



Bruxelles, 10.1.2017.
COM(2017) 7 final

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU

Razmjena i zaštita osobnih podataka u globaliziranom svijetu

1. UVOD

Zaštita osobnih podataka dio je europske zajedničke ustavne strukture i ugrađena je u članak 8. Povelje EU-a o temeljnim pravima. Središnji je dio prava EU-a već više od 20 godina, od Direktive o zaštiti osobnih podataka iz 1995.¹ (dalje u tekstu „Direktiva iz 1995.”) do donošenja Opće uredbe o zaštiti podataka² i Direktive o policiji³ 2016.

Kako je predsjednik Juncker istaknuo u govoru o stanju Europske unije 14. rujna 2016.: „[b]iti Europljanin znači imati pravo na zaštitu svojih osobnih podataka u okviru čvrstih europskih zakona. Jer Europa cijeni privatnost. To je pitanje ljudskog dostojanstva.”

Međutim, potražnja za zaštitom osobnih podataka nije ograničena samo na Europu. Potrošači diljem svijeta sve više cijene privatnost. S druge strane, poduzeća uviđaju da im čvrsta zaštita podataka daje konkurentnu prednost jer se povećava povjerenje u njihove usluge. Mnoga, posebno ona koja posluju u cijelom svijetu, usklađuju svoje politike zaštite podataka s Općom uredbom o zaštiti podataka jer žele poslovati u EU-u, a ujedno je vide i kao primjer koji mogu slijediti.

Slično tomu, neke zemlje i regionalne organizacije izvan EU-a, od najbližeg susjedstva do Azije, Latinske Amerike i Afrike, donose novo ili ažuriraju postojeće zakonodavstvo o zaštiti podataka kako bi iskoristile prilike koje pruža svjetsko digitalno gospodarstvo i odgovorile na rastuću potražnju za čvršćom zaštitom podataka i privatnosti. Iako u tim zemljama postoje razlike u pristupu i stupnju zakonodavnog razvoja, vide se znakovi uzlazne konvergencije važnih načela zaštite podataka, posebno u određenim regijama svijeta⁴. Većom kompatibilnošću različitih sustava za zaštitu podataka olakšali bi se međunarodni tokovi osobnih podataka u komercijalne svrhe ili u svrhu suradnje javnih tijela (npr. pri izvršavanju zakonodavstva). EU bi trebao iskoristiti ovu priliku za promicanje svojih vrijednosti u pogledu zaštite podataka i olakšavanje tokova podataka poticanjem konvergencije pravnih sustava. Kako je najavljeno u programu rada Komisije⁵, ovom se Komunikacijom stoga utvrđuje strateški okvir Komisije za odluke o primjerenosti i druge alate za prijenos podataka te međunarodne instrumente za zaštitu podataka.

¹ 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.).

² 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 (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.-88.). Stupila je na snagu 24. svibnja 2016. i počinje se primjenjivati 25. svibnja 2018.

³ 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.). Na snagu je stupila 5. svibnja 2016. Države članice EU-a moraju je prenijeti u nacionalno zakonodavstvo do 6. svibnja 2018.

⁴ Vidjeti „Data protection regulations and international data flows: Implications for trade and development”, UNCTAD (2016): http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

⁵ Program rada Komisije za 2017. „Izgradnja Europe koja štiti, osnažuje i brani”, COM(2016) 710 final, 25.10.2016., str. 12. i Prilog 1.

2. PAKET REFORMI ZAŠTITE PODATAKA U EU-U – SUVREMEN ZAKONODAVNI OKVIR KOJIM SE PODUPIRU MEĐUNARODNI TOKOVI PODATAKA UZ VISOKU RAZINU ZAŠTITE

Reformom zakonodavstva EU-a o zaštiti podataka donesenom u travnju 2016. uspostavlja se sustav kojim se osigurava visoka razina zaštite i koji je otvoren za mogućnosti svjetskog informacijskog društva. Pojedinci su tom reformom dobili veću kontrolu nad vlastitim podacima te je tako ojačano povjerenje potrošača u digitalno gospodarstvo. Usklađivanjem i pojednostavnjenjem pravnog okruženja domaćim je i stranim poduzećima poslovanje u EU-u, među ostalim i putem međunarodnih razmjena podataka, olakšano te uključuje manje opterećenja. EU danas pruža otvorenost za međunarodne tokove podataka uz najvišu razinu zaštite za pojedince. Ima potencijal postati središte za podatkovne usluge za koje su potrebni slobodni tokovi i povjerenje.

2.1. Sveobuhvatan, objedinjen i pojednostavnjen okvir EU-a za zaštitu podataka

Reformom EU-a uspostavlja se sveobuhvatan okvir kojim se uređuje obrada osobnih podataka u privatnom i javnom sektoru te u trgovinskom sektoru i sektoru izvršavanja zakonodavstva (Opća uredba o zaštiti podataka odnosno Direktiva o policiji).

Na temelju Opće uredbe o zaštiti podataka od svibnja 2018. postojat će jedinstven paneuropski skup pravila za razliku od 28 nacionalnih zakona koji postoje danas. Novostvorenim mehanizmom jedinstvene kontaktne točke osigurat će se da jedno tijelo za zaštitu podataka bude odgovorno za nadzor prekograničnih aktivnosti obrade podataka koje provodi poduzeće iz EU-a. Osigurat će se i dosljedno tumačenje novih pravila. Konkretno, u prekograničnim slučajevima u kojima sudjeluje nekoliko nacionalnih tijela za zaštitu podataka, donijet će se jedna odluka kako bi se osiguralo da za zajedničke probleme postoje i zajednička rješenja. Osim toga, Općom uredbom o zaštiti podataka stvaraju se ravnopravni uvjeti za poduzeća iz EU-a i strana poduzeća tako što će poduzeća sa sjedištem izvan EU-a morati primjenjivati ista pravila kao i europska poduzeća ako nude robu i usluge ili nadziru ponašanje pojedinaca u EU-u. Komercijalni subjekti iz EU-a i vanjski komercijalni subjekti imat će koristi od više razine povjerenja potrošača.

Direktivom o policiji pružaju se zajednička pravila za obradu osobnih podataka pojedinaca u kaznenim postupcima, neovisno o tome jesu li osumnjičeni, žrtve ili svjedoci, uzimajući u obzir posebnu prirodu područja policije i kaznenog pravosuđa. Usklađivanjem pravila o zaštiti podataka u sektoru izvršavanja zakonodavstva, uključujući pravila o međunarodnim prijenosima, olakšat će se prekogranična suradnja policijskih i pravosudnih tijela unutar EU-a i s međunarodnim partnerima te će se tako stvoriti uvjeti za djelotvorniju borbu protiv kriminala. To je važan doprinos Europskom programu sigurnosti⁶.

