos podataka.

Promicanje konvergencije i razvoj međunarodne suradnje

Komisija će učiniti sljedeće:

- podupirati tekuće procese reformi u trećim zemljama povezane s novim ili moderniziranim pravilima o zaštiti podataka razmjenom iskustava i najbolje prakse;
- surađivati s afričkim partnerima na promicanju regulatorne konvergencije i podržavanju izgradnje kapaciteta nadzornih tijela u okviru digitalnog poglavlja novog partnerstva EU-a i Afrike;
- procijeniti kako bi se mogla olakšati suradnja privatnih gospodarskih subjekata i tijela kaznenog progona, među ostalim putem pregovora o bilateralnim i multilateralnim okvirima za prijenose podataka u kontekstu pristupa stranih tijela kaznenog progona elektroničkim dokazima, kako bi se izbjegli sukobi zakona te istodobno osigurale odgovarajuće mjere za zaštitu podataka;
- surađivati s međunarodnim i regionalnim organizacijama kao što su OECD, ASEAN ili skupina G20 radi promicanja pouzdanog protoka podataka koji se temelji na visokim standardima zaštite podataka, među ostalim u kontekstu inicijative „slobodnog protoka podataka uz puno povjerenje”;
- osnovati „Akademiju za zaštitu podataka” kako bi se olakšale i podupirale razmjene između europskih i međunarodnih regulatornih tijela;
- promicati međunarodnu suradnju među nadzornim tijelima u području provedbe, među ostalim putem pregovora o sporazumima o suradnji i uzajamnoj pomoći.