



18/HR

WP 254 rev.01

Radna skupina iz članka 29.

Referentni dokument o primjerenosti

Donesen 28. studenoga 2017.

Zadnji put revidiran i donesen 6. veljače 2018.

Radna skupina osnovana je u skladu s člankom 29. Direktive 95/46/EZ. To je nezavisno europsko savjetodavno tijelo za zaštitu podataka i privatnost. Njegovi su zadaci opisani u članku 30. Direktive 95/46/EZ i članku 15. Direktive 2002/58/EZ.

Tajništvo osigurava Uprava C (Temeljna prava i građanstvo Unije) Europske komisije, Glavna uprava za pravosuđe, B-1049 Bruxelles, Belgija, ured br. MO-59 02/013.

Internetska stranica:

http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Uvod

Radna skupina tijela EU-a za zaštitu podataka¹ (Radna skupina iz članka 29.) već je objavila Radni dokument o prijenosima osobnih podataka trećim zemljama (Radni dokument 12)². Nakon što je Direktiva zamijenjena Općom uredbom o zaštiti podataka (GDPR)³, Radna skupina iz članka 29. revidira Radni dokument 12, svoje prethodne smjernice, kako bi ga ažurirala u kontekstu novog zakonodavstva i novije sudske prakse Suda Europske unije (SEU)⁴.

Ovim se radnim dokumentom nastoji ažurirati poglavlje 1. Radnog dokumenta 12, koje se odnosi na središnje pitanje primjerene razine zaštite podataka u trećoj zemlji, području ili jednom ili više određenih sektora unutar te treće zemlje ili u međunarodnoj organizaciji (dalje u tekstu: „treće zemlje ili međunarodne organizacije”). Ovaj će se dokument u nadolazećim godinama kontinuirano preispitivati i prema potrebi ažurirati na temelju praktičnog iskustva stečenog primjenom Opće uredbe o zaštiti podataka. Poglavlje 2. (Primjena pristupa na zemlje koje su ratificirale Konvenciju 108) i poglavlje 3. (Primjena pristupa na samoregulaciju industrije) Radnog dokumenta 12 trebalo bi ažurirati u kasnijoj fazi.

Ovaj radni dokument usmjeren je isključivo na odluke o primjerenosti, a to su provedbeni akti⁵ Europske komisije, u skladu s člankom 45. Opće uredbe o zaštiti podataka. Ostali aspekti prijenosa osobnih podataka trećoj zemlji i međunarodnoj organizaciji bit će ispitani u narednim radnim dokumentima koji će se objavljivati zasebno (obvezujuća korporativna pravila, odstupanja).

Cilj je ovog dokumenta pružiti smjernice, na temelju Opće uredbe o zaštiti podataka, Europskoj komisiji i Radnoj skupini iz članka 29. za procjenu razine zaštite podataka u trećim zemljama i međunarodnim organizacijama uspostavom temeljnih načela zaštite podataka koja moraju biti prisutna u pravnom okviru treće zemlje ili međunarodne organizacije kako bi se osigurala neophodna usklađenost s okvirom EU-a. Osim toga, može poslužiti kao vodič trećim zemljama i međunarodnim organizacijama koje su zainteresirane za dobivanje zaključka o primjerenosti. Međutim, načela utvrđena u ovom radnom dokumentu nisu izravno upućena voditeljima obrade podataka ili izvršiteljima obrade podataka.

Ovaj se dokument sastoji od četiri poglavlja:

Poglavlje 1.: Neke opće informacije povezane s pojmom primjerenosti

Poglavlje 2.: Postupovni aspekti zaključaka o primjerenosti u skladu s Općom uredbom o zaštiti podataka

Poglavlje 3.: Opća načela zaštite podataka. To poglavlje uključuje temeljna opća načela zaštite podataka kako bi se osiguralo da razina zaštite podataka u trećoj zemlji ili međunarodnoj organizaciji bude u načelu istovjetna onoj koja je uspostavljena zakonodavstvom EU-a.

Poglavlje 4.: Ključna jamstva za pristup podacima za potrebe izvršavanja zakonodavstva i nacionalne sigurnosti kako bi se ograničilo zadiranje u temeljna prava. To poglavlje uključuje ključna jamstva za pristup podacima za potrebe izvršavanja zakonodavstva i nacionalne sigurnosti koja slijede presudu Suda Europske unije u predmetu Schrems iz 2015. i temelje se na radnom dokumentu Radne skupine iz članka 29. o ključnim jamstvima, koji je donesen 2016.