2.2. Obnovljen i raznolik skup alata za međunarodne prijenose

Zakonodavstvom EU-a o zaštiti podataka od samog je početka pruženo nekoliko mehanizama kojima se omogućuju međunarodni prijenosi podataka. Primarna je svrha tih pravila osigurati

⁶ Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija „Europski program sigurnosti”, COM(2015) 185 final, 28.4.2015.

da osobni podaci Europljana budu zaštićeni u svakom trenutku njihova prijenosa u inozemstvo. Ta su pravila tijekom godina postala primjer za reguliranje međunarodnih tokova podataka u mnogim jurisdikcijama. Iako struktura ostaje gotovo ista kao i u Direktivi iz 1995., reformom pravila o međunarodnim prijenosima razjašnjava se i pojednostavnjuje njihova upotreba te uvode novi alati za prijenose.

Na temelju prava EU-a jedan je od načina za prijenos osobnih podataka u inozemstvo na temelju Komisijine „odluke o primjerenosti” kojom se potvrđuje da zemlja izvan EU-a pruža razinu zaštite podataka koja je „bitno ekvivalentna”⁷ zaštiti u EU-u. Učinak je takve odluke omogućiti slobodan tok osobnih podataka u tu treću zemlju a da pritom izvoznik podataka ne mora pružiti dodatne zaštitne mjere ili ishoditi odobrenje. Zainteresiranim zemljama ili međunarodnim organizacijama dostupan je precizan i detaljan popis elemenata koje Komisija mora uzeti u obzir pri procjeni primjerenosti zaštite u stranom sustavu⁸. Komisija sad može donositi odluke o primjerenosti i za sektor izvršavanja zakonodavstva⁹. Nadalje, na temelju prakse iz Direktive iz 1995. reformom se izričito omogućuje utvrđivanje primjerenosti s obzirom na određeno državno područje neke treće zemlje ili određeni sektor ili industriju u trećoj zemlji (tzv. djelomična primjerenost)¹⁰.

U nedostatku odluke o primjerenosti međunarodni se prijenosi mogu provesti na temelju niza drugih alata za prijenos kojima se pružaju primjerene mjere za zaštitu podataka¹¹. Reformom se formaliziraju i proširuju mogućnosti upotrebe postojećih instrumenata poput standardnih ugovornih odredaba¹² i obvezujućih korporativnih pravila¹³. Primjerice, standardne se ugovorne odredbe sad mogu uključiti u ugovor između izvršitelja obrade u EU-u i izvršitelja obrade u zemlji izvan EU-a (tzv. model klauzula „izvršitelji”)¹⁴. Kad je riječ o obvezujućim korporativnim pravilima, koja su dosad bila ograničena na dogovore među subjektima iste grupe poduzeća, njih sad može primjenjivati grupa poduzeća koja obavljaju zajedničku

⁷ Presuda Suda Europske unije od 6. listopada 2015. u predmetu C-362/14, *Maximillian Schrems protiv Data Protection Commissioner*, točke 73., 74. i 96. Vidjeti i uvodnu izjavu (104) Opće uredbe o zaštiti podataka i uvodnu izjavu (67) Direktive o policiji koje se odnose na standard bitne ekvivalentnosti.

⁸ Vidjeti članak 45. Opće uredbe o zaštiti podataka. Kako je utvrđeno u članku 45. stavku 2. Komisija u procjeni mora uzeti u obzir, među ostalim, vladavinu prava, poštovanje ljudskih prava i temeljnih sloboda te relevantno zakonodavstvo, uključujući zakonodavstvo u području zaštite podataka, javne sigurnosti, obrane, nacionalne sigurnosti i kaznenog prava te pristupa tijela javne vlasti osobnim podacima. Njih moraju podupirati i djelotvorna i provediva prava, uključujući upravnu i sudsku zaštitu pojedinaca, te djelotvorno funkcioniranje neovisnog nadzornog tijela kako bi se osiguralo i izvršilo poštovanje pravila o zaštiti podataka. Pridržavanje pravno obvezujućih konvencija, posebno Konvencije br. 108 Vijeća Europe, te sudjelovanje u multilateralnim ili regionalnim sustavima koji se bave zaštitom podataka, isto će se tako uzeti u obzir.

⁹ Vidjeti članak 36. stavak 2. Direktive o policiji za posebne elemente procjene primjerenosti.

¹⁰ Vidjeti članak 45. stavak 1. Opće uredbe o zaštiti podataka i članak 36. stavak 1. Direktive o policiji.

¹¹ Vidjeti npr. Komunikaciju Komisije Europskom parlamentu i Vijeću o prijenosu osobnih podataka iz EU-a u Sjedinjene Američke Države u skladu s Direktivom 95/46/EZ nakon presude Suda u predmetu C-362/14 (*Schrems*), COM(2015) 566 final, 6.11.2015.

¹² Standardnim ugovornim odredbama utvrđuju se obveze u pogledu zaštite podataka za izvoznike iz EU-a i uvoznike u treću zemlju.

¹³ Obvezujuća korporativna pravila interna su pravila koja donosi multinacionalna grupa poduzeća za prijenos podataka unutar iste grupe poduzeća subjektima u zemljama koje ne pružaju primjerenu razinu zaštite. Iako su obvezujuća korporativna pravila već u upotrebi na temelju Direktive iz 1995., Općom uredbom o zaštiti podataka kodificira se i formalizira njihova uloga kao alata za prijenose.

¹⁴ Vidjeti članak 46. stavak 2. točke (c) i (d) te uvodnu izjavu (168) Opće uredbe o zaštiti podataka.

gospodarsku djelatnost, ali nisu nužno dio iste grupe poduzeća¹⁵. Reformom se smanjuje i birokracija tako što su ukinuti opći zahtjevi prethodnog obavješćivanja tijela za zaštitu podataka o prijenosima u treće zemlje ili odobrenja tijela za zaštitu podataka za taj prijenos na temelju standardnih ugovornih odredaba ili obvezujućih korporativnih pravila¹⁶. Time je EU-ov sustav međunarodnih prijenosa podataka bitno pojednostavnjen jer se postojanje takvih zahtjeva, koji se trenutačno razlikuju u državama članicama, često smatra velikom preprekom tokovima podataka, posebno u malim poduzećima¹⁷.

Osim toga, reformom su uvedeni novi instrumenti za međunarodne prijenose¹⁸. Voditelji i izvršitelji obrade uz određene će uvjete¹⁹ moći upotrebljavati odobrene kodekse ponašanja ili mehanizme certificiranja (poput pečata ili oznaka povjerljivosti) radi utvrđivanja primjerenih zaštitnih mjera. Time bi se trebao omogućiti razvoj prilagođenijih rješenja za međunarodne prijenose u kojima bi primjerice bile vidljive posebne značajke i potrebe određenog sektora ili industrije ili određenih tokova podataka. Omogućeno je i predviđanje primjerenih zaštitnih mjera za prijenose podataka među javnim tijelima na temelju međunarodnih sporazuma ili administrativnih dogovora²⁰. Naposljetku, Općom uredbom o zaštiti podataka razjašnjava se upotreba tzv. odstupanja²¹ (npr. pristanak, izvršavanje ugovora ili važni razlozi od javnog interesa) na kojima subjekti u posebnim situacijama mogu temeljiti prijenose podataka u nedostatku odluke o primjerenosti i neovisno o upotrebi nekog od prethodno navedenih instrumenata. Konkretno, Uredba sadržava novo, iako ograničeno, odstupanje koje se odnosi na prijenose koji se mogu izvršavati radi ostvarenja legitimnih interesa²² poduzeća.

