Europski okvir zaštite osobnih podataka: aktualnosti

Doc. dr. sc. Nina Gumzej, Pravni fakultet Sveučilišta u Zagrebu

1. Uvod

Tijekom travnja 2016. godine konačno je, nakon četiri teške godine zakonodavnog postupka usuglašen tekst novog općeg okvira zaštite osobnih podataka EU-a: *Uredbe 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, dalje u tekstu i kao: Uredba).[1]

Uredba je objavljena u Službenom listu Europske unije 4. svibnja te je stupila na snagu 25. svibnja 2016. godine. Rok njezine primjene odgođen je za dvije godine, što znači da će se primjenjivati u državama članicama od 25. svibnja 2018. godine.[2] Tada će Uredba zamijeniti trenutno važeću *Direktivu 95/46/EZ o zaštiti pojedinaca u pogledu obrade osobnih podataka i slobodnog kolanja takvih podataka* (dalje u tekstu: Direktiva ZOP).[3]

Radi se o opsežnom i kompleksnom pravnom instrumentu koji sadrži 99 članaka s ukupno 173 dodatna pojašnjenja, odnosno razloga. Novim pravilima nastoji se u što je većoj mjeri ujednačiti europski domaći okvir zaštite osobnih podataka i na taj način osigurati što višu razinu pravne sigurnosti u aktivnostima obrade osobnih podataka i što više ujednačenu te provedivu zaštitu prava potrošača u EU-u čiji su osobni podaci predmet tih obrada. Ispunjenje navedenih ciljeva očituje se i kroz postroženu odgovornost onih koji obrađuju osobne podatke

[1] Službeni list Europske unije (dalje: SL) L 119, 04.5.2016, str. 1–88.
[2] Članak 99. Uredbe.
[3] SL, L 281, 23.11.1995., str. 31-50.

ispitanika u EU-u, osnažene ovlasti nadzornih tijela za zaštitu osobnih podataka te novouvedene postupke namijenjene jačanju njihove međusobne suradnje i osiguravanju dosljedne primjene Uredbe u EU-u. Nova pravila zahvaćaju široki krug aktera na globalnoj razini, budući da se osim na obradu osobnih podataka u okviru aktivnosti poslovnog nastana voditelja obrade ili izvršitelja obrade u EU-u ona primjenjuju i kada isti nema poslovni nastan u EU-u i to u slučaju aktivnosti obrade osobnih podataka ispitanika u EU-u koje su povezane bilo s ponudom robe ili usluga tim ispitanicima, bilo s praćenjem njihova ponašanja unutar EU-a. Glede potonjeg se pojašnjava kako određivanje toga može li se aktivnost obrade smatrati praćenjem ponašanja ispitanika traži utvrđivanje toga prati li se pojedinca na internetu među ostalim mogućom naknadnom upotrebom tehnika obrade osobnih podataka koje se sastoje od izrade profila pojedinca, osobito radi donošenja odluka koje se odnose na njega ili radi analize ili predviđanja njegovih osobnih sklonosti, ponašanja i stavova.[4]

Potreba što učinkovitije prilagodbe europskog pravnog okvira zaštite osobnih podataka izazovima novijih tehnologija i uvjetima digitalne ekonomije koje obilježavaju sve opsežniji i kompleksniji postupci obrade podataka pojedinaca, pogotovo u umreženom globaliziranom okruženju, predstavlja bitan povod za donošenje Uredbe. Osobito u spomenutom okruženju neometani je međunarodni prijenos osobnih podataka preduvjet cilju daljnjeg jačanja međunarodne trgovine i suradnje a koji, pokazuje se, dugoročno nije održiv bez istovremenog jačanja povjerenja potrošača u EU-u, odnosno bez istovremenog osiguravanja primjerene i provedive zaštite njihovih prava (u skladu s novim pravilima).

Ovo istraživanje odnosi se na pitanja povezana s realizacijom potonje navedenih ciljeva nove Uredbe, kako slijedi. U prvom dijelu istraživanja usredotočit ću se na kvalifikaciju pojma osobnog podatka gledano u odnosu na digitalne identifikatore. Radi se ovdje o pitanju u

[4] Članak 3. i razlog 24. Uredbe.

pogledu koje dulje vrijeme nije bilo konzistentnog tumačenja i prakse kako od strane nadzornih tijela tako i sudova u EU-u, a pogotovo sagleda li se situacija u Hrvatskoj gdje je prijeko potreban rad na osvješćivanju struke i javnosti općenito uz potrebna tumačenja i stvaranje prakse. To je pitanje potrebno analizirati na prvome mjestu kroz tumačenje *acquis*-a koji je danas u primjeni. Kada je riječ o obvezujućem tumačenju Direktive ZOP, koja je implementirana u nacionalnom zakonodavnom okviru država članica pa tako i u našem Zakonu o zaštiti osobnih podataka, ovdje je bitna praksa Suda Europske unije koji je nedavno na tu temu donio već drugu važnu presudu. Daljnja razrada ove teme produbit će se kroz analizu pojma osobnog podatka prema novoj Uredbi.

Proteklih je par godina osobito u poslovnoj zajednici i kod potrošača u EU-u obilježeno svojevrsnim osjećajem nesigurnosti u pogledu međunarodnih prijenosa osobnih podataka izvan EU-a/EGP-a u treće zemlje. Takvi prijenosi danas su neizbježni i kontinuirano se odvijaju, osobito sagleda li se korištenje interneta. Drugi dio istraživanja usredotočit će se na detaljnu analizu novih pravila Uredbe koja imaju za cilj uspostaviti održiva rješenja za međunarodne prijenose izvan EU-a/EGP-a uz jamstva primjerene i provedive zaštite prava ispitanika. Tom ispitivanju pridružit ću i činjenicu nedavno uspostavljenog novog europsko-američkog sustava zaštite privatnosti. Uz pregled rezultata ranijeg istraživanja o utjecaju presude Suda Unije kojom je ukinuta Odluka Komisije o primjerenosti zaštite načela ranijeg sustava „sigurne luke“ (engl. *Safe Harbour*)[5], na održivost i drugih mehanizama prijenosa prema *acquis*-u, na kraju rada daje se i opći pregled aktualnih postupaka i inicijativa pokrenutih u smjeru njihove

[5] C-362/14, Maximillian Schrems protiv Data Protection Commissioner, EU:C:2015:650. Presudom je ukinuta Odluka Komisije 2000/520/EZ od 26. srpnja 2000. sukladno s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o primjerenosti zaštite koju pružaju načela privatnosti „sigurne luke” i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a (priopćena pod brojem dokumenta C(2000) 2441), SL L 215/7, 25.8.2000. – posebno izdanje na hrvatskom jeziku: 16/Sv.3, str. 9–49; Ispravak Odluke Komisije 2000/520/EZ od 26. srpnja 2000. sukladno s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o primjerenosti zaštite koju pružaju načela privatnosti „sigurne luke” i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a (SL L 215 od 25.8.2000), SL L 115, 25.4.2001, str. 14.

revizije, odnosno osporavanja njihove valjanosti.

2. Digitalni identifikatori i pojam osobnog podatka

U *online* okruženju postoje informacije koje se smatraju dijelom digitalnog identiteta umreženog pojedinca, te postoji mogućnost da one pod određenim uvjetima predstavljaju njihove osobne podatke. Primjer su takvih informacija IP adrese kao jedinstvene identifikacijske oznake računala i drugih uređaja spojenih na internetu kojima se koriste pojedinci. Europski nadzornik zaštite osobnih podataka i radna skupina članka 29. već dulji niz godina zauzimaju stav kako IP adrese u velikom dijelu slučajeva jesu osobni podaci prema Direktivi ZOP.[6]

Davatelji usluga pristupa internetu dodjeljuju IP adrese korisnicima svojih usluga i o tome vode evidenciju. IP adresa može biti statička ili dinamička. U pogledu statičke IP adrese zauzet je stav da ona zbog svoje nepromjenjivosti gotovo uvijek predstavlja osobni podatak.[7] Dinamička IP adresa je promjenjiva, odnosno ona se mijenja svaki puta kada se korisnik spoji na internet, a kada mu se dodjeljuje nova adresa. U online uvjetima pretežito se koriste dinamičke IP adrese, no to ne znači istovremeno da u pravnom smislu ne postoji mogućnost utvrđivanja identiteta pojedinca na temelju takve adrese. U tom smislu, na primjer, radna skupina članka

[6] Vidi npr. Hustinx, Peter. Protection of personal data on-line: the issue of IP addresses, 15. travnja 2009., dostupno na: http://www.edps.europa.eu/; Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, 20. 6. 2007, str. 16-17.

[7] Schnabel potkrepljuje tezu da su statičke IP adrese u pravilu osobni podaci i kada se radi o davateljima drugih internetskih usluga (pored davatelja usluga pristupa internetu) primjerom u kojem je korisnik internetske usluge jednom dostavio davatelju ove usluge svoje podatke (npr. ispunjavanjem online narudžbe). Ti su njegovi osobni podaci od tada pa nadalje povezani s njegovom statičkom IP adresom. Prema tome, ukoliko ovaj korisnik neki idući put posjeti istu web-stranicu i davatelju te internetske usluge i ne da ponovno svoje osobne podatke, iako bi možda pretpostavio da taj put koristi uslugu anonimno, on će svejedno biti prepoznat po svojoj statičkoj IP adresi (i vezi između te adrese s osobnim podacima koje je davatelju usluge dao barem jednom ranijom prilikom). Schnabel, Christoph. Privacy and Data Protection in EC Telecommunications Law, u: Koenig, Christian *et al*. EC Competition and Telecommunications Law. 2. izdanje, Alphen aan den Rijn: Kluwer Law International, International Competition Law Series, vol. 6., 2009, str. 532.