¹Osnovana u skladu s člankom 29. Direktive EU-a o zaštiti podataka 95/46/EZ

²Radni dokument 12, „Radni dokument: Prijenosi osobnih podataka trećim zemljama: primjena članaka 25. i 26. Direktive EU-a o zaštiti podataka” koji je Radna skupina donijela 24. srpnja 1998.

³Uredba (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) (Tekst značajan za EGP)

⁴Uključujući predmet C-362/14, Maximilian Schrems protiv Data Protection Commissioner, 6. listopada 2015.

⁵Vidjeti relevantan članak 45. stavak 3. i članak 93. stavak 2. Opće uredbe o zaštiti podataka za dodatne informacije o provedbenim aktima.

Poglavlje 1.: Neke opće informacije povezane s pojmom primjerenosti

Člankom 45. stavkom 1. Opće uredbe o zaštiti podataka utvrđeno je načelo da se prijenosi podataka trećoj zemlji ili međunarodnoj organizaciji mogu provesti samo ako predmetna treća zemlja, područje, ili jedan ili više određenih sektora unutar te treće zemlje, ili međunarodna organizacija osiguravaju primjerenu razinu zaštite.

Pojam „primjerene razine zaštite”, koji je postojao već u Direktivi 95/46, dodatno je razradio Sud Europske unije. Ovdje je važno prisjetiti se standarda koji je Sud Europske unije utvrdio u predmetu Schrems, a koji glasi da „razina zaštite” u trećoj zemlji mora biti „bitno ekvivalentna” onoj koja je zajamčena u EU-u, iako se „u tom pogledu pravna sredstva kojima se koristi treća zemlja za osiguranje takve razine zaštite mogu razlikovati od onih koja se provode u [EU-u].”⁶ Cilj stoga nije preslikati europsko zakonodavstvo točku po točku, već uspostaviti bitne temeljne zahtjeve tog zakonodavstva.

Svrha je odluka o primjerenosti koje donosi Europska komisija službeno potvrditi, uz obavezujuće učinke za države članice,⁷ da je razine zaštite podataka u trećoj zemlji ili međunarodnoj organizaciji bitno ekvivalentna razini zaštite podataka u Europskoj uniji.⁸ Primjerenost se može ostvariti kombinacijom prava ispitanika i obveza onih koji obrađuju podatke, ili onih koji izvršavaju kontrolu nad obradom i nadzorom koji provode neovisna tijela. No, pravila o zaštiti podataka djelotvorna su samo ako su provediva i ako se slijede u praksi. Stoga je nužno razmotriti sadržaj pravila primjenjivih na osobne podatke koji se prenose trećoj zemlji ili međunarodnoj organizaciji, ali i sustav koji je uspostavljen radi osiguravanja djelotvornosti tih pravila. Učinkoviti mehanizmi provedbe iznimno su važni za djelotvornost pravila o zaštiti podataka.

Člankom 45. stavkom 2. Opće uredbe o zaštiti podataka utvrđeni su elementi koje Europska komisija uzima u obzir pri procjeni primjerenosti razine zaštite u trećoj zemlji i međunarodnoj organizaciji.

Na primjer, Komisija uzima u obzir vladavinu prava, poštovanje ljudskih prava i temeljnih sloboda, relevantno zakonodavstvo, postojanje i djelotvorno funkcioniranje jednog neovisnog nadzornog tijela ili više njih i međunarodne obveze koje je treća zemlja ili međunarodna organizacija preuzela.

Stoga je jasno da se svaka smisljena analiza primjerene zaštite mora sastojati od dva osnovna elementa: sadržaja pravila koja se primjenjuju i sredstava za osiguravanje njihove djelotvorne primjene. Europska komisija dužna je redovito provjeravati jesu li postojeća pravila djelotvorna u praksi.