Naposljetku, reformom se Komisiji daju ovlasti za razvoj mehanizama međunarodne suradnje radi lakšeg provođenja pravila o zaštiti podataka, među ostalim dogovorima o uzajamnoj pomoći²³. Time se priznaje doprinos koji bi se mogao ostvariti bližom suradnjom nadzornih tijela na međunarodnoj razini radi osiguranja djelotvornije zaštite prava pojedinaca i veće pravne sigurnosti za poduzeća.

3. MEĐUNARODNI PRIJENOSI PODATAKA U TRGOVINSKOM SEKTORU: POTICANJE TRGOVINE ZAŠTITOM PRIVATNOSTI

Poštovanje privatnosti uvjet je za stabilne, sigurne i konkurentne svjetske trgovinske tokove. Privatnost nije roba kojom se trguje²⁴. Internet i digitalizacija robe i usluga promijenili su

¹⁵ Vidjeti članak 46. stavak 2. točku (b), članak 47. i uvodnu izjavu (110) Opće uredbe o zaštiti podataka.

¹⁶ Vidjeti članak 46. stavak 2. Opće uredbe o zaštiti podataka.

¹⁷ Činjenica da zahtjevi za registraciju otežavaju trgovinu mnogim poduzećima, posebno malim i srednjim poduzećima, istaknuta je u izvješću UNCTAD-a, str. 34.

¹⁸ Vidjeti članak 46. stavak 2. točke (e) i (f) Opće uredbe o zaštiti podataka.

¹⁹ Voditelji obrade podataka izvan EU-a moći će se pridržavati kodeksa ponašanja ili mehanizma certificiranja EU-a preuzimanjem obvezujućih i provedivih obveza, putem ugovornih ili drugih pravno obvezujućih instrumenata, za primjenu mjera zaštite podataka sadržanih u tim instrumentima. Vidjeti članak 42. stavak 2. Opće uredbe o zaštiti podataka.

²⁰ Vidjeti članak 46. stavak 2. točku (a) i članak 46. stavak 3. točku (b) Opće uredbe o zaštiti podataka.

²¹ Vidjeti članak 49. Opće uredbe o zaštiti podataka.

²² Vidjeti članak 49. stavak 1. drugi podstavak.

²³ Vidjeti članak 50. Opće uredbe o zaštiti podataka.

²⁴ Vidjeti primjerice Komunikaciju Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija „Trgovina za sve – Prema odgovornijoj trgovinskoj i ulagačkoj politici”, COM(2015) 497 final, 14.10.2015., str. 7.

svjetsko gospodarstvo, a prekogranični prijenos podataka, uključujući osobne podatke, dio je svakodnevnog poslovanja europskih poduzeća svih veličina i u svim sektorima. Budući da trgovinske razmjene sve više ovise o tokovima osobnih podataka, privatnost i sigurnost tih podataka postale su glavni faktor povjerenja potrošača. Primjerice, dvije trećine Europljana izjavilo je da su zabrinuti jer nemaju nadzor nad podacima koje pružaju na internetu, dok je polovina ispitanika zabrinuta da će postati žrtve prijevare²⁵. Istodobno, europska poduzeća koja posluju u nekim trećim zemljama sve se više suočavaju s protekcionističkim ograničenjima koja se ne mogu opravdati legitimnim pitanjima zaštite privatnosti.

U digitalnom dobu promicanje visokih standarda zaštite podataka i olakšavanje međunarodne trgovine moraju stoga biti povezani. Dok u trgovinskim sporazumima zaštita osobnih podataka nije predmet rasprave²⁶, režimom EU-a o međunarodnim prijenosima podataka, kako je prethodno opisano, pružen je širok i raznolik skup alata radi omogućenja protoka podataka u različitim situacijama uz istodobno osiguranje visoke razine zaštite.

3.1. Odluke o primjerenosti

Zaključkom o primjerenosti dopušta se slobodan protok osobnih podataka iz EU-a a da pritom izvoznik podataka iz EU-a ne mora uvoditi dodatne zaštitne mjere niti podliježe dodatnim uvjetima. Zaključkom kako pravni poredak neke zemlje pruža primjerenu razinu zaštite, u odluci se priznaje da sustav te zemlje približno odgovara sustavima država članica EU-a. Posljedično će se prijenosi u dotičnu zemlju izjednačiti s prijenosima podataka unutar EU-a i tako omogućiti povlašten pristup jedinstvenom tržištu EU-a uz istodobno otvaranje komercijalnih kanala za subjekte iz EU-a. Kako je prethodno objašnjeno, za to je priznavanje nužna razina zaštite usporediva s onom (ili „bitno ekvivalentna” onoj)²⁷ koja se jamči u Uniji. To uključuje sveobuhvatnu procjenu sustava treće zemlje, uključujući njezina pravila o pristupu javnih tijela osobnim podacima u svrhu izvršavanja zakonodavstva, nacionalne sigurnosti i drugog javnog interesa.

Istodobno, kako je 2015. potvrdio Sud u presudi u predmetu Schrems, standard primjerenosti ne podrazumijeva doslovno ponavljanje pravila EU-a²⁸, nego se ispituje pruža li dotični strani sustav kao cjelina potrebnu razinu zaštite podataka sadržajem prava na privatnost i njihovom djelotvornom provedbom, izvršivošću i nadzorom. Kako je vidljivo iz dosad donesenih odluka o primjerenosti, Komisija kao primjerene može priznati razne sustave za zaštitu privatnosti s različitim pravnim tradicijama. Te se odluke odnose na zemlje koje su blisko povezane s Europskom unijom i njezinim državama članicama (Švicarska, Andora, Farski otoci, Guernsey, Jersey, Otok Man), važne trgovinske partnere (Argentina, Kanada, Izrael, Sjedinjene Američke Države) i zemlje koje imaju pionirsku ulogu u razvoju zakona o zaštiti podataka u svojoj regiji (Novi Zeland, Urugvaj).

²⁵ Posebno istraživanje Eurobarometra 431 – Zaštita podataka, lipanj 2015.

²⁶ Političke smjernice predsjednika Junckera: „Novi početak za Europu: moj program za zapošljavanje, rast, pravednost i demokratske promjene”.

²⁷ Vidjeti bilješku 7.

²⁸ Vidjeti točku 74. presude u predmetu Schrems.

Odluke o Kanadi i Sjedinjenim Američkim Državama „djelomični” su zaključci o primjerenosti. Odluka o Kanadi primjenjuje se samo na privatne subjekte koji su obuhvaćeni područjem primjene kanadskog Zakona o zaštiti osobnih podataka i elektroničkim dokumentima. Nedavno donesena odluka o europsko-američkom sustavu zaštite privatnosti²⁹ poseban je slučaj jer se, u nedostatku općeg zakonodavstva o zaštiti podataka u SAD-u³⁰, temelji na obvezama poduzeća koja sudjeluju u sustavu da primjenjuju visoke standarde zaštite podataka postavljene tim dogovorom koje su, s druge strane, provedive na temelju prava SAD-a. Nadalje, europsko-američki sustav zaštite privatnosti temelji se na posebnim izjavama i jamstvima vlade SAD-a u pogledu pristupa u svrhu nacionalne sigurnosti³¹ kojima se podupire zaključak o primjerenosti. Komisija će pomno pratiti poštovanje tih obveza te će to biti dio godišnjeg preispitivanja funkcioniranja okvira.