29. ukazuje na davatelje usluge pristupa internetu, koji mogu odrediti identitet korisnika svoje usluge i prema dinamičkoj IP adresi, jer vode evidenciju njihovih ugovornih podataka te bilježe između ostalog datum i vrijeme njihovog pristupa internetu kao i pritom dodjeljivane IP adrese.[8]

Za davatelje drugih internetskih usluga relativno je uobičajeno da prikupljaju i dalje obrađuju podatke u vezi s pristupom i korištenjem njihovog web-mjesta, a ti podaci mogu uključivati IP adrese posjetitelja, odnosno korisnika. Primjer prakse koja u ovome smislu naglašava zaštitu privatnosti korisnika bila bi usluga internetskog pretraživača u okviru čijeg se pružanja ne čuvaju IP adrese korisnika te usluge (npr. *Ixquick* kojem je nedavno potvrđen europski žig privatnosti - *European Privacy Seal*, a koji mu je izvorno dodijeljen 2008. godine).[9]

U pregledu prakse pojedinih davatelja usluga u *online* okruženju, koja bi uključivala njihovo prikupljanje i daljnju obradu korisničkih podataka koji se smatraju ili mogu smatrati osobnim podacima, radna je skupina članka 29. nastojala pronaći odgovore na pitanja postoje li i ako da, u kojem opsegu postoje u tom smislu obveze i odgovornosti davatelja ovih usluga, poglavito u pogledu zaštite prava korisnika usluga u svojstvu ispitanika. Ona je između ostalog detaljno analizirala pitanja primjene Direktive ZOP u kontekstu pružanja usluga internetskog pretraživanja, *online* društvenih mreža i *online* bihevioralnog oglašavanja, uključujući obveze i odgovornosti prvenstveno davatelja ovih usluga za provedbu zaštite osobnih podataka ispitanika.[10] Važno preliminarno pitanje u tom je pogledu postojanje obveze davatelja internetskih usluga (na primjer, davatelja usluga internetskog pretraživanja) na obradu IP adresa u skladu s propisima o zaštiti osobnih podataka i onda kada ti davatelji, pored IP adrese

[8] Working Document Privacy on the Internet - An integrated EU Approach to On-line Data Protection, 5063/00/EN/FINAL, WP 37, 21. studenog 2000, str. 11 i 21.

[9] European Privacy Seal, EuroPriSe: Privacy-friendly Internet search with Ixquick and Startpage reaffirmed, 20.7.2015, Bonn, https://www.ixquick.com/eng/press/europrise-reaffirmed.html; https://www.european-privacy-seal.eu/EPS-en/Ixquick-Startpage/.

[10] Vidi osobito sljedeća mišljenja radne skupine: Opinion 1/2008 on data protection issues related to search engines, 00737/EN, WP 148, 4. travnja 2008 i Opinion 2/2010 on online behavioural advertising, 00909/10/EN, WP 171, 22. lipnja 2010.

koju bilježe, ne raspolažu dodatnim podacima na temelju kojih bi mogli identificirati korisnika.[11]

Zaključak je da se i u takvim slučajevima korisnika može identificirati (uz pomoć primjene razloga Direktive ZOP) i to uz pomoć trećih strana. Naime, prema razlogu 26 Direktive ZOP radit će se o osobnom podatku ako je identifikacija moguća korištenjem bilo kojeg sredstva kojeg bi voditelj zbirke osobnih podataka ili neka druga osoba razumno, tj. opravdano mogla koristiti. Tako je prema IP adresi kojom raspolažu ovlaštene treće osobe u propisanim slučajevima moguće zatražiti identifikaciju korisnika od davatelja usluge internet pristupa koji je korisniku dodijelio predmetnu IP adresu.[12] Ovdje se kao primjer ukazuje na praksu u području zaštite prava intelektualnog vlasništva, prema kojoj nositelji ovih prava (u pravilu treće specijalizirane tvrtke koje nositelji prava angažiraju) „hvataju" IP adrese na internetu za koje smatraju da su povezane s radnjama neovlaštene razmjene odnosno korištenja njihovih zaštićenih djela. Međutim, nositelji prava ne raspolažu podacima na temelju kojih bi mogli utvrditi identitet osobe kojima su ove IP adrese dodijeljene (ime i prezime). Oni će se radi toga trebati obratiti davatelju usluge internet pristupa i to bilo izravno, bilo putem ovlaštenih tijela za progon i sudova. Valja skrenuti pažnju i na stav da bi u opisanim slučajevima nositelji prava u svojstvu voditelja zbirki ovih podataka, koji utvrđuju način i svrhu obrade IP adresa koje prikupljaju (prvenstveno kao dokaz radi sankcioniranja moguće povrede njihovih prava) trebali već kod njihova prikupljanja predvidjeti postojanje mogućnosti identifikacije osoba na njihovu temelju.

[11] Ohm daje za primjer osobne identifikacijske brojeve koji dođu u ruke trećih osoba, a koje ne mogu temeljem podataka kojima same raspolažu doznati identitet osoba kojima ovi brojevi pripadaju. U tom slučaju smatra da se ne može tvrditi da onda kada se ovi brojevi nalaze u njihovim rukama, te osobe zapravo ne drže „osobne podatke" (samo zašto što jedino nadležno državno tijelo može nedvojbeno povezati broj s osobom). Ohm, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review, 57, 2010, 6, str. 1701-1777., dostupno na: http://uclalawreview.org/pdf/57-6-3.pdf, str. 1773-1774.

[12] Opinion 1/2008 on data protection issues related to search engines, 00737/EN, WP 148, 4. travnja 2008, str. 8.

Osim toga vrlo je važan element i svrha koja se želi postići namjeravanom obradom IP adresa, jer njihovo prikupljanje zapravo nema smisla ne poduzima li se s ciljem naknadne identifikacije korisnika na njihovu temelju (naloži li sud takvu obvezu davatelju usluge internet pristupa, na primjer).[13]

Svakako, postoje okolnosti i kada se najčešće neće moći utvrditi identitet korisnika IP adrese (kao što je to, na primjer, neregistrirani korisnik internet kafića). Ipak, uzme li se za primjer obrada IP adresa od strane davatelja internetskih usluga, radna skupina članka 29. napominje da ti davatelji najvjerojatnije neće moći unaprijed sa sigurnošću utvrditi radi li se o IP adresi na temelju koje neće ili hoće biti moguća identifikacija korisnika. Zaključuje, stoga, ukoliko pojedini davatelj internetske usluge nije sasvim siguran da se u pojedinom slučaju radi o IP adresi na temelju koje neće biti omogućena identifikacija korisnika, on bi trebao *za svaki slučaj* sve IP adrese pravno tretirati kao osobne podatke.[14]

Sud Europske unije u svojim je presudama do danas u osnovi potvrdio srž gore navedenih (neobvezujućih) tumačenja te dao dugo očekivano pravno obvezujuće tumačenje pojma osobnog podatka u vezi s digitalnim identifikatorima, konkretno IP adresom, sukladno Direktivi ZOP. Na prvome mjestu izdvajam presudu Suda u predmetu C-70/10 (*Scarlet Extended SA protiv SABAM)* u kojoj je ovaj Sud utvrdio da se IP adrese korisnika usluge pristupa internetu trebaju smatrati osobnim podacima *u odnosu na davatelje usluge pristupa internetu*. To stoga što davatelji tih usluga izdaju IP adrese kod spajanja na internet te vode bazu podataka korisnika svojih usluga s podacima o izdanim IP adresama, kao i s njihovim identifikacijskim podacima kao što su ime, prezime i adresa.[15]

[13] Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, 20. 6. 2007, str. 17.
[14] Ibid.
[15] C-70/10, Scarlet Extended SA protiv SABAM, EU:C:2011:771, t. 51.

Nedavno je ovaj Sud donio drugu važnu presudu po pitanju pravnog utvrđenja pojma osobnog podatka prema Direktivi ZOP, koja se odnosi na dinamičke IP adrese koje prikupljaju, odnosno pohranjuju davatelji drugih internetskih usluga. Naime, presudom u predmetu *C-582/14 (Patrick Breyer protiv Savezne Republike Njemačke*)[16] dana 19. listopada 2016. godine taj je Sud protumačio pojam osobnog podatka prema Direktivi ZOP u odnosu na dinamičku IP adresu koje pohranjuje davatelj usluga internetskih medija. Radi se o davatelju internetske usluge koja nije usluga pristupa internetu i koji sam ne raspolaže dodatnim informacijama na temelju kojih je moguće identificirati pojedinca. Sud je utvrdio da okolnost da sam davatelj usluge ne raspolaže dodatnim informacijama uz pomoć kojih je moguća identifikacija osobe ne isključuje *per se* mogućnost da se dinamička IP adresa o kojoj je riječ za tog davatelja usluga pravno ne smatra osobnim podatkom u smislu Direktive ZOP.

Prilikom tumačenja pojma osobnog podatka prema Direktivi ZOP Sud je koristio tumačenje *neizravne identifikacije* pojedinca, utvrdivši na prvome mjestu da korištenje pojma „neizravno" od strane zakonodavca Unije ima za cilj istaknuti da za kvalifikaciju informacije kao osobnog podatka nije potrebno da ta informacija sama po sebi omogućuje identifikaciju osobe o kojoj je riječ. Potom je tumačio mogućnost neizravne identifikacije pojedinca u skladu s razlogom 26 Direktive ZOP, prema kojem će se raditi o osobnom podatku *ako je identifikacija moguća korištenjem bilo kojeg sredstva kojeg bi voditelj zbirke ili neka druga osoba razumno, tj. opravdano mogla koristiti*. Navedeno neće prema Sudu biti slučaj ako je identifikacija osobe o kojoj je riječ zabranjena zakonom ili ako je ona neostvariva u praksi, na primjer ukoliko bi

[16] C-582/14, Patrick Breyer protiv Savezne Republike Njemačke, EU:C:2016:779.

zahtijevala nerazmjerne napore u pogledu vremena, troškova i rada, tako da se rizik identifikacije u stvarnosti čini neznatnim.