„Jezgra” „sadržajnih” načela i „postupovnih/provedbenih” zahtjeva u pogledu zaštite podataka, koji se mogu promatrati kao minimalan uvjet da bi zaštita bila primjerena, proizlazi iz Povelje Europske unije o temeljnim pravima i Opće uredbe o zaštiti podataka. Osim toga, trebalo bi uzeti u obzir i druge međunarodne sporazume o zaštiti podataka, npr. Konvenciju 108.⁹

Treba obratiti pozornost i na pravni okvir na temelju kojeg javna tijela pristupaju osobnim podacima. Dodatne smjernice o tome mogu se pronaći u Radnom dokumentu 237 (tj. dokumentu o ključnim jamstvima)¹⁰ o zaštitnim mjerama u kontekstu nadzora.

Opće odredbe koje se odnose na zaštitu podataka i privatnost u trećoj zemlji nisu dostatne. Naprotiv, u pravni okvir treće zemlje ili međunarodne organizacije moraju biti uključene posebne odredbe kojima se rješavaju konkretne potrebe za praktično relevantnim aspektima prava za zaštitu podataka. Te odredbe moraju biti provedive.

Poglavlje 2.: Postupovni aspekti zaključaka o primjerenosti u skladu s Općom uredbom o

⁶ Predmet C-362/14, Maximillian Schrems protiv Data Protection Commissioner, 6. listopada 2015. (točke 73. i 74.).

⁷ Članak 288. stavak 2. Ugovora o funkcioniranju Europske unije.

⁸ Predmet C-362/14, Maximillian Schrems protiv Data Protection Commissioner, 6. listopada 2015. (točka 52.).

⁹ Uvodna izjava 105. Opće uredbe o zaštiti podataka.

¹⁰ Radni dokument 01/2016 o opravdanosti zadiranja u temeljna prava na privatnost i zaštitu podataka u okviru mjera nadzora pri prijenosu osobnih podataka (Europska ključna jamstva), 16/EN WP 237, 13. travnja 2016.

zaštiti podataka

Kako bi Europski odbor za zaštitu podataka ispunio svoju zadaću u pogledu savjetovanja Europske komisije u skladu s člankom 70. stavkom 1. Opće uredbe o zaštiti podataka, Europskom odboru za zaštitu podataka trebalo bi dostaviti svu relevantnu dokumentaciju, uključujući relevantnu korespondenciju i nalaze Europske komisije. U slučaju složenog pravnog okvira trebalo bi uključiti sva izvješća o razini zaštite podataka u trećoj zemlji ili međunarodnoj organizaciji. Informacije koje dostavlja Europska komisija trebale bi u svakom slučaju biti iscrpne i Europski odbor za zaštitu podataka trebao bi zahvaljujući njima biti u mogućnosti provesti vlastitu procjenu razine zaštite podataka u trećoj zemlji. Europski odbor za zaštitu podataka pravodobno dostavlja mišljenje o nalazima Europske komisije i utvrđuje moguće nedostatke okvira primjerenosti. Europski odbor za zaštitu podataka ujedno nastoji predlagati izmjene ili dopune kako bi se riješili mogući nedostaci.

U skladu s člankom 45. stavkom 4. Opće uredbe o zaštiti podataka, Europska komisija dužna je kontinuirano pratiti razvoj događaja koji bi mogli utjecati na funkcioniranje odluke o primjerenosti.

Člankom 45. stavkom 3. Opće uredbe o zaštiti podataka propisano je da se periodično preispitivanje provodi najmanje svake četiri godine. No, to je općeniti vremenski okvir koji se odlukom o primjerenosti mora prilagoditi svakoj trećoj zemlji ili međunarodnoj organizaciji. Ovisno o postojanju posebnih okolnosti može se odobriti kraći ciklus preispitivanja. Osim toga, incidenti ili druge informacije o pravnom okviru predmetne treće zemlje ili međunarodne organizacije ili promjene u tom pravnom okviru mogu dovesti do potrebe za ranijim preispitivanjem. Ujedno se čini prikladnim da se prvo preispitivanje potpuno nove odluke o primjerenosti provede relativno rano i da se ciklus preispitivanja postupno prilagođava ovisno o ishodu.