Posljednjih je godina sve više zemalja diljem svijeta donijelo novo zakonodavstvo u području zaštite podataka i privatnosti ili je u postupku njegova donošenja. Broj zemalja koje su donijele zakone o zaštiti podataka 2015. iznosio je 109, što je znatan porast u odnosu na 76 sredinom 2011.³² Uz to, 35 zemalja trenutačno izrađuje nacрте zakona o zaštiti podataka³³. Ti se novi ili modernizirani zakoni uglavnom temelje na osnovnom skupu zajedničkih načela, uključujući, među ostalim, priznavanje zaštite podataka kao temeljnog prava, donošenje sveobuhvatnog zakonodavstva u tom području, postojanje izvršivih prava pojedinaca na privatnost te osnivanje neovisnog nadzornog tijela. To otvara nove mogućnosti, posebice zaključcima o primjerenosti, za daljnje olakšavanje protoka podataka uz istodobno osiguranje trajno visoke razine zaštite osobnih podataka.

Na temelju prava EU-a za zaključak o primjerenosti potrebna su utvrđena pravila o zaštiti podataka usporediva s onima u EU-u³⁴. To se odnosi na materijalnu zaštitu primjenjivu na osobne podatke te relevantne mehanizme nadzora i pravne zaštite dostupne u trećoj zemlji.

Unutar okvira za zaključke o primjerenosti Komisija smatra da bi se sljedeći kriteriji trebali uzeti u obzir pri procjeni s kojim trećim zemljama treba nastaviti dijalog o primjerenosti³⁵:

- (i) opseg (stvarnih ili potencijalnih) trgovinskih odnosa EU-a s određenom trećom zemljom, uključujući postojanje sporazuma o slobodnoj trgovini ili tekućih pregovora;

²⁹ Provedbena odluka EU (2016) 1250 od 12. srpnja 2016.

³⁰ Komisija potiče SAD da nastavi nastojanja u stvaranju sveobuhvatnog sustava privatnosti i zaštite podataka kako bi se između ta dva sustava dugoročno mogla ostvariti konvergencija. Vidjeti Komunikaciju Komisije Europskom parlamentu i Vijeću „Transatlantski protok podataka: primjena jakih zaštitnih mjera radi vraćanja povjerenja”, COM(2016) 117 final, 29.2.2016.

³¹ To posebice uključuje primjenu Predsjedničkog ukaza (PPD-28) kojim se nameće niz ograničenja i zaštitnih mjera za operacije prikupljanja obavještajnih podataka te imenovanje posebnog pravobranitelja za žalbe pojedinaca iz EU-a na ta pitanja.

³² G. Greenleaf, „Global data privacy laws 2015: 109 countries, with European laws now in a minority”, (2015) 133 Privacy Laws & Business International Report, str. 14.-17.

³³ Studija UNCTAD-a, str. 8. i 42. (bilješka 4).

³⁴ U tom pogledu Komisija pri procjeni primjerenosti uzima u obzir i obveze treće zemlje koje proizlaze iz pravno obvezujućih konvencija, posebice pristupanja Konvenciji br. 108 i njezinu dodatnom Protokolu. Vidjeti članak 45. stavak 2. točku (c) te uvodnu izjavu (105) Opće uredbe o zaštiti podataka.

³⁵ Kad je riječ o zemljama u kojima postoje relevantni interesi za suradnju u području unutarnje sigurnosti i izvršavanja zakonodavstva Komisija će istražiti mogućnost posebnih zaključaka o primjerenosti na temelju Direktive o policiji, vidjeti odjeljak 4.

- (ii) opseg tokova osobnih podataka iz EU-a u kojima se odražavaju geografske i/ili kulturne veze;
- (iii) pionirska uloga treće zemlje u području privatnosti i zaštite podataka koja bi mogla poslužiti kao primjer drugim zemljama u regiji³⁶ i
- (iv) cjelokupan politički odnos s dotičnom trećom zemljom, posebice s obzirom na promicanje zajedničkih vrijednosti i ciljeva na međunarodnoj razini.

Na temelju tih razmatranja Komisija će aktivno surađivati s ključnim trgovinskim partnerima u istočnoj i jugoistočnoj Aziji, najprije s Japanom i Korejom 2017.³⁷, te, ovisno o njezinu napretku u modernizaciji zakona o zaštiti podataka, s Indijom, ali i sa zemljama Latinske Amerike, posebice zemljama Mercosura, te zemljama iz europskog susjedstva koje su izrazile interes za dobivanje zaključka o primjerenosti. Osim toga, Komisija poziva ostale treće zemlje voljne surađivati u tom području da izraze interes. Rasprave o mogućem zaključku o primjerenosti dvostrani su dijalog koji uključuje pružanje nužnih objašnjenja pravila EU-a o zaštiti podataka te otkrivanje načina za povećanje konvergencije zakona i praksi trećih zemalja.

U određenim situacijama umjesto pristupa na razini cijele zemlje moglo bi biti prikladnije iskoristiti druge opcije poput djelomične ili sektorske primjerenosti (npr. za sektor financijskih usluga ili sektor IT-a) koja se može odnositi na geografska područja ili industrije koji su važan dio gospodarstva određene treće zemlje. To će se morati razmotriti s obzirom na elemente kao što su priroda i stanje razvoja režima za zaštitu privatnosti (zaseban zakon, višestruki ili sektorski zakoni itd.), ustavna struktura treće zemlje ili posebna izloženost određenih sektora gospodarstva tokovima podataka iz EU-a.

Donošenje odluke o primjerenosti uključuje pokretanje posebnog dijaloga i blisku suradnju s dotičnom trećom zemljom. Odluke o primjerenosti „živi” su dokumenti koje Komisija treba pomno nadzirati i prilagođavati u slučaju razvoja događaja koji bi utjecao na razinu zaštite koju osigurava dotična treća zemlja³⁸. U tu će se svrhu provoditi periodično preispitivanje barem svake četiri godine kako bi se riješila novonastala pitanja i razmjenjivale najbolje prakse među bliskim partnerima³⁹. Taj dinamični pristup primjenjuje se i na postojeće odluke o primjerenosti, donesene na temelju Direktive iz 1995., koje će trebati preispitati u slučaju da više ne ispunjavaju primjenjivi standard⁴⁰. Dotične se treće zemlje stoga pozivaju da obavijeste Komisiju o svim relevantnim promjenama zakona i prakse koje su se dogodile od

³⁶ To može biti posebno važno za zemlje u razvoju i tranzicijske zemlje jer je zaštita osobnih podataka ključan element vladavine prava i važan čimbenik gospodarske konkurentnosti.

³⁷ Japan i Koreja nedavno su donijeli ili modernizirali zakonodavstvo kako bi uspostavili sveobuhvatne režime za zaštitu podataka.

