Preporuke

Preporuke 01/2021 o kriteriju primjerenosti u skladu s Direktivom o zaštiti podataka pri izvršavanju zakonodavstva

Doneseno 2. veljače 2021.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Povijest verzija

Verzija 1.1.	6. srpnja 2021.	Promjena formatiranja
Verzija 1.0	2. veljače 2021.	Donošenje preporuka

Sadržaj

Europski odbor za zaštitu podataka,

uzimajući u obzir članak 51. stavak 1. točku (b) Direktive (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP[1],

uzimajući u obzir članke 12. i 22. svojeg poslovnika,

DONIO JE SLJEDEĆE PREPORUKE:

1. UVOD

1. Radna skupina iz članka 29. (RS29) objavila je radni referentni dokument[2] o primjerenosti u skladu s Općom uredbom o zaštiti podataka (GDPR)[3]. Taj radni dokument podržao je Europski odbor za zaštitu podataka na svojoj prvoj plenarnoj sjednici.

2. Kako je navedeno u Izjavi br. 21 priloženoj Ugovoru iz Lisabona, posebna pravila o zaštiti osobnih podataka i slobodnom kretanju takvih podataka u područjima pravosudne suradnje u kaznenim predmetima i policijske suradnje na temelju članka 16. Ugovora o funkcioniranju Europske unije mogu se pokazati potrebnima zbog posebne naravi tih područja.

3. Na toj je osnovi zakonodavac EU-a donio Direktivu (EU) 2016/680 (Direktivu o zaštiti podataka pri izvršavanju zakonodavstva, dalje u tekstu „Direktiva o zaštiti podataka") kojom se utvrđuju posebna pravila u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe **sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti**.

4. U Direktivi o zaštiti podataka utvrđuju se razlozi na osnovi kojih se može omogućiti prijenos osobnih podataka trećoj zemlji ili međunarodnoj organizaciji u tom kontekstu. Jedan od razloga za takav prijenos jest odluka Europske komisije da predmetna treća zemlja ili međunarodna organizacija mora osigurati odgovarajuću razinu zaštite.

5. Dok se radnim referentnim dokumentom o primjerenosti WP254.rev01 nastoje pružiti smjernice Europskoj komisiji o razini zaštite podataka u trećim zemljama i međunarodnim organizacijama u skladu s Općom uredbom o zaštiti podataka, ovim se dokumentom nastoje pružiti slične smjernice u skladu s Direktivom o zaštiti podataka. U njemu se u tom kontekstu utvrđuju temeljna načela zaštite podataka koja moraju postojati u pravnom okviru treće zemlje ili međunarodne

[1] SL L 119, 4.5.2016., str. 89.
[2] WP254.rev01 koji je 28. studenoga 2017. donijela Radna skupina iz članka 29. kako je posljednji put revidiran i donesen 6. veljače 2018. Njime se ažurira poglavlje I. radnog dokumenta „Prijenosi osobnih podataka trećim zemljama: Primjena članaka 25. i 26. Direktive EU-a o zaštiti podataka", RS12, koji je 24. srpnja 1998. donijela Radna skupina iz članka 29.
[3] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 26. 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 (GDPR)), SL L 119, 4.5.2016., str. 1.

organizacije kako bi se osigurala bitna ekvivalentnost s okvirom EU-a u području primjene Direktive o zaštiti podataka (tj. za obradu osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija). Osim toga, može poslužiti kao vodič trećim zemljama i međunarodnim organizacijama koje su zainteresirane za postizanje primjerenosti.

6. Ovaj je dokument usmjeren isključivo na odluke o primjerenosti. One su provedbeni akti Europske komisije u skladu s člankom 36. stavkom 3. Direktive o zaštiti podataka.

2. POJAM PRIMJERENOSTI

7. Direktivom o zaštiti podataka utvrđuju se pravila za prijenos osobnih podataka trećim zemljama i međunarodnim organizacijama u mjeri u kojoj su takvi prijenosi obuhvaćeni njezinim područjem primjene. Pravila o međunarodnim prijenosima osobnih podataka utvrđena su u poglavlju V. Direktive o zaštiti podataka, a posebno u njezinim člancima od 35. do 39.

8. U skladu s člankom 36. Direktive o zaštiti podataka, prijenosi podataka u treću zemlju ili međunarodnu organizaciju mogući su ako treća zemlja, područje ili jedan ili više određenih sektora unutar treće zemlje ili međunarodna organizacija osigurava primjerenu razinu zaštite. Iz sudske prakse Suda Europske unije[4] proizlazi da se ta odredba mora tumačiti u vezi s člankom 35. Direktive o zaštiti podataka, koji se naziva „Opća načela za prijenose osobnih podataka" i određuje da „[s]ve odredbe [iz poglavlja V. Direktive o zaštiti podataka] primjenjuju se kako bi se osiguralo da se ne ugrozi razina zaštite pojedinaca osigurana ovom Direktivom".

9. Ako Europska komisija odluči da je takva primjerena razina zaštite osigurana, mogući su prijenosi osobnih podataka u tu treću zemlju, područje, sektor ili međunarodnu organizaciju, bez posebnog odobrenja, osim ako druga država članica iz koje su podaci dobiveni mora dati svoje odobrenje za prijenos kako je propisano člancima 35. i 36. te uvodnom izjavom 66. Direktive o zaštiti podataka. Time se ne dovodi u pitanje potreba da tijela dotičnih država članica moraju obrađivati podatke u skladu s nacionalnim odredbama donesenima na temelju Direktive (EU) 2016/680.