S obzirom na zadatak da Europskoj komisiji dostavi mišljenje o tome jesu li treća zemlja, područje ili jedno ili više određenih sektora unutar te treće zemlje ili međunarodna organizacija prestali osiguravati primjerenu razinu zaštite, Europski odbor za zaštitu podataka mora pravodobno primiti smislene informacije povezane s praćenjem relevantnih razvoja događaja u toj trećoj zemlji ili međunarodnoj organizaciji koje provodi Europska komisija. Stoga bi trebalo redovito obavješćivati Europski odbor za zaštitu podataka o svim postupcima preispitivanja i misijama preispitivanja u trećoj zemlji ili međunarodnoj organizaciji. Europski odbor za zaštitu podataka cijenio bi da ga se poziva da sudjeluje u tim postupcima i misijama preispitivanja.

Treba napomenuti i da Europska komisija na temelju članka 45. stavka 5. Opće uredbe o zaštiti podataka ima pravo stavljati izvan snage, mijenjati ili suspendirati odluke o primjerenosti. U postupak stavljanja izvan snage, mijenjanja ili suspenzije stoga mora biti uključen Europski odbor za zaštitu podataka na način da se zatraži njegovo mišljenje u skladu s člankom 70. stavkom 1.

Nadalje, kao što je prepoznato u članku 58. stavku 5. Opće uredbe o zaštiti podataka i u skladu s presudom Suda Europske unije u predmetu Schrems, tijela za zaštitu podataka trebala bi moći sudjelovati u pravnom postupku ako zaključe da je zahtjev neke osobe protiv odluke o primjerenosti osnovan: „U tom je pogledu nacionalni zakonodavac dužan predvidjeti pravna sredstva koja neovisnom nadzornom tijelu omogućavaju isticanje prigovora pred nacionalnim sudovima koje smatra osnovanima, kako bi ti sudovi mogli, u slučaju da dijele sumnje tog tijela u vezi s valjanošću Komisijine odluke, uputiti zahtjev za prethodnu odluku radi ispitivanja valjanosti te odluke.”¹¹

¹¹ Predmet C-362/14, Maximillian Schrems protiv Data Protection Commissioner, 6. listopada 2015. (točka 65.).

Poglavlje 3.: Temeljna opća načela zaštite podataka kako bi se osiguralo da je razina zaštite u trećoj zemlji, području ili jednom ili više određenih sektora unutar te treće zemlje ili u međunarodnoj organizaciji u načelu istovjetna onoj koja je zajamčena zakonodavstvom EU-a

Sustav koji postoji u trećoj zemlji ili međunarodnoj organizaciji mora sadržavati sljedeća sadržajna i postupovna/provedbena načela i mehanizme zaštite podataka:

A. Sadržajna načela:

1) Koncepti

Trebali bi postojati osnovni pojmovi i/ili načela u vezi sa zaštitom podataka. Ne moraju biti istovjetni terminologiji iz Opće uredbe o zaštiti podataka, no trebali bi odražavati pojmove sadržane u europskom pravu o zaštiti podataka i biti usklađeni s njima. Na primjer, Opća uredba o zaštiti podataka uključuje sljedeće važne pojmove: „osobni podaci”, „obrada osobnih podataka”, „voditelj obrade podataka”, „izvršitelj obrade podataka”, „primatelj” i „osjetljivi podaci”.

2) Osnove za zakonitu i pravednu obradu u legitimne svrhe

Podaci se moraju obrađivati na zakonit, pravedan i legitiman način.

Legitimne osnove, na temelju kojih se osobni podaci mogu obrađivati zakonito, pravedno i legitimno, trebale bi biti utvrđene dovoljno jasno. U europskom okviru priznaje se nekoliko takvih legitimnih osnova koje primjerice uključuju odredbe u nacionalnom pravu, privolu ispitanika, izvršavanje ugovora ili legitimnog interesa voditelja obrade podataka ili treće strane koji ne nadvladavaju interese pojedinca.

3) Načelo ograničenja svrhe

Podaci bi se trebali obrađivati u određenu svrhu i zatim se upotrebljavati samo ako to nije protivno svrsi obrade.

4) Načelo kvalitete podataka i proporcionalnosti

Podaci bi trebali biti točni i, kad je to potrebno, ažurirani. Podaci bi trebali biti primjereni, relevantni i ne preopsežni u odnosu na svrhu radi koje se prikupljaju.

5) Načelo zadržavanja podataka

Podaci se u pravilu ne bi trebali čuvati duže nego što je potrebno u odnosu na potrebe radi kojih se osobni podaci obrađuju.