U konkretnom primjeru Sud je utvrdio, međutim, da postoje pravni putevi koji omogućuju davatelju usluge internetskih medija da se obrati, *osobito u slučaju kibernetskih napada*, nadležnom tijelu kako bi ono poduzelo korake za identifikaciju pojedinca, odnosno za dobivanje tih informacija od davatelja usluge pristupa internetu i za pokretanje kaznenog postupka. Sukladno tome utvrdio je kako davatelj usluga internetskih medija raspolaže sredstvima koja se mogu opravdano koristiti za identifikaciju pojedinca na temelju pohranjenih IP adresa uz pomoć drugih osoba, konkretno nadležnog tijela i davatelja usluge pristupa internetu.

Prema tome, relevantnu odredbu Direktive ZOP o pojmu osobnog podatka (članak 2, točka a) valja tumačiti na način da dinamička IP adresa koju pohranjuje davatelj usluga informatičkih medija kod posjeta njegovim internetskim stranicama predstavlja u odnosu na tog davatelja usluge osobni podatak, ukoliko isti raspolaže pravnim sredstvima koji mu omogućuju identifikaciju pojedinca uz pomoć dodatnih informacija, a kojima raspolaže davatelj usluge pristupa interneta tog pojedinca.

Kada je riječ o pojmu osobnog podatka prema novoj Uredbi, sama definicija ne odstupa značajno od one utvrđene Direktivom ZOP. Naime, osobni podaci svi su podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi (ispitanik). Nešto bitnije izmjene u odnosu na Direktivu ZOP predstavljaju novo uneseni primjeri identifikatora na temelju kojih je moguće identificirati pojedinca. Naime, pojedinac čiji se identitet može utvrditi je osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, *podaci o lokaciji, mrežni identifikator* ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili

socijalni identitet tog pojedinca.[17] Kada je riječ o dodatnim pojašnjenjima, a koja su kako sam pokazala imala značajnu ulogu kod tumačenja pojma osobnog podatka prema ranije spomenutoj presudi Suda Unije, Uredba u tom pogledu slijedi pristup Direktive ZOP. Tako se i u Uredbi utvrđuje u dodatnim pojašnjenjima (ali ne i u njezinoj operativnoj odredbi tj. članku) da se kod određivanja toga može li se identitet pojedinca utvrditi trebaju uzeti u obzir *sva sredstva radi izravnog ili neizravnog utvrđivanja identiteta za koja je po svemu sudeći izgledno da ih voditelj obrade ili bilo koja druga osoba može upotrijebiti*. Kako bi se utvrdilo je li po svemu sudeći izgledno da se koriste sredstva za utvrđivanje identiteta pojedinca, trebalo bi uzeti u obzir sve objektivne čimbenike, kao što su *troškovi i vrijeme potrebno za utvrđivanje identiteta, uzimajući u obzir i dostupnu tehnologiju u vrijeme obrade i tehnološki razvoj*.[18] Navedeno se primjenjuje i u digitalnom okruženju u kojem pojedinci mogu biti pridruženi mrežnim identifikatorima koje pružaju njihovi uređaji, aplikacije, alati i protokoli (npr. IP adrese, identifikatori kolačića, oznake za radiofrekvencijsku identifikaciju). Tako mogu ostati tragovi koji se, posebno u kombinaciji s jedinstvenim identifikatorima i drugim informacijama koje primaju poslužitelji, mogu upotrijebiti za izradu profila fizičkih osoba i njihovu identifikaciju.[19]

3. Međunarodni prijenos osobnih podataka u treće zemlje ili organizacije: rješenja nove Uredbe

3.1. Odluka Komisije o primjerenosti zaštite

[17] Članak 4, točka 1. Uredbe.
[18] Razlog 26. Uredbe.
[19] Razlog 30. Uredbe.

Osnovno načelo prijenosa ostaje prema Uredbi isto kao i prema Direktivi ZOP, jer se kada je riječ o izvozu osobnih podataka izvan EU-a/EGP-a prijenos osobnih podataka trećoj zemlji ili međunarodnoj organizaciji dopušta na temelju odluke Komisije o tome da dotična treća zemlja, odnosno međunarodna organizacija osigurava *primjerenu razinu zaštite*. Međutim, za razliku od Direktive ZOP odluka Komisija o primjerenosti zaštite se prema Uredbi može odnositi ne samo na treću zemlju, *već i na područje ili jedan ili više određenih sektora unutar treće zemlje, odnosno na međunarodnu organizaciju*.

Kriteriji koji se osobito uzimaju u obzir kod ocjene o primjerenoj razini zaštite prema Uredbi jesu:

(a) vladavina prava, poštovanje ljudskih prava i temeljnih sloboda, relevantan zakonodavni okvir (opći i sektorski zakoni, što uključuje zakone o javnoj sigurnosti, obrani, nacionalnoj sigurnosti, kaznenom pravu i pristupu tijela javne vlasti osobnim podacima) te njegova provedba, pravila o zaštiti podataka, pravila struke i mjere sigurnosti (uključujući pravila za daljnji prijenos osobnih podataka još jednoj trećoj zemlji ili međunarodnoj organizaciji, koja se poštuju u toj trećoj zemlji ili međunarodnoj organizaciji), sudska praksa te postojanje djelotvornih i provedivih prava ispitanika te učinkovite upravne i sudske zaštite ispitanika čiji se osobni podaci prenose;

(b) postojanje i djelotvorno funkcioniranje jednog neovisnog nadzornog tijela ili više njih u trećoj zemlji, ili tijela kojem podliježe međunarodna organizacija, s odgovornošću osiguravanja i provođenja poštovanja pravila o zaštiti podataka, što uključuje primjerene provedbene ovlasti za pomoć ispitanicima i savjetovanje ispitanika u ostvarivanju njihovih prava te za suradnju s nadzornim tijelima država članica; i

(c) međunarodne obveze koje je dotična treća zemlja ili međunarodna organizacija preuzela, ili druge obveze koje proizlaze iz pravno obvezujućih konvencija ili instrumenata, kao i iz njezina sudjelovanja u multilateralnim ili regionalnim sustavima, osobito u vezi sa zaštitom osobnih podataka (posebno bi trebalo uzeti u obzir pristupanje treće zemlje *Konvenciji Vijeća Europe za zaštitu osoba glede automatizirane obrade*

osobnih podataka i *Dodatnom protokolu*).

U odluci odnosno provedbenom aktu o primjerenoj razini zaštite Komisija precizira i teritorijalnu, odnosno sektorsku primjenu iste, te se mora predvidjeti mehanizam za periodično preispitivanje odluke *najmanje svake četiri godine*, kojim će se uzeti u obzir svi relevantni događaji u trećoj zemlji ili međunarodnoj organizaciji o kojoj je riječ.

Komisija je dužna kontinuirano pratiti razvoj događaja u trećim zemljama i međunarodnim organizacijama koji bi mogli utjecati na funkcioniranje odluka o primjerenosti zaštite prema Uredbi, ali i već donesenih odluka donesenih na temelju Direktive ZOP[20]. Novim odlukama o primjerenosti zaštite Komisija može i *staviti izvan snage, izmijeniti ili suspendirati* ranije svoje odluke (bez retroaktivnog učinka).[21]

[20] Postojeće odluke Komisije prema Direktivi ZOP jesu, kako slijedi: **Andora**: Odluka Komisije od 19. listopada 2010. sukladno Direktivi 95/46/EZ Europskog parlamenta i Vijeća o odgovarajućoj zaštiti osobnih podataka u Andori (priopćena pod brojem dokumenta C(2010) 7084), SL L 277/27, 21.10.2010. - posebno izdanje na hrvatskom jeziku: 13/Sv.59, str. 158–160; **Argentina** - Odluka Komisije od 30. lipnja 2003. sukladno Direktivi 95/46/EZ Europskog parlamenta i Vijeća o odgovarajućoj zaštiti osobnih podataka u Argentini), SL L 168/19, 5.7.2003. - posebno izdanje na hrvatskom jeziku: 13/Sv.58, str. 57–60; **Farski otoci** - Odluka Komisije od 5. ožujka 2010. sukladno Direktivi 95/46/EZ Europskog parlamenta i Vijeća o odgovarajućoj zaštiti osobnih podataka prema zakonu Farskih otoka o obradi osobnih podataka, SL L 58, 9.3.2010, str. 17–19; **Guernsey** - Odluka Komisije od 21. studenoga 2003. o odgovarajućoj zaštiti osobnih podataka u Guernseyju, SL L 308/27, 25.11.2003. - posebno izdanje na hrvatskom jeziku: 16/Sv.3, str. 50–51; **Otok Man** - Odluka Komisije od 28. travnja 2004. o odgovarajućoj zaštiti osobnih podataka na Otoku Manu, SL 151/51, 30.4.2004. - posebno izdanje na hrvatskom jeziku: 13/Sv. 58, str. 79-80; **Istočna Republika Urugvaj** - Provedbena odluka Komisije od 21. kolovoza 2012. sukladno Direktivi 95/46/EZ Europskog parlamenta i Vijeća o odgovarajućoj zaštiti osobnih podataka u Istočnoj Republici Urugvaj u odnosu na automatiziranu obradu osobnih podataka, SL L 227, 23.8.2012, str. 11–14; **Izrael** - Odluka Komisije od 31. siječnja 2011. sukladno Direktivi 95/46/EZ Europskog parlamenta i Vijeća o odgovarajućoj zaštiti osobnih podataka u Državi Izrael s obzirom na automatiziranu obradu osobnih podataka, SL L 27/39, 1.2.2011. - posebno izdanje na hrvatskom jeziku: 16/Sv. 2, str. 240-243; **Jerseya**- Odluka Komisije od 8. svibnja 2008. u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o odgovarajućoj zaštiti osobnih podataka u Jerseyju, SL L 138/21, 28.5.2008. - posebno izdanje na hrvatskom jeziku: 13/Sv. 055, str. 173-175; **Kanada (komercijalne organizacije)** - Odluka Komisije od 20. prosinca 2001. u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o odgovarajućoj zaštiti osobnih podataka propisanoj u Zakonu o zaštiti osobnih podataka i elektroničkih dokumenata Kanade, SL L 2/13, 4.1.2002. - posebno izdanje na hrvatskom jeziku: 13/Sv. 57., str. 171-174; **Novi Zeland** - Provedbena odluka Komisije od 19. prosinca 2012. u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o odgovarajućoj zaštiti osobnih podataka koja postoji u Novom Zelandu, SL L 28/12, 30.1.2013. - posebno izdanje na hrvatskom jeziku: 11/Sv. 127, str. 219-221; **Švicarska** - Odluka Komisije od 26. srpnja 2000. sukladno Direktivi 95/46/EZ Europskog parlamenta i Vijeća o odgovarajućoj zaštiti osobnih podataka koja postoji u Švicarskoj, SL L 215/1, 25.8.2000. - posebno izdanje na hrvatskom jeziku: 16/Sv.1, str. 28-30.