³⁸ Člankom 45. stavcima 4. i 5. Opće uredbe o zaštiti podataka od Komisije se zahtijeva da kontinuirano prati razvoj događaja u trećim zemljama te joj se daje ovlast da stavi izvan snage, izmijeni ili suspendira odluku o primjerenosti ako otkrije da određena zemlja više ne osigurava primjerenu razinu zaštite.

³⁹ Članak 45. stavak 3. Opće uredbe o zaštiti podataka.

⁴⁰ Člankom 97. stavkom 2. točkom (a) Opće uredbe o zaštiti podataka od Komisije se zahtijeva i da Europskom parlamentu i Vijeću podnese izvješće o ocjeni do 2020.

donošenja odluke o primjerenosti koja se na njih odnosi. To je važno kako bi se osigurao kontinuitet tih odluka prema novim pravilima reforme⁴¹.

Pravila EU-a o zaštiti podataka ne mogu biti predmet pregovora u sporazumu o slobodnoj trgovini⁴². Dok se dijalozi o zaštiti podataka i trgovinski pregovori s trećim zemljama moraju voditi zasebno, odluka o primjerenosti, među ostalim i odluka o djelomičnoj ili sektorskoj primjerenosti, najbolje je sredstvo izgradnje uzajamnog povjerenja kojim se jamči neometani protok osobnih podataka te tako olakšavaju trgovinske razmjene koje uključuju prijenose osobnih podataka u dotičnu treću zemlju. Takve odluke stoga mogu olakšati trgovinske pregovore ili upotpuniti postojeće trgovinske sporazume te tako omogućiti stvaranje njihove bolje iskoristivosti. Istodobno, poticanjem konvergencije u razini zaštite u EU-u i u trećoj zemlji putem zaključka o primjerenosti smanjit će se rizik od pozivanja te zemlje na zaštitu osobnih podataka kao temelja za nametanje neopravdanih zahtjeva u pogledu lokalizacije ili pohrane podataka. Osim toga, kako je navedeno u Komunikaciji „Trgovina za sve”, Komisija će nastojati upotrijebiti trgovinske sporazume EU-a za uspostavu pravila za e-trgovinu i prekogranične tokove podataka te poraditi na novim oblicima digitalnog protekcionizma potpuno u skladu s pravilima EU-a o zaštiti podataka i ne dovodeći ta pravila u pitanje⁴³.

Komisija će učiniti sljedeće:

- dati prioritet raspravama o mogućim odlukama o primjerenosti s ključnim trgovinskim partnerima u istočnoj i jugoistočnoj Aziji, najprije s Japanom i Korejom 2017., ali uzimajući u obzir i druge strateške partnere poput Indije, te sa zemljama Latinske Amerike, posebice zemljama Mercosura, i zemljama iz europskog susjedstva,
- pomno pratiti funkcioniranje postojećih odluka o primjerenosti. To konkretno uključuje provedbu europsko-američkog sustava zaštite privatnosti, posebice putem mehanizma godišnjeg zajedničkog preispitivanja,
- surađivati sa zemljama koje žele donijeti čvršće zakone o zaštiti podataka, pomagati im i podupirati njihovu konvergenciju s načelima zaštite podataka u EU-u.

3.2. Alternativni mehanizmi za prijenos podataka

Pravilima EU-a o zaštiti podataka uvijek se priznavalo da nema jedinstvenog pristupa kad je riječ o međunarodnim prijenosima podataka. To se posebno odnosi na pravila koja proizlaze iz reforme. Zaključci o primjerenosti bit će dostupni samo onim trećim zemljama koje ispune

⁴¹ Kao posljedica presude u predmetu Schrems, u kojoj je utvrđeno da je Komisija prekoračila ovlasti time što je ograničila ovlasti tijela za zaštitu podataka da suspendiraju ili zabranjuju protok podataka u odluci o „sigurnoj luci”, Komisija je 16. prosinca 2016. donijela skupnu odluku o izmjeni kojom se slične odredbe u postojećim odlukama o primjerenosti brišu i zamjenjuju odredbama kojima se samo predviđaju zahtjevi za obavješćivanje među državama članicama i Komisijom u slučaju da tijelo za zaštitu podataka suspendira ili zabrani prijenose u treću zemlju. Skupnom se odlukom uvodi zahtjev da Komisija mora pratiti relevantne promjene u trećoj zemlji. Vidjeti SL L 344, 17.12.2016., str. 83.

⁴² Konkretno, zaključak o primjerenosti jednostrana je provedbena odluka Komisije u skladu s pravom EU-a o zaštiti podataka i temelji se na njegovim kriterijima.

⁴³ Vidjeti Komunikaciju „Trgovina za sve”, str. 12. (bilješka 24).

relevantne kriterije, a Općom uredbom o zaštiti podataka predviđa se raznovrstan skup mehanizama koji su dovoljno fleksibilni da se prilagode nizu različitih situacija prijenosa. Mogu se razvijati instrumenti kojima bi se uzeli u obzir posebne potrebe ili uvjeti pojedinih industrija, poslovnih modela i/ili subjekata. Mogli bi primjerice biti u obliku standardnih ugovornih odredaba usmjerenih na zahtjeve određenog sektora, npr. posebne zaštitne mjere pri obradi osjetljivih podataka u zdravstvenom sektoru, ili na zahtjeve određene vrste aktivnosti obrade koja se najčešće primjenjuje u određenim trećim zemljama, npr. usluge eksternalizacije koje se izvršavaju za europska poduzeća. To bi se moglo postići donošenjem novog skupa standardnih odredaba ili dopunom postojećih dodatnim zaštitnim mjerama koje bi mogle biti od tehničkih preko organizacijskih rješenja do rješenja koja se odnose na poslovni model⁴⁴. Posebne sektorske potrebe mogu se ispuniti obvezujućim korporativnim pravilima koja bi se primjenjivala na grupe poduzeća koja obavljaju zajedničku gospodarsku djelatnost, primjerice u turizmu. Međunarodnim prijenosima između izvršitelja obrade mogao bi pridonijeti razvoj standardnih ugovornih odredaba za izvršitelje i/ili obvezujućih korporativnih pravila za izvršitelje. Naposljetku, novim mehanizmima za prijenos poput odobrenih kodeksa ponašanja i potvrda akreditiranih trećih strana industriji se omogućuje uvođenje prilagođenih rješenja za međunarodne prijenose uz istodobno ostvarenje koristi od konkurentne prednosti koja je primjerice povezana s pečatom ili oznakom povjerljivosti. Neki od tih instrumenata mogu se razviti kao mehanizmi za pojedine prijenose ili kao dio općenitijih alata kojima se dokazuje poštovanje svih odredaba Opće uredbe o zaštiti podataka, kao u slučaju odobrenog kodeksa ponašanja.