6) Načelo sigurnosti i povjerljivosti

Svako tijelo koje obrađuje osobne podatke trebalo bi osigurati da se podaci obrađuju na način kojim se osigurava sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade i od slučajnog gubitka, uništenja ili oštećenja, primjenom odgovarajućih tehničkih ili organizacijskih mjera. Kad je riječ o razini sigurnosti, trebalo bi uzeti u obzir najnovija dostignuća i povezane troškove.

7) Načelo transparentnosti

Svakog bi pojedinca trebali obavijestiti o glavnim elementima obrade njegovih/njezinih osobnih podataka na jasan, lako dostupan, sažet, transparentan i razumljiv način. Takve bi informacije trebale uključivati svrhu obrade, identitet voditelja obrade podataka, prava koja su mu/joj omogućena i ostale informacije ako je to potrebno kako bi se osigurala pravednost. Pod određenim uvjetima mogu postojati neke iznimke od tog prava na informacije, primjerice kad je potrebno zaštititi kaznene istrage, nacionalnu sigurnost, neovisnost pravosuđa i sudskih postupaka ili druge važne ciljeve od općeg javnog interesa, kao što je navedeno u članku 23. Opće uredbe o zaštiti podataka.

8) Pravo na pristup, ispravak, brisanje i prigovor

Ispitanik bi trebao imati pravo dobiti potvrdu o tome provodi li se obrada podataka koja se odnosi na njega/nju, ali i pravo na pristup svojim podacima, što uključuje dobivanje kopije svih podataka koji se obrađuju, a odnose se na njega/nju.

Ispitanik bi prema potrebi trebao imati pravo na ispravak svojih podataka na temelju određenih razloga, primjerice ako se pokaže da su netočni ili nepotpuni, ali i pravo na brisanje podataka ako primjerice njihova obrada više nije potrebna ili ako je nezakonita.

Ispitanik bi na temelju uvjerljivih legitimnih razloga koji se odnose na njegovu posebnu situaciju u svakom trenutku trebao imati pravo uložiti prigovor na obradu svojih podataka pod određenim uvjetima utvrđenima u pravnom okviru treće zemlje. Takvi uvjeti u Općoj uredbi o zaštiti podataka primjerice uključuju situaciju kad je obrada nužna radi izvršavanja zadaće koja se obavlja u javnom interesu ili kad je nužna radi izvršavanja službene dužnosti povjerene voditelju obrade ili za potrebe legitimnih interesa voditelja obrade podataka ili treće strane.

Iskorištavanje tih prava ne bi trebalo biti pretjerano složeno za ispitanika. Moguća ograničenja tih prava mogla bi primjerice postojati kako bi se zaštitile kaznene istrage, nacionalna sigurnost, neovisnost pravosuđa i sudski postupci ili drugi važni ciljevi od općeg javnog interesa, kao što je navedeno u članku 23. Opće uredbe o zaštiti podataka.

9) Ograničenja daljnjeg prijenosa

Daljnji prijenosi osobnih podataka koje provodi prvi primatelj prvotnog prijenosa podataka trebali bi biti dopušteni samo ako daljnji primatelj (tj. primatelj daljnjeg prijenosa) isto tako podliježe pravilima (uključujući ugovorna pravila) kojima se omogućava primjerena razina zaštite i ako pri obradi podataka u ime voditelja obrade podataka slijedi odgovarajuće upute. Daljnjim se prijenosom ne smije narušiti razina zaštite fizičkih osoba čiji se podaci prenose. Prvi primatelj podataka prenesenih iz EU-a dužan je u nedostatku odluke o primjerenosti osigurati prikladne zaštitne mjere za daljnje prijenose podataka. Takvi daljnji prijenosi podataka trebali bi se provoditi samo u ograničene i određene svrhe i dokle god postoji pravna osnova za tu obradu.

B. Primjeri dodatnih sadržajnih načela koja se primjenjuju na određene oblike obrade:

1) Posebne kategorije podataka

Trebale bi postojati posebne zaštitne mjere ako su obuhvaćene „posebne kategorije” podataka.¹² Te bi kategorije trebale odgovarati onima sadržanima u člancima 9. i 10. Opće uredbe o zaštiti podataka. Ta bi zaštita trebala biti uspostavljena strožim zahtjevima za obradu podataka, primjerice zahtjevom da ispitanik daje izričitu privolu za obradu ili dodatnim sigurnosnim mjerama.