[21] Članak 45. Uredbe. Dodatno vidi i razloge 103-107.

3.2. Prijenos u treće zemlje ili međunarodne organizacije bez primjerene zaštite

Voditelji obrade, kao i izvršitelji obrade ne smiju izvršiti prijenos osobnih podataka prema Uredbi u treće zemlje ili međunarodne organizacije bez primjerene zaštite *osim ako nisu ispunjene odgovarajuće zaštitne mjere i ako ispitanicima ne budu osigurana provediva prava i učinkovita sudska zaštita.*

A. Odgovarajuće zaštitne mjere

Odgovarajuće zaštitne mjere na temelju kojih se omogućuje prijenos prema Uredbi jesu, kako slijedi:

1) Instrumenti sklopljeni između tijela javne vlasti ili javnih tijela (trenutno nisu predviđeni Direktivom ZOP kao osnova za prijenos): radi li se o *pravno obvezujućem i provedivom instrumentu,* među ostalim o odredbama koje se uključuju u administrativne aranžmane poput memoranduma o razumijevanju, *kojima se ispitaniku osiguravaju ostvariva i učinkovita prava,* **nije potrebno odobrenje nadležnog nadzornog tijela**. No ako se zaštitne mjere predviđaju putem odredbi koje se unose u administrativne dogovore između tijela javne vlasti ili javnih tijela i koja sadrže provediva i djelotvorna prava ispitanika, a radi se o aranžmanima koji nisu pravno obvezujući, **tada je nužno ishoditi ovlaštenje nadležnog nadzornog tijela**[22].

[22] Detaljnije vidi u članku 46, stavku 2a, 3b i 4 te članku 63. Dodatno vidi i razlog 108.

2) Ugovorne klauzule između voditelja obrade ili izvršitelja obrade i voditelja obrade, izvršitelja obrade ili primatelja osobnih podataka u trećoj zemlji ili međunarodnoj organizaciji: nužno je ishoditi ovlaštenje nadležnog nadzornog tijela[23]. Napominjem da sva dana odobrenja ugovornih klauzula na temelju Direktive ZOP ostaju na snazi sve dok ih nadležno nadzorno tijelo prema potrebi ne izmijeni, zamijeni ili stavi izvan snage.[24]

U oba gore navedena slučaja pod točkama 1 i 2, kada se prijenos osobnih podataka temelji na osnovama za koja je potrebno odobrenje nadležnog nadzornog tijela, to se odobrenje daje kroz posebno propisani postupak međusobne suradnje nadzornih tijela (*mehanizam konzistentnosti*)[25], a kako bi se doprinijelo dosljednoj primjeni Uredbe u EU-u.[26]

3) Obvezujuća korporativna pravila

Uredba izričito uvodi obvezujuća korporativna pravila kao novu pravnu osnovu za međunarodni prijenos osobnih podataka. Ta se pravila u Uredbi definiraju kao „politike zaštite osobnih podataka kojih se voditelj obrade ili izvršitelj obrade s poslovnim nastanom na državnom području države članice pridržava za prijenose ili skupove prijenosa osobnih podataka voditelju obrade ili izvršitelju obrade u jednoj ili više trećih zemalja unutar grupe poduzetnika ili grupe poduzeća koja se bave zajedničkom gospodarskom djelatnošću“.[27] Kao relevantne s time u svezi potrebno je istaknuti i pojmove: a) *poduzeća* kao fizičke ili pravne osobe koja se bavi gospodarskom djelatnošću, bez obzira na pravni oblik te djelatnosti

[23] Članak 46, stavak 3a Uredbe.
[24] Članak 46, stavak 5 Uredbe.
[25] Detaljno o mehanizmu konzistentnosti vidi u poglavlju VII, 2. odjeljku Uredbe.
[26] Članak 46, stavci 3-4 i članak 63. Uredbe.
[27] Članak 4, točka 20. Uredbe.

(uključujući partnerstva ili udruženja koja se redovno bave gospodarskom djelatnošću), te b) *grupe poduzetnika*, kao poduzetnika u vladajućem položaju i njemu podređenih poduzetnika.[28]

Iako obvezujuća korporativna pravila trenutno nisu predviđena Direktivom ZOP, ona se danas primjenjuju u praksi multinacionalnih grupa kompanija kao osnova za kontinuirane prijenose osobnih podataka u članice grupe u trećim zemljama bez odgovarajuće razine zaštite osobnih podataka. Problematičan aspekt odobravanja tih pravila u smislu predviđenih osnova za prijenos osobnih podataka prema Direktivi ZOP u koju ta pravila spadaju (ugovorne odredbe prema čl. 26. st. 2.) jest taj da nadzorno tijelo za zaštitu osobnih podataka svake uključene države članice mora ta pravila pregledati i odobriti. Drugim riječima, da bi ta pravila bila punosnažna prema Direktivi ZOP svako to tijelo trebalo bi utvrditi da li je voditelj zbirke dao dovoljna jamstva u pogledu zaštite privatnosti i temeljnih prava pojedinaca, kao i u odnosu na izvršavanje povezanih prava. Tijekom proteklih je godina radna skupina članka 29. kroz niz dokumenata detaljno razradila sadržaj tih pravila i brojna druga pitanja u vezi s njihovom obvezujućom prirodom i učinkovitom provedbom, kako interno u poslovnim subjektima, tako i u odnosu na ispitanike i zaštitu njihovih prava. Iako neobvezujući, navedeni dokumenti (smjernice) široko su prihvaćeni u praksi nadzornih tijela.[29] Iste priznaje i naša Agencija za

[28] Članak 4, točke 18-19. Uredbe.

[29] Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, 11639/02/EN, WP 74, 3. lipnja 2003; Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules", 05/EN, WP107, 14. travnja 2005; Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, 05/EN, WP 108, 14. travnja 2005; Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data, WP 133, 10. siječnja 2007; Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, 1271-00-00/08/EN, WP 153, 24. lipnja 2008; Working Document Setting up a framework for the structure of Binding Corporate Rules, 1271-00-01/08/EN, WP 154, 24. lipnja 2008; Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules, 1271-04-02/08/EN, WP 155 rev.04, 24.6.2008, a zadnje revidirano 8. travnja 2009; National filing requirements for controller BCR ("BCR-C"), zadnja izmjena veljača 2016, http://ec.europa.eu/justice/data-protection/international-transfers/files/table_nat_admin_req_en.pdf.

zaštitu osobnih podataka, koja primjenjuje postupak priznavanja tih pravila sukladno postupku koja su razradila nadzorna tijela u državama članicama EU-a u okviru radne skupine članka 29.

Osim dogovorenih kriterija, čije ispunjavanje u značajnijoj mjeri osigurava usklađen postupak priznavanja obvezujućih korporativnih pravila od strane uključenih nadzornih tijela, činjenica jest da sam postupak njihova priznavanja od strane svakog uključenog nadzornog tijela u praksi može biti dugotrajan. Međutim, kroz razradu i primjenu u praksi *posebnog postupka suradnje* do danas je postignut značajan korak prema ubrzavanju postupka odobravanja tih pravila. Taj se postupak sastoji od sljedećeg. Prijava za odobrenje obvezujućih korporativnih pravila daje se na pregled *vodećem* nadzornom tijelu za zaštitu osobnih podataka. Kod utvrđivanja vodećeg nadzornog tijela za zaštitu podataka istaknuti su kriteriji, kako slijedi: europska lokacija sjedišta grupe tvrtki, mjesto odakle se donose ključne odluke u vezi sa svrhom i načinom obrade osobnih podataka, mjesto odakle se većinom izvoze osobni podaci, te mjesto tvrtke unutar grupe kompanija, koja je u najboljem položaju za predvođenje sustava podnošenja zahtjeva za odobrenje korporativnih pravila i, u slučaju primjene, za osiguravanje pridržavanja tih pravila. Vodeće će nadzorno tijelo po pregledu pravila i savjetovanju s voditeljem zbirke koji je podnio prijavu dalje koordinirati postupak odobrenja pravila s nadzornim tijelima drugih uključenih država članica.[30] U okviru navedenog postupka suradnje utvrđeni su i odgovarajući rokovi kako bi se onemogućilo njegovo odugovlačenje.