Komisija će surađivati s industrijom, civilnim društvom i tijelima za zaštitu podataka kako bi iskoristili puni potencijal skupa alata za međunarodne prijenose iz Opće uredbe o zaštiti podataka. Otvoreni dijalog s dionicima u kontekstu provedbe reformi pomoći će pri utvrđivanju prioriteta područja djelovanja u tom pogledu. To može uključivati dovršetak rada koji je već započeo, kao što je sastavljanje standardnih ugovornih odredaba za izvršitelje⁴⁵ u suradnji s Radnom skupinom iz članka 29. (koja će 2018. biti zamijenjena Europskim odborom za zaštitu podataka). Može uključivati i razvoj novih sastavnica infrastrukture EU-a za poštovanje odredaba, primjerice tako da Komisija odredi zahtjeve i tehničke standarde za uspostavu i funkcioniranje mehanizama certificiranja, među ostalim i za aspekte povezane s međunarodnim prijenosima⁴⁶. Neke od tih mjera mogu se dopuniti radom na međunarodnoj razini, posebice s organizacijama koje su razvile slične mehanizme za prijenos. Primjerice, mogle bi se istražiti metode za promicanje konvergencije između obvezujućih korporativnih pravila na temelju prava EU-a i prekograničnih pravila o privatnosti koja su razvile države Azijsko-pacifičke gospodarske suradnje (APEC)⁴⁷ u

⁴⁴ Vidjeti članak 46. stavak 2. točke (c) i (d) te uvodnu izjavu (109) Opće uredbe o zaštiti podataka u kojima se objašnjava da su prilagodbe odobrenih modela klauzula moguće ako nisu u suprotnosti, izravno ili neizravno, s tim modelom klauzula ili ako ne dovode u pitanje temeljna prava i slobode pojedinaca.

⁴⁵ Trenutačno nisu uspostavljene standardne ugovorne odredbe za prijenos od izvršitelja iz EU-a izvršitelju izvan EU-a.

⁴⁶ Članak 43. stavci 8. i 9. Opće uredbe o zaštiti podataka.

⁴⁷ Vidjeti zajednički vodič APEC-a i EU-a iz 2014. za strukturu obvezujućih korporativnih pravila EU-a i sustav APEC-a za pravila o prekograničnoj privatnosti, u kojem se uspoređuju zahtjevi za poštovanje odredaba i certificiranje u oba sustava: http://www.apec.org/~media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.

pogledu primjenjivih standarda i postupka primjene u svakom od sustava. Time bi se trebalo pridonijeti promicanju visokih standarda zaštite podataka na svjetskoj razini uz istodobno premošćivanje razlika u pristupima zaštiti privatnosti i podataka te pomoći komercijalnim subjektima pri prelasku s jednog na drugi sustav i osmišljavanje politika koje su s njima u skladu.

Komisija će učiniti sljedeće:

- surađivati s dionicima na razvoju alternativnih mehanizama za prijenos osobnih podataka prilagođenih posebnim potrebama ili uvjetima posebnih industrija, poslovnih modela i/ili subjekata.

3.3. Međunarodna suradnja s ciljem zaštite osobnih podataka

3.3.1. Promicanje standarda zaštite podataka putem multilateralnih instrumenata i foruma

Pravni okvir EU-a za zaštitu podataka često je služio kao referentna točka trećim zemljama pri razvoju zakonodavstva u tom području. EU će i dalje aktivno voditi dijalog s međunarodnim partnerima na bilateralnoj i multilateralnoj razini kako bi poticao konvergenciju razvojem visokih i interoperabilnih standarda zaštite osobnih podataka na svjetskoj razini. To pridonosi djelotvornijoj zaštiti prava pojedinaca i istodobno smanjuje prepreke prekograničnom protoku podataka kao važan element slobodne trgovine.

Komisija posebice potiče pristupanje trećih zemalja Konvenciji br. 108 Vijeća Europe i njezinu dodatnom Protokolu⁴⁸. Ta Konvencija, koja je otvorena zemljama koje nisu članice Vijeća Europe i koju je već ratificiralo 50 zemalja, uključujući afričke i južnoameričke države⁴⁹, jedini je obvezujući multilateralni instrument u području zaštite podataka. Trenutačno je u postupku revizije i Komisija će aktivno poticati brzo donošenje moderniziranog teksta s ciljem da EU postane njezina stranka. U njoj će se odraziti načela jednaka onima utemeljenima u novim pravilima EU-a o zaštiti podataka te će se tako pridonijeti konvergenciji skupa visokih standarda zaštite podataka.

Sastanak skupine G20 2017. pružit će dodatnu priliku EU-u za rad na konvergenciji na temelju načela da su visoki standardi zaštite podataka bitna sastavnica daljnjeg razvoja globalnog informacijskog društva sposobnog promicati inovacije, rast i društveni napredak⁵⁰.

Komisija sa zadovoljstvom očekuje suradnju s važnim novim akterima, poput posebnog izvjestitelja UN-a za pravo na privatnost⁵¹, i daljnji razvoj radnih odnosa s regionalnim

⁴⁸ Konvencija Vijeća Europe od 28. siječnja 1981. za zaštitu pojedinaca u vezi s automatskom obradom osobnih podataka (ETS br. 108) i Dodatni protokol Konvencije Vijeća Europe za zaštitu pojedinaca u vezi s automatskom obradom osobnih podataka, koji se odnosi na nadzorna tijela i prekogranični protok podataka iz 2001. (ETS br. 181).

⁴⁹ Mauricijus, Senegal i Urugvaj ratificirali su Konvenciju. Osim toga, Kabo Verde, Maroko i Tunis pozvani su da pristupe.

⁵⁰ Vidjeti i Ministarsku deklaraciju OECD-a o digitalnom gospodarstvu („Ministerial Declaration on the Digital Economy: Innovation, Growth and Social Prosperity” („Cancún Declaration”), 23. lipnja 2016.

⁵¹ Vidjeti: <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>.

organizacijama kao što je APEC radi poticanja kulture poštovanja prava na privatnost i zaštitu osobnih podataka na svjetskoj razini.

Kao dio širih nastojanja za povećanje razine svijesti o privatnosti i uspostavljanje mjera za zaštitu podataka na međunarodnoj razini, 15. studenoga 2016. Europska komisija odobrila je u okviru Instrumenta za partnerstvo projekt za jačanje suradnje s partnerskim zemljama u tom području⁵². To će uključivati financiranje aktivnosti kao što su osposobljavanje i podizanje razine svijesti. S druge strane, u kontekstu provedbe reforme EU može imati koristi od razmjene najboljih praksi i iskustava drugih sustava s novim izazovima u zaštiti privatnosti i novim pravnim ili tehničkim rješenjima, uključujući u pogledu izvršenja, alata za ostvarenje poštovanja odredaba (npr. mehanizama certificiranja, procjena učinaka u pogledu privatnosti) ili zaštite određenih skupova podataka (npr. podataka o djeci).

3.3.2. Suradnja u izvršenju

Jačanje suradnje s relevantnim tijelima za izvršenje zaštite privatnosti i nadzornim tijelima trećih zemalja sve je potrebnije s obzirom na globalno poslovanje multinacionalnih poduzeća koja obrađuju goleme količine osobnih podataka u velikom broju zemalja. Problemi nepoštovanja pravila o zaštiti podataka ili krađe podataka često istodobno utječu na ljude u više od jedne jurisdikcije. U tim bi se slučajevima zaštita pojedinaca mogla učiniti djelotvornijom zajedničkim djelovanjem. Istodobno bi gospodarski subjekti mogli imati koristi od jasnijeg pravnog okruženja u kojem se alati za zajedničko tumačenje i prakse izvršenja razvijaju na svjetskoj razini.