¹² U uvodnoj izjavi 10. Opće uredbe o zaštiti podataka te se posebne kategorije nazivaju i „osjetljivim podacima”.

2) Izravni marketing

Ako se podaci obrađuju za potrebe izravnog marketinga, ispitanik bi u bilo koje vrijeme i besplatno trebao imati pravo uložiti prigovor na obradu svojih podataka u takve svrhe.

3) Automatizirane odluke i izrada profila

Odluke koje se temelje isključivo na automatiziranoj obradi (automatizirano pojedinačno donošenje odluka), uključujući izradu profila, te koje proizvode pravne učinke ili znatno utječu na ispitanika mogu se dopustiti samo pod određenim uvjetima utvrđenima u pravnom okviru treće zemlje. Takvi uvjeti u europskom okviru primjerice uključuju potrebu za dobivanjem izričite privole ispitanika ili nužnost takve odluke radi sklapanja ugovora. Ako odluka nije u skladu s tim uvjetima koji su utvrđeni u pravnom okviru treće zemlje, ispitanik bi trebao imati pravo da se na njega ta odluka ne odnosi. U pravu treće zemlje u svakom bi slučaju trebale biti predviđene potrebne zaštitne mjere, uključujući pravo na dobivanje informacija o obrazloženju odluke i popratnoj logici, na ispravak netočnih ili nepotpunih informacija i na osporavanje odluke ako je donesena na netočnoj činjeničnoj osnovi.

C. Postupovni i provedbeni mehanizmi:

Iako se pravna sredstva kojima se koristi treća zemlja za osiguravanje primjerene razine zaštite mogu razlikovati od onih koja se provode u Europskoj uniji,¹³ sustav koji je usklađen s europskim mora sadržavati sljedeće elemente:

1) Nadležno neovisno nadzorno tijelo

U trećoj bi zemlji trebalo postojati najmanje jedno neovisno nadzorno tijelo čija je zadaća praćenje, osiguravanje i provođenje poštovanja odredbi o zaštiti podataka i privatnosti. Nadzorno tijelo djeluje potpuno neovisno i nepristrano u obavljanju svojih dužnosti i izvršavanju svojih ovlasti, a pritom ne traži i ne prihvaća upute. Nadzorno tijelo u tom bi kontekstu trebalo imati sve potrebne i dostupne ovlasti i misije radi osiguravanja usklađenosti s pravima na zaštitu podataka i promicanja osviještenosti. Trebalo bi isto tako uzeti u obzir osoblje i proračun nadzornog tijela. Nadzorno bi tijelo ujedno trebalo biti u mogućnosti provoditi istrage na vlastitu inicijativu.

2) Sustavom zaštite podataka mora se osigurati dobra razina usklađenosti

Treća zemlja trebala bi osigurati visok stupanj odgovornosti i svijesti među voditeljima obrade podataka i onima koji u njihovo ime obrađuju osobne podatke o njihovim obvezama, zadaćama i odgovornostima, a među ispitanicima o njihovim pravima i načinima za ostvarivanje tih prava. Postojanje učinkovitih i odvraćajućih sankcija može imati važnu ulogu u osiguravanju poštovanja pravila, a to se, naravno, može postići i sustavima izravne provjere koju provode nadležna tijela, revizori ili neovisni službenici za zaštitu podataka.

3) Odgovornost

Okvirom za zaštitu podataka treće zemlje trebalo bi obvezati voditelje obrade podataka i one koji u njihovo ime obrađuju osobne podatke da se s njime usklade i da budu u mogućnosti dokazati da su usklađeni s njime, posebno nadležnom nadzornom tijelu. Takve mjere primjerice mogu uključivati procjene učinka na zaštitu podataka, vođenje evidencije ili datoteka zapisnika o aktivnostima obrade podataka tijekom odgovarajućeg vremenskog razdoblja, imenovanje službenika za zaštitu podataka ili tehničku i integriranu zaštitu podataka.

¹³ Predmet C-362/14, Maximilian Schrems protiv Data Protection Commissioner, 6. listopada 2015., točka 74.