2008. je godine napravljen bitan pomak radi rješavanja problema dugotrajnog postupka priznavanja pravila od strane nadzornih tijela uključenih različitih država članica. Naime, tada je između određenog broja nadzornih tijela za zaštitu osobnih podataka postignut sporazum o primjeni *politike uzajamnog priznavanja* jednom odobrenih obvezujućih korporativnih pravila od strane vodećeg nadzornog tijela. Drugim riječima, odobri li vodeće nadzorno tijelo

[30] Article 29 Data Protection Working Party, Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules", 05/EN, WP 107, 14. travnja 2005.

obvezujuća korporativna pravila, po načelu uzajamnog povjerenja odobravaju ih i ostala nadležna tijela koje su članice predmetnog sporazuma. Od 28 država članica EU-a trenutno je njih 21 dio predmetnog sporazuma uzajamnog priznanja obvezujućih korporativnih pravila (Austrija, Belgija, Bugarska, Cipar, Češka, Estonija, Francuska, Njemačka, Island, Irska, Italija, Latvija, Lihtenštajn, Luksemburg, Malta, Nizozemska, Norveška, Slovačka, Slovenija, Španjolska i Ujedinjeno Kraljevstvo).[31]

Republika Hrvatska nije članica sporazuma uzajamnog priznanja. Prema objavljenim informacijama od 1. ožujka o.g., od Agencije je potrebno zatražiti odobrenje sadržaja obvezujućih korporativnih pravila koji su na snazi u drugim državama članicama, a koje ta Agencija nije odobrila. Radi odobrenja ovih pravila u svrhu njihove primjene u Republici Hrvatskoj potrebno je dostaviti sljedeću dokumentaciju:

a) obrazac WP133 (za voditelje zbirke osobnih podataka) ili WP195 (za izvršitelje zbirke osobnih podataka);
b) tekst obvezujućih korporativnih pravila;
c) opis iznošenja podataka; te
d) presliku odluke vodećeg nadzornog tijela koje je vodilo postupak odobravanja obvezujućih korporativnih pravila.

Iz dostavljene dokumentacije mora jasno proizlaziti obvezatnost primjene obvezujućih korporativnih pravila, osobni podaci na koje se ta pravila odnose i popis društava obuhvaćenih

[31] European Commission, What is mutual recognition?, http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/mutual_recognition/index_en.htm (zadnja izmjena sadržaja na stranici 24.11.2016).

tim pravilima.[32] Svoje odluke Agencija javno ne objavljuje, a procijenjeni rok za njihovo donošenje je najmanje 45 dana i to pod uvjetom da su svi dokumenti dostavljeni. [33]

Uredbom se postojeći nedostaci u pogledu odobravanja obvezujućih korporativnih pravila od strane svakog uključenog nadzornog tijela nastoje riješiti na način da ta pravila postaju punosnažna pod uvjetom ispunjenja propisanih uvjeta o sadržaju pravila, a što potvrđuje nadležno nadzorno tijelo u skladu s Uredbom predviđenim mehanizmom konzistentnosti u svrhu što dosljednije primjene Uredbe u EU-u.

Kada je riječ o tvrtkama koje će koristiti obvezujuća korporativna pravila a imaju poslovne nastane u više država članica, potrebno je imati na umu i pravila Uredbe o utvrđivanju *glavnog poslovnog nastana*[34] na temelju kojih se utvrđuje i ovlast *vodećeg nadzornog tijela*[35]. Kada je riječ o voditelju obrade s poslovnim nastanima u više država članica, glavni poslovni nastan je mjesto njegove središnje uprave u EU-u, *osim ako se odluke o svrhama i sredstvima obrade osobnih podataka donose u drugom poslovnom nastanu u EU-u koji je te odluke ovlašten provoditi*. U potonjem se slučaju taj drugi poslovni nastan smatra glavnim. Kada je riječ o izvršitelju obrade s poslovnim nastanima u više država članica, glavni je poslovni nastan mjesto njegove središnje uprave u EU-u. Nema li tamo središnju upravu, glavni poslovni nastan je onaj gdje se odvijaju glavne aktivnosti obrade u kontekstu aktivnosti poslovnog nastana izvršitelja obrade. Nadzorno tijelo glavnog poslovnog nastana (ili jedinog poslovnog nastana)

[32] Agencija za zaštitu osobnih podataka, Međunarodni transfer osobnih podataka - prava i obaveze ispitanika, http://azop.hr/aktualno/detaljnije/medunarodni-transfer-osobnih-podataka-prava-i-obaveze-ispitanika, 1. ožujka 2016.
[33] Article 29 Working Party, National filing requirements for controller BCR ("BCR-C"), zadnja izmjena veljača 2016, http://ec.europa.eu/justice/data-protection/international-transfers/files/table_nat_admin_req_en.pdf, str. 6.
[34] Članak 4, točka 16. Uredbe.
[35] Članak 56. u vezi s člankom 60. Uredbe.

voditelja obrade ili izvršitelja obrade nadležno je djelovati kao vodeće nadzorno tijelo za prekograničnu obradu koju provodi taj voditelj obrade ili izvršitelj obrade, u skladu s Uredbom propisanim postupkom suradnje vodećeg nadzornog tijela i drugih tzv. predmetnih nadzornih tijela (engl. *supervisory authority concerned*). [36]

U postupku konzistentnosti radi odobrenja obvezujućih korporativnih pravila sudjeluje Europski odbor za zaštitu osobnih podataka[37] koji daje mišljenje na nacrt odluke nadležnog nadzornog tijela (u ovdje opisanom slučaju vodećeg) o odobrenju obvezujućih korporativnih pravila.[38]

Uredbom propisani uvjeti koje obvezujuća pravila moraju zadovoljavati jesu, kako slijedi:

(a) pravila moraju biti pravno obvezujuća i primjenjivati se na svakog zainteresiranog člana određene grupe poduzetnika ili grupe poduzeća koja se bave zajedničkom gospodarskom djelatnošću, što uključuje njihove zaposlenike, i oni ih moraju provoditi;

(b) pravila moraju izrijekom pružati provediva prava ispitanicima u pogledu obrade njihovih osobnih podataka; i

(c) pravila moraju određivati najmanje:

> (i) strukturu i kontaktne podatke grupe poduzetnika ili grupe poduzeća koja se bave zajedničkom gospodarskom djelatnošću i svakog od njezinih članova;
>
> (ii) prijenose podataka ili skupove prijenosa, uključujući i kategorije osobnih podataka, vrste obrade i njezine svrhe, vrstu ispitanika te identifikaciju treće zemlje ili zemalja o kojima je riječ;

[36] Detaljnije o postupku suradnje vidi u poglavlju VII, 1. odjeljku Uredbe.
[37] Europski odbor za zaštitu osobnih podataka osniva se Uredbom kao tijelo Europske unije s pravnom sposobnošću, koje će zamijeniti današnju radnu skupinu članka 29, a njegovi su članovi voditelji po jednog nadzornog tijela iz svake države članice te Europski nadzornik za zaštitu podataka, odnosno njihovi predstavnici. Detaljnije o ovome Odboru vidi u poglavlju VII, odjeljku 3. Uredbe.
[38] Članak 64. stavak 1f Uredbe.

(iii) svoje pravno obvezujuće obilježje, kako iznutra tako i prema van;

(iv) primjenu općih načela zaštite osobnih podataka, osobito u pogledu ograničavanja svrhe, smanjenja količine podataka, ograničenog roka čuvanja, kvalitete podataka, tehničke i integrirane zaštite podataka, pravne osnove za obradu, obrade posebnih kategorija osobnih podataka, mjera za osiguravanje sigurnosti podataka i uvjeta za daljnji prijenos tijelima koja tim pravilima nisu obvezana;

(v) prava ispitanika s obzirom na obradu i načine za ostvarenje tih prava, uključujući i pravo da ne podliježu odlukama koje se isključivo temelje na automatiziranoj obradi, što uključuje izradu profila (u skladu s čl. 22. Uredbe), pravo na pritužbu nadležnom nadzornom tijelu i nadležnim sudovima država članica (u skladu s čl. 79. Uredbe) i na dobivanje sudske pomoći te, prema potrebi, naknade u slučaju kršenja obvezujućih korporativnih pravila;

(vi) to da voditelj obrade ili izvršitelj obrade s poslovnim nastanom na području države članice prihvati odgovornost za sva kršenja obvezujućih korporativnih pravila bilo kojeg zainteresiranog člana bez poslovnog nastana u EU-u. Voditelj obrade ili izvršitelj obrade bit će izuzet od ove odgovornosti, u cijelosti ili djelomično, samo ako dokaže da taj član nije odgovoran za događaj koji je prouzročio štetu;

(vii) kako se ispitanicima pružaju informacije o obvezujućim korporativnim pravilima (osobito o odredbama iz gornjih točaka iv-vi; pored informacija iz članaka 13. i 14. Uredbe);

(viii) zadaće svakog službenika za zaštitu podataka ili bilo koje druge osobe ili subjekta odgovornih za praćenje usklađenosti s obvezujućim korporativnim pravilima unutar grupe poduzetnika ili grupe poduzeća koja se bave zajedničkom gospodarskom djelatnošću, te praćenje osposobljavanja i rješavanja pritužbi;

(ix) postupke povodom pritužbi;