U povezanom svijetu protoka podataka koji nema granice vrijeme je stoga za jačanje suradnje među tijelima za izvršenje⁵³. EU je spreman odigrati svoju ulogu. Kako je prethodno istaknuto, Općom uredbom o zaštiti podataka Komisiji se omogućuje razvoj mehanizama međunarodne suradnje radi lakšeg i djelotvornijeg provođenja zakonodavstva o zaštiti podataka, među ostalim dogovorima o uzajamnoj pomoći. U tom bi kontekstu trebalo istražiti mogućnost razvoja okvirnog sporazuma za suradnju među tijelima EU-a za zaštitu podataka i tijelima za izvršavanje zakonodavstva u određenim trećim zemljama, uz primjenu iskustva Komisije u drugim područjima izvršenja poput tržišnog natjecanja i zaštite potrošača.

⁵² Provedbena odluka Komisije C(2016) 7198 o odobravanju druge faze godišnjeg akcijskog programa za 2016. u pogledu Instrumenta za partnerstvo.

⁵³ Postojeće mreže uključuju Globalnu mrežu za uspostavu privatnosti pokrenutu 2010. pod okriljem OECD-a. To je neformalna mreža tijela za izvršenje zaštite privatnosti u koju su uključena tijela za zaštitu podataka iz EU-a, čija je zadaća, među ostalim, suradnja u izvršavanju zakonodavstva, razmjena najboljih praksi u rješavanju prekograničnih izazova i potpora zajedničkim inicijativama izvršenja te kampanjama za podizanje razine svijesti. Sudionicima ne stvara nove pravne obveze i ponajprije je usmjerena na olakšavanje suradnje pri izvršavanju zakona o privatnosti kojima je uređen privatni sektor. Vidjeti <https://privacyenforcement.net/>.

Komisija će učiniti sljedeće:

- promicati brzo donošenje moderniziranog teksta Konvencije br. 108 Vijeća Europe s ciljem da EU postane njezina stranka te poticati pristupanje trećih zemalja,
- iskoristiti multilateralne forume poput Ujedinjenih naroda, skupine G20 ili APEC-a za promicanje kulture poštovanja prava na zaštitu podataka na svjetskoj razini,
- razviti mehanizme međunarodne suradnje s ključnim međunarodnim partnerima kako bi se olakšalo djelotvorno izvršenje.

4. DJELOTVORNIIJA SURADNJA TIJELA ZA IZVRŠAVANJE ZAKONODAVSTVA S ČVRSTIM MJERAMA ZA ZAŠTITU PODATAKA

Razmjene osobnih podataka sastavni su dio sprečavanja, istrage i progona kaznenih djela. U međusobno povezanom svijetu u kojem kriminal ne poznaje nacionalne granice, brza razmjena osobnih podataka ključna je za uspješnu suradnju u izvršavanju zakonodavstva i djelotvoran je odgovor na kriminal. Takve se razmjene podataka moraju poduprijeti čvrstim mjerama za zaštitu podataka. Time se pridonosi i stvaranju povjerenja među tijelima za izvršavanje zakonodavstva i jačanju pravne sigurnosti pri prikupljanju i/ili razmjeni podataka.

Pravilima o međunarodnim prijenosima u Direktivi o policiji uređene su razmjene podataka između tijela za izvršavanje zakonodavstva u EU-u i tijela izvan njega te u posebnim situacijama prijenosi iz tijela za izvršavanje zakonodavstva drugim subjektima. Direktivom se uvodi mogućnost donošenja zaključaka o primjerenosti u sektoru kaznenog progona. Komisija će promicati mogućnost donošenja takvih zaključaka o primjerenosti u trećim zemljama koje ispunjavaju uvjete, posebice u onim zemljama s kojima je potrebna bliska i brza suradnja u borbi protiv kriminala i terorizma te s kojima se već razmjenjuje mnogo osobnih podataka. Na temelju će toga Komisija dati prioritet raspravama o odlukama o primjerenosti s trećim zemljama koje su ključni partneri u tom nastojanju.

S druge je strane Krovni sporazum EU-a i SAD-a o zaštiti podataka⁵⁴, sklopljen u prosincu 2016., uspješan primjer načina na koji se suradnja u području izvršavanja zakonodavstva s važnim međunarodnim partnerom može pojačati pregovorima o čvrstom skupu mjera za zaštitu podataka. Automatskom dopunom postojećih pravnih instrumenata na kojima se temelje razmjene podataka (posebni bilateralni sporazumi na razini EU-a i na razini država članica) Krovni sporazum pojedincima osigurava neposredne koristi te se njime jača suradnja u izvršavanju zakonodavstva olakšavanjem razmjene informacija. Uz to, uspostavom osnove za buduće dogovore o prijenosu podataka sa Sjedinjenim Američkim Državama Krovni se sporazumom uklanja potreba za ponovnim pregovorima o istim zaštitnim mjerama. Krovni

⁵⁴ Sporazum između EU-a i SAD-a o zaštiti osobnih podataka koji se prenose i obrađuju u svrhu sprečavanja, istrage, otkrivanja i progona kaznenih djela, uključujući terorizam, u okviru policijske i pravosudne suradnje u kaznenim stvarima: http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf („Krovni sporazum”).

sporazum prvi je bilateralni međunarodni sporazum s opsežnim popisom prava na zaštitu podataka i obvezama u skladu s pravnom stečevinom EU-a. Stoga može poslužiti kao temelj za pregovore o sličnim sporazumima s trećim zemljama ne samo u području pravosudne i policijske suradnje, nego i u drugim područjima javne provedbe (npr. politici tržišnog natjecanja, zaštiti potrošača). Time bi se obuhvatile razmjene između vlada te prijenosi podataka između privatnih poduzeća i tijela za izvršavanje zakonodavstva. Uniji bi se moglo olakšati i sklapanje sporazuma o razmjeni podataka između relevantnih agencija EU-a (posebice Europol i Eurojusta) te trećih zemalja⁵⁵. Komisija će stoga istražiti mogućnost sklapanja sličnih okvirnih sporazuma s važnim partnerima u području izvršavanja zakonodavstva.

Nadalje, Direktivom o policiji predviđa se mogućnost, na temelju strogih zaštitnih mjera i u posebnim okolnostima, da tijela za izvršavanje zakonodavstva u EU-u zatraže informacije izravno od privatnog poduzeća u trećoj zemlji te da proslijede informacije (obično ime ili IP adresu) u tom zahtjevu⁵⁶. S druge strane, Općom uredbom o zaštiti podataka posebno se uređuju slučajevi u kojima privatni subjekti u EU-u na zahtjev prenose osobne podatke tijelima za izvršavanje zakonodavstva treće zemlje: takav prijenos izvan EU-a dopušten je samo u određenim uvjetima, npr. na temelju međunarodnog sporazuma ili ako je otkrivanje podataka nužno iz važnog razloga od javnog interesa, priznatog pravom Unije ili pravom države članice⁵⁷.