4) Sustavom zaštite podataka mora se pružiti potpora i pomoć pojedinačnim ispitanicima u ostvarivanju njihovih prava i odgovarajućih mehanizama sudske pomoći

Pojedinac bi trebao biti u mogućnosti ulagati pravne lijekove kako bi brzo i djelotvorno ostvario svoja prava, i to bez pretjeranih troškova, ali i kako bi se osigurala usklađenost. Da bi to mogao učiniti, moraju postojati mehanizmi nadzora kojima se omogućava neovisno istraživanje pritužbi i mogućnost da se sva kršenja prava na zaštitu podataka i poštovanje privatnog života utvrde i kazne u praksi.

Ako se ne poštuju pravila, ispitaniku bi trebalo isto tako pružiti djelotvornu upravnu i sudsku pomoć, uključujući naknadu štete nastale kao rezultat nezakonite obrade njegovih osobnih podataka. To je ključni element u koji se mora uključiti sustav neovisnog sudskog odlučivanja ili arbitraže kojim se omogućava plaćanje naknade i određivanje kazni prema potrebi.

Poglavlje 4.: Ključna jamstva u trećim zemljama za pristup podacima za potrebe izvršavanja zakonodavstva i nacionalne sigurnosti kako bi se ograničilo zadiranje u temeljna prava

Komisija je dužna, u skladu s člankom 45. stavkom 2. točkom (a), pri procjeni primjerenosti razine zaštite uzeti u obzir „relevantno zakonodavstvo, i opće i sektorsko, što uključuje zakonodavstvo o javnoj sigurnosti, obrani, nacionalnoj sigurnosti, kaznenom pravu i pristupu tijela javne vlasti osobnim podacima, kao i provedbu tog zakonodavstva [...]”.

Sud Europske unije napomenuo je sljedeće u predmetu Schrems: „izraz ‚odgovarajuća razina zaštite‘ mora se shvatiti na način da zahtijeva da ta treća zemlja djelotvorno osigura, temeljem domaćeg zakonodavstva ili međunarodnih obveza koje je preuzela, razinu zaštite temeljnih prava i sloboda koja je bitno ekvivalentna onoj zaštiti koja se jamči u okviru Unije na temelju Direktive 95/46, tumačene u svjetlu Povelje”. Iako se u tom smislu sredstva kojima se služi treća zemlja mogu razlikovati od onih koja se primjenjuju u Europskoj uniji, ta se sredstva u praksi ipak moraju pokazati djelotvornima.¹⁴

Sud je u tom kontekstu ujedno kritizirao prijašnju Odluku o „sigurnoj luci” koja „ne sadržava nikakvo utvrđenje o postojanju državnih pravila SAD-a za ograničavanje mogućih miješanja u temeljna prava osoba čiji se podaci prenose iz Unije u SAD, miješanja koja su državna tijela te zemlje ovlaštena provoditi kada slijede legitimne ciljeve kao što je to nacionalna sigurnost.”

Radna skupina iz članka 29. utvrdila je u mišljenju iz Radnog dokumenta 237, donesenom 13. travnja 2016., ključna jamstva koja odražavaju sudsku praksu Suda Europske unije i Europskog suda za ljudska prava u području nadzora. Iako su preporuke iz Radnog dokumenta 237 i dalje valjane i trebalo bi ih uzeti u obzir pri procjeni primjerenosti treće zemlje u području nadzora, primjena tih jamstava može se razlikovati u područjima pristupa podacima za potrebe izvršavanja zakonodavstva i nacionalne sigurnosti. Sve treće zemlje svejedno trebaju poštovati ta četiri jamstva u pogledu pristupa podacima kako bi ih se smatralo primjerenima, bez obzira na to pristupa li se podacima za potrebe nacionalne sigurnosti ili za potrebe izvršavanja zakonodavstva:

- 1) Obrada bi se trebala temeljiti na jasnim, preciznim i pristupačnim pravilima (pravna osnova)**
- 2) Treba dokazati nužnost i proporcionalnost u pogledu legitimnih ciljeva**
- 3) Obrada mora podlijegati neovisnom nadzoru**
- 4) Pojedincima moraju biti dostupni učinkoviti pravni lijekovi**

¹⁴ Predmet C-362/14, Maximilian Schrems protiv Data Protection Commissioner, 6. listopada 2015., točka 74.