(x) mehanizme unutar grupe poduzetnika ili grupe poduzeća koja se bave zajedničkom gospodarskom djelatnošću, kojima se osigurava provjera poštovanja obvezujućih korporativnih pravila. Ti mehanizmi uključuju revizije

zaštite podataka i metode za korektivne mjere za zaštitu prava ispitanika. Rezultati takve provjere trebali bi se priopćiti osobi ili subjektu iz točke (viii) i upravnom odboru poduzetnika u vladajućem položaju u grupi poduzetnika ili grupi poduzeća koja se bave zajedničkom gospodarskom djelatnošću, te se na zahtjev ustupiti nadležnom nadzornom tijelu;

(xi) mehanizme za izvješćivanje i vođenje evidencije o promjenama pravila i izvješćivanje nadzornog tijela o tim promjenama;

(xii) mehanizam suradnje s nadzornim tijelom radi osiguravanja usklađenosti svakog člana grupe poduzetnika ili grupe poduzeća koja se bave zajedničkom gospodarskom djelatnošću, osobito tako da se nadzornom tijelu stave na raspolaganje rezultati provjera mjera iz točke (x);

(xiii) mehanizme za izvješćivanje nadležnog nadzornog tijela o bilo kakvim pravnim obvezama koje se na člana grupe poduzetnika ili grupe poduzeća koja se bave zajedničkom gospodarskom djelatnošću primjenjuju u trećoj zemlji, a koje bi mogle imati značajan štetan utjecaj na jamstva pružena obvezujućim korporativnim pravilima; te

(xiv) odgovarajuće osposobljavanje za zaštitu podataka za osoblje koje ima stalan ili redovan pristup osobnim podacima.

4) Standardne klauzule o zaštiti podataka

Pored i danas predviđenih standardnih ugovornih klauzula koje donosi Europska komisija[39], posebnu novost prema Uredbi predstavlja mogućnost prijenosa osobnih podataka na temelju standardnih ugovornih klauzula *koje donosi nadzorno tijelo, a odobrava Europska komisija.*

[39] Prema Direktivi ZOP danas su izrađeni setovi ugovornih odredbi koje se koriste između voditelja zbirki (EU, treća zemlja), od kojih se može koristiti bilo koji od navedena dva: a) Odluka Komisije 2001/497/EZ od 15. lipnja 2001. o standardnim ugovornim klauzulama za prijenos osobnih podataka u treće zemlje, u skladu s Direktivom 95/46/EZ, SL L 181/19, 4.7.2001. – posebno izdanje na hrvatskom jeziku: 13/Sv.51, str. 31-43., Ispravak Odluke Komisije 2001/497/EZ od 15. lipnja 2001. o standardnim ugovornim klauzulama za prijenos osobnih podataka u treće zemlje, u skladu s Direktivom 95/46/EZ, SL L 253, 21.9.2001, str. 34; b) Odluka Komisije 2004/915/EZ od 27. prosinca 2004. o izmjeni Odluke Komisije 2001/497/EZ u pogledu uvođenja alternativnog skupa standardnih ugovornih klauzula za prijenos osobnih podataka u treće zemlje, SL L 385/74, 29.12.2004. - posebno izdanje na hrvatskom jeziku: 13/Sv. 016, str. 210-220. Nadalje, ugovorne odredbe koje se prema Direktivi ZOP danas koriste

Standardne ugovorne klauzule koje donosi Komisija i one koje donosi nadzorno tijelo ukoliko ih prihvati Komisija sukladno Uredbi *neće trebati biti posebno odobrene od strane nadzornih tijela.* To danas nije slučaj u svim državama članicama kada je riječ o ugovornim klauzulama Komisije prema Direktivi ZOP, između ostalog u Republici Hrvatskoj. Tako je prema objavljenim informacijama od 1. ožujka o.g.[40] od Agencije za zaštitu osobnih podataka potrebno zatražiti prethodno odobrenje međunarodnog prijenosa osobnih podataka koji se temelji na odlukama Komisije, budući da iste smatra u smislu Zakona o zaštiti osobnih podataka ugovornim odredbama putem kojih voditelj zbirke mora pružiti dovoljna jamstva glede zaštite privatnosti i temeljnih prava i sloboda pojedinaca, te u pogledu kojih Agencija mora utvrditi da su odgovarajuća u skladu s važećim propisima kojima se uređuje zaštita osobnih podataka.[41]

(5) Odobreni kodeks ponašanja ili odobreni mehanizam certificiranja, *zajedno s obvezujućim i provedivim obvezama voditelja obrade ili izvršitelja obrade u trećoj zemlji za primjenu odgovarajućih zaštitnih mjera, između ostalog u pogledu prava ispitanika*: prijenos osobnih podataka u tom slučaju neće trebati biti posebno odobren od strane nadzornih tijela.

Odobreni kodeksi ponašanja, odnosno odobreni mehanizmi certificiranja sasvim su nove predviđene osnove za međunarodni prijenos osobnih podataka u odnosu na Direktivu ZOP.

između voditelja zbirke (EU) i izvršitelja obrade (treća zemlja): Odluka Komisije 2010/87/EU od 5. veljače 2010. o standardnim ugovornim klauzulama za prijenos osobnih podataka izvršiteljima obrade u trećim zemljama u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća, SL L 39/5, 12.2.2010. - posebno izdanje na hrvatskom jeziku: 13/Sv.52, str. 250-263.

[40] Agencija za zaštitu osobnih podataka, Međunarodni transfer osobnih podataka - prava i obaveze ispitanika, http://azop.hr/aktualno/detaljnije/medunarodni-transfer-osobnih-podataka-prava-i-obaveze-ispitanika, 1. ožujka 2016.

[41] Članak 13. stavak 4. al. 3. Zakona o zaštiti osobnih podataka.

Što se tiče samih kodeksa ponašanja valja napomenuti kako je njihova izrada već i danas predviđena Direktivom ZOP[42] (ali ne i našim Zakonom o zaštiti osobnih podataka). S druge strane Uredbom predviđeno dobrovoljno certificiranje zaštite osobnih podataka te pečata i oznaka za zaštitu osobnih podataka u potpunosti je novouvedeni mehanizam koregulacije u općem okviru zaštite osobnih podataka EU-a.

Kada je riječ o kodeksima ponašanja u Direktivi ZOP utvrđuju se kako države članice trebaju predvidjeti mogućnost da udruženja trgovaca i druga tijela koja predstavljaju druge kategorije voditelja obrade mogu dostaviti nacrte nacionalnih kodeksa na pregled (mišljenje) nadležnom nadzornom tijelu za zaštitu podataka, kao i ovlast nadzornih tijela da utvrde jesu li takvi nacrti kodeksa u skladu s relevantnim domaćim propisima. Uz nacionalne kodekse predviđaju se i europski kodeksi tj. kodeksi s područjem primjene unutar EU-a. Oni se trebaju dostaviti na mišljenje (odobrenje) radnoj skupini članka 29.[43]

Gledano u odnosu na Direktivu ZOP Uredba daje vrlo konkretne konture značaju pridržavanja odobrenih kodeksa ponašanja. Drugim riječima, važnost pridržavanja odobrenih kodeksa za voditelje zbirke i izvršitelje obrade i njihova posebna vrijednost u tom smislu konkretizira se kroz niz propisanih slučajeva u Uredbi (koregulacija). Slično kao i u Direktivi ZOP predviđa se da kodekse mogu izraditi udruženja i druga tijela koja predstavljaju kategorije voditelja obrade *ili izvršitelja obrade*, s ciljem olakšavanja primjene Uredbe, a pritom se trebaju *uzeti u obzir posebna obilježja različitih sektora obrade i posebne potrebe mikro, malih i srednjih*

[42] Članak 27. i razlog 61 Direktive ZOP.
[43] Za odobrenje prvog europskog kodeksa sukladno Direktivi ZOP vidi: Article 29 Data Protection Working Party, Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing, 10066/03/EN final, WP 77, 13.6. 2003.

poduzeća. U Uredbi se predviđaju primjeri važnijih pitanja koje je moguće dalje razraditi kroz kodekse. Kodekse odobravaju nadležna nadzorna tijela za zaštitu osobnih podataka, odnosno Europski odbor za zaštitu podataka ukoliko se aktivnosti obrade odvijaju u više država članica ili čitavom EU-u. Osim toga, Europska je komisija ovlaštena je proglasiti opću valjanost kodeksa unutar EU-a u slučaju prethodnog pozitivnog mišljenja Europskog odbora za zaštitu osobnih podataka (o tome da je kodeks u skladu s Uredbom). Konačno, kako poštovanje odobrenih kodeksa ponašanja može poslužiti radi dokazivanja usklađenog postupanja s Uredbom, važnu novost predstavlja obveza osiguravanja odgovarajućeg mehanizma nadzora nad njihovim pridržavanjem. Taj nadzor moraju vršiti stručna i neovisna, akreditirana treća tijela. Odobreni kodeksi ponašanja javno se objavljuju.[44]

Kako sam ranije napomenula, Uredbom predviđeno *dobrovoljno certificiranje zaštite osobnih podataka te pečata i oznaka za zaštitu osobnih podataka* potpuna je novost gledano u odnosu na Direktivu ZOP. Osim što takvo certificiranje omogućuje ispitanicima brzu procjenu razine zaštite osobnih podataka za proizvode i usluge o kojima je riječ (transparentnost), ono može značajno pomoći pri dokazivanju usklađenosti postupaka obrade osobnih podataka (voditelja ili izvršitelja obrade) o kojima je riječ, s Uredbom. Uredba predviđa poticanje uspostave spomenutih mehanizama certificiranja zaštite osobnih podataka te pečata i oznaka za zaštitu osobnih podataka, osobito na razini EU-a, i to od strane država članica i nadzornih tijela za zaštitu osobnih podataka, Europskog odbora za zaštitu podataka i Europske komisije. Pritom treba uzeti u obzir posebne potrebe mikro, malih i srednjih poduzeća. Certifikate će izdavati nadležna nadzorna tijela za zaštitu osobnih podataka, odnosno akreditirana certifikacijska tijela na najviše tri godine, uz mogućnost obnove. Kriterije za certifikaciju odredit će nadležno