Ta suradnja, koja je postala presudna za uspješnu istragu i progon kaznenih djela i terorizma, istaknuta je u zaključcima Vijeća o unapređenju kaznenog pravosuđa u kiberprostoru. Vijeće je zatražilo od Komisije da na temelju zajedničkog pristupa EU-a poduzme konkretne mjere za poboljšanje suradnje s pružateljima usluga i veću učinkovitost uzajamne pravne pomoći te predloži rješenja za problem utvrđivanja i izvršenja jurisdikcije u kiberprostoru⁵⁸. Tim su mjerama obuhvaćene razmjene između tijela za izvršavanje zakonodavstva i pružatelja usluga sa sjedištem u EU-u te razmjene s tijelima i poduzećima izvan EU-a. Komisija će izraditi nacrt mogućnosti za pristup elektroničkim dokazima u lipnju 2017. uzimajući u obzir potrebu za brзом i pouzdanom suradnjom koja počiva na čvrstim standardima zaštite podataka iz Direktive o policiji i Opće uredbe o zaštiti podataka u situacijama unutar EU-a i pri međunarodnim prijenosima.

Naposljetku, u skladu s novom pravnom osnovom za Europol Komisija će ocijeniti odredbe tih sporazuma o operativnoj suradnji između Europol i trećih strana sklopljenih na temelju Odluke Vijeća 2009/371/PUP, uključujući i odredbe o zaštiti podataka⁵⁹. Nadalje, kako je

⁵⁵ Sklapanje operativnih sporazuma s Europolom i Eurojustom bilo je ključan trenutak u dijalozima o liberalizaciji viza s određenim trećim zemljama, među ostalim u kontekstu tekućeg dijaloga s Turskom.

⁵⁶ Vidjeti članak 39. i uvodnu izjavu (73) Direktive o policiji.

⁵⁷ Vidjeti članak 48. i uvodnu izjavu (115) Opće uredbe o zaštiti podataka.

⁵⁸ Zaključci Vijeća Europske unije o unapređenju kaznenog pravosuđa u kiberprostoru, 9. lipnja 2016.: www.consilium.europa.eu/en/meetings/jha/2016/06/cyberspace--en_pdf/. Komisija je zadužena predstaviti Vijeću rezultate ostvarene u tom području do lipnja 2017., nakon izvješća o napretku koje je Vijeću podneseno u prosincu 2016.

⁵⁹ Vidjeti članak 25. stavak 4. Uredbe (EU) 2016/794 Europskog parlamenta i Vijeća od 11. svibnja 2016. o Agenciji Europske unije za suradnju tijela za izvršavanje zakonodavstva (Europol) te zamjeni i stavljanju izvan snage odluka Vijeća 2009/371/PUP, 2009/934/PUP, 2009/935/PUP, 2009/936/PUP i 2009/968/PUP,

utvrđeno u Europskom programu sigurnosti iz 2015., u budućem pristupu Unije razmjenu podataka iz evidencije s imenima putnika sa zemljama izvan EU-a uzet će se u obzir potreba za primjenom dosljednih standarda i posebnih oblika zaštite temeljnih prava. Komisija će raditi na zakonski čvrstim i održivim rješenjima za razmjenu podataka iz evidencije s imenima putnika s trećim zemljama, među ostalim razmatranjem modela sporazuma o evidenciji s imenima putnika u kojem se utvrđuju zahtjevi koje treće zemlje trebaju ispuniti da bi primale podatke iz evidencije s imenima putnika od EU-a. Sve buduće politike u tom području ovisit će, međutim, posebno o predstojećem mišljenju Suda Europske unije o predviđenom sporazumu EU-a i Kanade o evidenciji podataka o putnicima⁶⁰.

DJELOTVORNIJA SURADNJA TIJELA ZA IZVRŠAVANJE ZAKONODAVSTVA S ČVRSTIM MJERAMA ZA ZAŠTITU PODATAKA

Komisija će učiniti sljedeće:

- na temelju Direktive o policiji promicati mogućnost donošenja odluka o primjerenosti za treće zemlje koje ispunjavaju uvjete,
- promicati pregovore o sporazumima u području izvršavanja zakonodavstva s važnim međunarodnim partnerima prema modelu Krovnog sporazuma sa SAD-om,
- nastaviti rad na unapređenju kaznenog pravosuđa u kiberprostoru na temelju zaključaka Vijeća kako bi se olakšala prekogranična razmjena e-dokaza u skladu s pravilima o zaštiti podataka.

5. ZAKLJUČAK

Zaštita i razmjena osobnih podataka nisu međusobno isključive. Čvrstim sustavom za zaštitu podataka olakšavaju se tokovi podataka jer se stvara povjerenje potrošača u poduzeća kojima je stalo do toga kako obrađuju osobne podatke klijenata. Visoki su standardi zaštite podataka stoga postali prednost u globalnom digitalnom gospodarstvu. Isto vrijedi i za suradnju u području izvršavanja zakonodavstva: mjere za zaštitu privatnosti sastavni su dio djelotvorne i brze razmjene informacija u borbi protiv kriminala koja se temelji na uzajamnom povjerenju i pravnoj sigurnosti.

Nakon završetka reforme pravila o zaštiti podataka EU bi trebao proaktivno surađivati s trećim zemljama u tom području. Trebao bi nastojati ostvariti veću uzlaznu konvergenciju načela zaštite podataka na međunarodnoj razini, bilateralno i multilateralno. To je u interesu i u korist građana i poduzeća. Novim zakonodavnim okvirom za zaštitu podataka EU je dobio nužne i prikladne alate za postizanje tih ciljeva. Na temelju strateškog pristupa iz ove

SL L 135, 24.5.2016. (str. 53.-114.). Komisija mora podnijeti izvješće o ocjeni do 14. lipnja 2021. u pogledu Europolovih sporazuma o suradnji sklopljenih prije 1. svibnja 2017.

⁶⁰ Mišljenje Suda o nacrtu sporazuma između EU-a i Kanade o evidenciji podataka o putnicima iz 2014.; zahtjev za donošenje mišljenja Suda je uputio Europski parlament (Mišljenje 1/15). Od Suda je zatraženo da ocijeni usklađenost nacrta sporazuma s Poveljom EU-a o temeljnim pravima.

Komunikacije Komisija će aktivno surađivati s ključnim trećim zemljama u istraživanju mogućnosti donošenja zaključaka o primjerenosti, najprije s Japanom i Korejom 2017., s ciljem poticanja regulatorne konvergencije standarda EU-a i olakšavanja trgovinskih odnosa. Istodobno će EU u potpunosti iskoristiti niz alternativnih alata za prijenos radi zaštite prava na zaštitu podataka i potpore gospodarskim subjektima kad se podaci prenose u zemlje čije nacionalno pravo ne osigurava primjerenu razinu zaštite podataka. Takvi alati trebali bi se upotrebljavati i za daljnje pojednostavnjenje suradnje između nadzornih tijela i tijela za izvršavanje zakonodavstva u EU-u te njihovih međunarodnih partnera. Komisija će osigurati usklađenost unutarnje i vanjske dimenzije politike EU-a o zaštiti podataka te promicati čvrstu zaštitu podataka na međunarodnoj razini kako bi poboljšala suradnju u području izvršavanja zakonodavstva, pridonijela slobodnoj trgovini i razvila visoke standarde zaštite osobnih podataka na svjetskoj razini.