[44] Detaljnije vidi u člancima 40-41; članku 57. stavku 1m, 1p, 1q i članku 58. stavku 3d (zadaci i ovlasti nadzornih tijela); članku 64. st. 1b-1c (mehanizam konzistentnosti - mišljenja Odbora); članku 70. stavku 1n i 1x (zadaće Odbora). Dodatno vidi i razloge 98-99 Uredbe.

nadzorno tijelo, odnosno Europski odbor za zaštitu osobnih podataka koji može izraditi kriterije i za zajedničku certifikaciju (*Europski pečat za zaštitu osobnih podataka*). Odbor unosi u evidenciju i objavljuje sve mehanizme certificiranja, pečate i oznake za zaštitu osobnih podataka. Europska komisija ovlaštena je donositi provedbene akte kojima propisuje tehničke standarde za mehanizme certificiranja, pečate i oznake za zaštitu podataka te mehanizme promicanja i priznavanja tih mehanizama certificiranja, pečata i oznaka.[45]

B. Druge Uredbom predviđene osnove

i) Odstupanja za posebne situacije

Ukoliko u vezi s namjeravanim prijenosom osobnih podataka trećoj zemlji ili organizaciji nema odluke Komisije o primjerenosti niti su ispunjene ranije navedene odgovarajuće zaštitne mjere, prijenos je ipak moguće izvršiti ako je ispunjen jedan od sljedećih uvjeta:

(1) ispitanik je *izričito pristao* na predloženi prijenos, nakon što je bio obaviješten o *mogućim rizicima takvih prijenosa za ispitanika zbog nepostojanja odluke o primjerenosti i odgovarajućih zaštitnih mjera* [46]

Prema Direktivi ZOP se i danas privola ispitanika predviđa kao moguća osnova za prijenos, međutim Uredbom se dodatno predviđa obavijest ispitaniku o mogućim rizicima takvih prijenosa te se postavlja *kriterij izričite* privole.

(2) prijenos je nužan za izvršavanje ugovora između ispitanika i voditelja obrade ili provedbu predugovornih mjera na zahtjev ispitanika[47]

[45] Detaljnije vidi u člancima 42-43; članku 57. stavcima 1n, 1o, 1p i 1q; članku 58. stavku 1c, stavku 2 h, stavku 3e i stavku 3f (zadaci i ovlasti nadzornih tijela); članku 64. stavku 1c (mehanizam konzistentnosti - mišljenja Odbora) i članku 70. stavku 1n – 1q (zadaće Odbora). Dodatno vidi i razloge 100 i 168 Uredbe.
[46] Ne primjenjuju se na aktivnosti koje provode tijela javne vlasti izvršavajući svoje javne ovlasti.
[47] Ibid.

(3) prijenos je nužan radi sklapanja ili izvršavanja ugovora sklopljenog u interesu ispitanika između voditelja obrade i druge fizičke ili pravne osobe[48];

(4) prijenos je nužan iz važnih razloga javnog interesa, *koji mora biti priznat u pravu EU-a ili pravu države članice kojem podliježe voditelj obrade* (značajnija izmjena u odnosu na Direktivu ZOP posebno je označena)

(5) prijenos je nužan za postavljanje, ostvarivanje ili obranu pravnih zahtjeva;

(6) prijenos je nužan za zaštitu životno važnih interesa ispitanika *ili drugih osoba ako ispitanik fizički ili pravno ne može dati privolu* (značajnija izmjena u odnosu na Direktivu ZOP posebno je označena)

(7) prijenos se obavlja iz registra koji prema pravu Unije ili pravu države članice služi pružanju informacija javnosti i koji je otvoren na uvid javnosti ili na zahtjev bilo kojoj osobi koja može dokazati "neki opravdani interes"[49] ali samo u mjeri u kojoj su ispunjeni uvjeti propisani u pravu EU-a ili pravu države članice za uvid u tom posebnom slučaju.

Iz registra se ne bi smjeli prenijeti svi osobni podaci ili sve kategorije osobnih podataka. Kada registar služi na uvid osobama koje imaju opravdani interes, prijenos se obavlja samo na zahtjev tih osoba ili ako su one primatelji.

ii) Uvjerljiv legitiman interes voditelja obrade

Uredba predviđa uvjerljiv legitiman interes voditelja obrade kao osnovu za prijenos osobnih podataka u treću zemlju ili organizaciju *koja se može koristiti samo u iznimnim slučajevima*. Osim toga, ta se osnova ne primjenjuje na aktivnosti koje provode tijela javne vlasti izvršavajući svoje javne ovlasti. Propisani uvjeti za korištenje te osnove moraju se kumulativno ispuniti, kako slijedi:

[48] Ibid.

[49] Napominjem da se u engleskoj verziji Uredbe utvrđuje potreba dokazivanja legitimnog interesa za prijenos, dok hrvatska verzija Uredbe sadrži pojam „nekog opravdanog" interesa, iako je moguće da u domaćoj praksi neće biti razlike prilikom primjene, odnosno tumačenja tog interesa kod međunarodnog prijenosa osobnih podataka prema toj osnovi.

1) nije primjenjiva niti jedna druga predviđena osnova za prijenos (odluka o primjerenosti, zaštitne mjere, odstupanja za posebne situacije),

2) prijenos se ne ponavlja,

3) prijenos se odnosi samo na ograničen broj ispitanika, i

4) prijenos je nužan za potrebe uvjerljivih, legitimnih interesa voditelja obrade koji nisu podređeni interesima ili pravima i slobodama ispitanika, a voditelj obrade procijenio je sve okolnosti prijenosa te je na temelju te procjene predvidio odgovarajuće zaštitne mjere u pogledu zaštite osobnih podataka.

Voditelj obrade o takvom je prijenosu dužan obavijestiti nadzorno tijelo, ali i ispitanika.[50]

iii) Prijenos na temelju presude suda ili odluke upravnog tijela treće zemlje

Sve presude suda ili sve odluke upravnog tijela treće zemlje kojima se od voditelja ili izvršitelja obrade zahtijeva prijenos ili otkrivanje osobnih podataka mogu biti priznate ili izvršive na bilo koji način *samo ako se temelje na nekom međunarodnom sporazumu*, poput ugovora o uzajamnoj pravnoj pomoći, *koji je na snazi između treće zemlje koja je podnijela zahtjev i EU-a ili države članice EU-a* (ne dovodeći u pitanje druge osnove za prijenos u skladu s Uredbom[51]).[52]

[50] Detaljnije o obvezama informiranja ispitanika vidi u člancima 13.-14. Uredbe.
[51] Kako se pojašnjava u Uredbi, jedna od dopuštenih osnova za prijenos u takvim slučajevima mogao bi na primjer biti prijenos koji je nužan iz važnih razloga javnog interesa priznatog pravom EU-a ili pravom države članice koje se primjenjuje na voditelja obrade (razlog 115).
[52] Članak 48. Uredbe.

3.3. Mogućnost ograničenja prijenosa određenih kategorija osobnih podataka

Uredba dopušta državama članicama da iz važnih razloga javnog interesa izričito odrede ograničenja prijenosa određenih kategorija osobnih podataka trećoj zemlji ili međunarodnoj organizaciji. To je dopušteno samo ako nije donesena odluka o primjerenosti. Države članice dužne su obavijestiti Komisiju o takvim odredbama.[53]

4. Zaključne napomene

U današnje doba digitalne ekonomije i Velikih Podataka u radu analizirana utvrđenja Suda Unije o mogućnosti identifikacije umreženih pojedinaca na temelju IP adrese kao digitalnog identifikatora vrlo su značajna za umrežene aktere u svrhu osiguravanja usklađenog postupanja prilikom daljnjeg prikupljanja, odnosno obrade takvih podataka. Iako Uredba ne donosi značajnije pomake s obzirom na u radu razmatranu praksu Suda Unije pri tumačenju osobnog podatka prema Direktivi ZOP, očekujem da će poglavito pitanja povezana s mogućnostima neizravne identifikacije pojedinaca predstavljati izazove u praksi domaćih nadzornih tijela, ali i sudova država članica EU-a. Stoga je vrlo važno pratiti aktivnosti Europskog odbora za zaštitu podataka u čije zadatke spada *inter alia* ispitivanje svih pitanja koja obuhvaćaju primjenu Uredbe te izdavanje smjernica, preporuka i primjera najbolje prakse kako bi se poticala dosljedna primjena Uredbe. Sva ta pitanja nužno je odgovarajuće popratiti u aktivnostima domaće Agencije za zaštitu osobnih podataka, a to se odnosi i na potrebu pravovremene objave relevantne prakse Suda EU-a i u pogledu tumačenja trenutno važeće Direktive ZOP.

Kada je riječ o novom sustavu međunarodnog prijenosa osobnih podataka izvan EU-a/EGP-a, a koji općenito gledano odražava isto temeljno načelo kao i Direktiva ZOP, istraživanje u ovome radu ukazalo je na značajne novosti koje donosi Uredba, bilo u vidu pojedinih sasvim

[53] Članak 49, stavak 5. Uredbe.

novih osnova za takav prijenos (npr. odobreni kodeks ponašanja ili mehanizam certificiranja), bilo u vidu razrađenijih pravila oko već postojećih mehanizama prijenosa (npr. kriteriji za donošenje odluke o primjerenosti zaštite, a iz kojih je razvidan i utjecaj presude Suda EU-a u predmetu Schrems). S druge strane, koliko god danas razumljiva i opravdana, novouvedena mogućnost da države članice ograniče prijenos određenih kategorija osobnih podataka iz važnog javnog interesa svakako komplicira ideju neometanog tijeka budućih međunarodnih prijenosa. Trenutno je teško predvidjeti mogu li opisana nova pravila umiriti u najmanjoj mjeri percepciju pravne nesigurnosti koja se javlja u praksi s obzirom na brojne tekuće događaje koji se nadovezuju na presudu Suda Unije o ukidanju Safe Harboura. Naime, potreba ispunjenja visokih standarda koje prema Sudu treće zemlje moraju zadovoljiti kako bi se utvrdila odgovarajuća razina zaštite osobnih podataka potencijalno dovodi u pitanje valjanost i drugih predviđenih instrumenata za prijenos osobnih podataka prema *acquis*-u. Pritom treba imati na umu i to da prema Uredbi odluke o odgovarajućoj razini zaštite u trećim zemljama koje je Komisija donijela na temelju Direktive ZOP ostaju na snazi dok se ne izmijene, zamijene ili stave izvan snage novim provedbenim aktom tj. odlukom donesenom prema Uredbi, a isto se odnosi na standardne ugovorne klauzule koje su ranije donesene na temelju Direktive ZOP.

Kada je riječ o međunarodnom prijenosu nakon ukidanja Odluke Komisije 2000/520/EZ o Safe Harbouru treba napomenuti da je Europska komisija nakon višemjesečnih pregovora s Ministarstvom trgovine SAD-a nedavno donijela odluku o primjerenoj zaštiti novog sustava zaštite privatnosti u skladu s Direktivom ZOP (EU-SAD Štit privatnosti, engl. *EU-US Privacy Shield)* [54]. Iako se i ovaj sustav temelji na samocertificiranju primatelja podataka kao i Safe Harbour, općenito se može reći da isti predstavlja značajno poboljšanje. To je s obzirom na utvrđene strože obveze primatelja podataka u SAD-u i kontrole njihova pridržavanja s

[54] Provedbena odluka Komisije (EU) 2016/1250 od 12. srpnja 2016. o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća, SL L 207, 1.8.2016, str. 1–112.

pravilima Štita privatnosti, razrađena ograničenja i pisana jamstva Vlade SAD-a u vezi s pristupom podacima u svrhe progona i zaštite nacionalne sigurnosti, utvrđene postupke preispitivanja, uključujući obvezna godišnja zajednička preispitivanja koji mogu dovesti i do suspenzije ili čak stavljanja na snagu predmetne odluke Komisije, te uspostavljene mehanizme za osiguranje provedive pravne zaštite ispitanika u EU-u. Glede potonjeg treba imati na umu novouvedenu instituciju neovisnog američkog Pravobranitelja za sustav zaštite privatnosti zaduženog za rješavanje pritužbi ispitanika u EU-u u vezi s obradom njihovih osobnih podataka za potrebe nacionalne sigurnosti, odnosno u vezi s pristupom njihovim podacima od strane sigurnosnih službi. Osim međunarodnih prijenosa temeljem ove odluke Komisije taj bi se mehanizam trebao primjenjivati i na prijenose na temelju drugih instrumenata trenutno predviđenih *acquis*-om pa čak i specifičnih osnova koje se predviđaju u novoj Uredbi.[55]

Imajući u vidu da će po početku primjene Uredbe u državama članicama EU-a prestati važiti Direktiva ZOP na kojoj se temelji ova odluka o primjerenosti zaštite, Europska se komisija obvezala nakon početka primjene Uredbe ponovno procijeniti razinu zaštite koju pruža Štit privatnosti. No tome će prethoditi njegovo zajedničko preispitivanje, a čiji rezultat može polučiti utjecaj i na druge instrumente prijenosa osobnih podataka kada je riječ o pristupu osobnim podacima od strane američkih tijela vlasti.[56]

Svim ovim pitanjima danas se pristupa vrlo ozbiljno kada je riječ o zaštiti prava ispitanika u EU-u, na što na prvome mjestu upućuju nedavno pokrenuti postupci pred Sudom EU-a radi poništenja Štita privatnosti. Prva je poništenje tijekom rujna 2016. godine zatražila neprofitna

[55] PRILOG III., Prilog A. Mehanizam pravobranitelja za europsko-američki sustav za zaštitu privatnosti, ibid.
[56] Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf.

organizacija *Digital Rights Ireland*[57], dok su drugi zahtjev krajem listopada postavile i organizacije La *Quadrature du Net*, *French Data Network* i *Fédération FDN*.[58]

Istovremeno, Europska komisija iz razloga osiguravanja sukladnosti s presudom Suda u predmetu Schrems radi na izmjenama ranijih odluka o postojanju odgovarajuće, odnosno primjerene zaštite osobnih podataka u trećim zemljama, kao i odluka o standardnih ugovornim klauzulama. No njezina razmatranja o mogućim nezakonitostima tih odluka ograničena su na otklanjanje nezakonitosti s obzirom na utvrđenja Suda Unije u Schrems presudi o prekoračenju ovlasti Komisije, jer je spornom odlukom ograničila ovlast nadzornih tijela da zabrane međunarodne prijenose osobnih podataka. Kako se slična odredba nalazi u sadašnjim odlukama o odgovarajućoj razini zaštite te standardnim ugovornim klauzulama, glavni je cilj najavljenih izmjena prema Komisiji taj da se spomenuta ograničenja otklone te osigura mogućnost korištenja svih ovlasti domaćih nadzornih tijela prema pravu EU-a i prema domaćem pravu.[59]

Moguće ocjenjivanje (ne)valjanosti odluka Komisije pred Sudom Unije i to (u najmanjoj mjeri) njezinih standardnih ugovornih klauzula, iz šireg aspekta razloga od onih koje Komisija ističe pri njihovoj trenutnoj reviziji, daje dodatnu težinu svoj ovdje razmatranoj problematici međunarodnih prijenosa. Naime, trenutno (studeni 2016.) se pred irskim Visokim sudom očekuje njegova odluka o prihvaćanju ili neprihvaćanju zahtjeva irske povjerenice za zaštitu osobnih podataka o pokretanju prethodnog postupka pred Sudom EU-a u vezi s nevaljanošću tih klauzula. U domaćem se postupku ovdje radi o nastavku postupka kojeg je ranije pokrenuo Schrems u vezi s prijenosom osobnih podataka od strane tvrtke Facebooka Irska u tvrtku majku

[57] Predmet T-670/16, tužba podnesena 16. rujna 2016, Digital Rights Ireland protiv Europske komisije.
[58] Predmet T-738/16, La Quadrature du Net i drugi protiv Europske komisije, 25.10.2016.; Recours en annulation (263 TFUE) contre la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016, https://cdn2.nextinpact.com/medias/exegetes_requete_ps.pdf; Next INpact, Le Privacy Shield attaqué en Europe par la Quadrature, FDN et FFDN, 31.10.2016., http://www.nextinpact.com/news/101950-le-privacy-shield-attaque-en-europe-par-quadrature-fdn-et-ffdn.htm.
[59] Summary record of the 72nd meeting of the Committee on the Protection of Individuals with regard to the Processing of Personal Data (Article 31 Committee), 03. listopada 2016., dostupno pretragom na: http://ec.europa.eu/transparency/regcomitology/index.cfm.

Facebook Inc. u SAD-u. On je takav prijenos prvotno osporavao kada se isti zasnivao na Safe Harbour mehanizmu i povodom toga je u konačnici Sud EU-a donio presudu o njegovu ukidanju. No nakon ukidanja Safe Harbour programa utvrđeno je da Facebook Irska nastavlja s takvim prijenosom, ali na temelju Komisijinih standardnih ugovornih klauzula. Schrems sada osporava prijenos na temelju tih klauzula. Ovo sve imajući u vidu razloge Suda EU-a za ukidanje Odluke Komisije o Safe Harbouru, a koji se u nizu aspekata *per analogiam* mogu smatrati primjenjivima i na standardne ugovorne klauzule osobito kada je riječ o problematici pristupanja prenašanim osobnim podacima ispitanika u EU-u od strane američkih vladinih tijela. Prema posljednjim je informacijama irska povjerenica za zaštitu osobnih podataka u skladu sa svojim ovlastima utvrdila postojanje valjanih razloga za uvažavanje Schremsovih tvrdnji. Radi razjašnjenja spornih pitanja ona je stoga pred irskim Visokim sudom podnijela zahtjev za pokretanjem prethodnog postupka pred Sudom EU-a. Odluka Visokog suda očekuje se najranije tijekom prve polovice 2017. godine, a iznimnom značaju tog postupka svjedoči svakako i činjenica da je i američka Vlada zatražila svojstvo umješača kao prijatelj suda (*amicus curiae*), što je Visoki sud odobrio.[60] U daljnjem je praćenju teme potrebno imati na umu i ranije spomenuto područje primjene mehanizma pravobranitelja za europsko-američki sustav za zaštitu privatnosti, a koji se primjenjuje i na prijenose temeljem standardnih ugovornih klauzula, obvezujućih korporativnih pravila, ali i drugih u ovome radu analiziranih osnova koje se predviđaju samom novom Uredbom.

[60] Data Protection Commissioner, Update on litigation involving Facebook and Maximilian SchremS - Explanatory Memo, https://www.dataprotection.ie/docs/28-9-2016-Explanatory-memo-on-litigation-involving-Facebook-and-Maximilian-Schrems/1598.htm; http://www.politico.eu/wp-content/uploads/2016/07/DPC-v.-Facebook-Final.pdf.