10. Taj pojam „primjerene razine zaštite" koji je već postojao u Direktivi 95/46[5] i Okvirnoj odluci Vijeća 2008/977/PUP[6] Sud EU-a dodatno je razradio u tom kontekstu, a nedavno u okviru Opće uredbe o zaštiti podataka.

11. Kako je naveo Sud EU-a, dok razina zaštite u trećoj zemlji mora biti bitno ekvivalentna onoj zaštiti koja se jamči u EU-u, „pravna sredstva kojima se koristi treća zemlja za osiguranje takve razine zaštite mogu [se] razlikovati od onih koja se provode u Uniji", ali „ta se sredstva ipak moraju u praksi pokazati djelotvornima"[7]. Stoga se standardom primjerenosti ne zahtijeva da se zakonodavstvo EU-a preslika točku po točku, nego da se uvedu bitni, odnosno osnovni, zahtjevi tog zakonodavstva.

---

[4] Predmet C-311/18, Data Protection Commissioner protiv Facebook Ireland Limited i Maximillian Schrems, 16. srpnja 2020., ECLI:EU:C:2020:559, t. 92. (Schrems II.).
[5] Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, SL L 281, 23.11.1995., str. 31.
[6] Okvirna odluka Vijeća 2008/977/PUP od 27. studenoga 2008. o zaštiti osobnih podataka obrađenih u okviru policijske i pravosudne suradnje u kaznenim stvarima, SL L 350, 30.12.2008., str. 60.
[7] Predmet C-362/14, Maximillian Schrems protiv Data Protection Commissioner, 6. listopada 2015., ECLI:EU:C:2015:650, t. 73. i 74. (Schrems I.).

12. U tom kontekstu Sud je također pojasnio da bi odluka Komisije o primjerenosti trebala sadržavati utvrđenje o postojanju državnih pravila treće zemlje za ograničavanje mogućih miješanja u temeljna prava osoba čiji se podaci prenose iz Europske unije u tu treću zemlju, miješanja koja su državna tijela te zemlje *ovlaštena* provoditi kada slijede legitimne ciljeve kao što je to nacionalna sigurnost[8].

13. Svrha je odluka Komisije o primjerenosti službeno potvrditi, uz obvezujuće učinke za države članice[9], uključujući njihova nadležna tijela za zaštitu podataka[10], da je razina zaštite podataka u trećoj zemlji ili međunarodnoj organizaciji bitno ekvivalentna razini zaštite podataka u Europskoj uniji. Treća bi zemlja trebala ponuditi jamstva kojima se osigurava primjerena razina zaštite, u osnovi istovjetna onoj koja je osigurana u Uniji, osobito ako se podaci obrađuju u jednom ili više posebnih sektora.[11]

14. 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. Međutim, 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 takvih pravila. Učinkoviti mehanizmi provedbe iznimno su važni za djelotvornost pravila o zaštiti podataka.[12]

3. POSTUPOVNI ASPEKTI ZAKLJUČAKA O PRIMJERENOSTI U SKLADU S DIREKTIVOM O ZAŠTITI PODATAKA

15. Kako bi ispunio svoju zadaću u pogledu savjetovanja Europske komisije u skladu s člankom 51. stavkom 1. točkom (g) Direktive o zaštiti podataka, Europski odbor za zaštitu podataka trebao bi zaprimiti svu relevantnu dokumentaciju, uključujući relevantnu korespondenciju i nalaze Europske komisije. Prijeko je potrebno da se svi relevantni dokumenti prevedu na engleski i Europskom odboru za zaštitu podataka dostave dovoljno rano kako bi se prije konačnog donošenja odluka o primjerenosti mogle održati korisne rasprave utemeljene na informacijama. 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 moći ocijeniti analizu Komisije u pogledu razine zaštite podataka u trećoj zemlji ili međunarodnoj organizaciji.

16. Europski odbor za zaštitu podataka pravodobno će dostaviti mišljenje o nalazima Europske komisije, u kojem će utvrditi moguće nedostatke okvira primjerenosti te, prema potrebi, dati moguće preporuke.

---

[8] Schrems I., t. 88.
[9] Članak 288. UFEU-a.
[10] Schrems I., t. 52.
[11] Uvodna izjava 67. Direktive o zaštiti podataka.
[12] Schrems I., t. 72. – 74. i Mišljenje Suda EU-a 1/15 o Prijedlogu sporazuma između Kanade i Europske unije, 26. srpnja 2017., ECLI:EU:C:2017:592 (Mišljenje 1/15), t. 134.: „To pravo na zaštitu osobnih podataka zahtijeva, među ostalim, kontinuitet visoke razine zaštite temeljnih prava i sloboda predviđenih pravom Unije u slučaju prijenosa osobnih podataka iz Unije u treću zemlju. Iako se sredstva za osiguranje takve razine zaštite mogu razlikovati od onih koja se provode u Uniji kao jamstvo poštovanja zahtjeva koji proizlaze iz prava Unije, ona se u praksi ipak moraju pokazati djelotvornima za osiguranje bitno ekvivalentne zaštite poput one koja se jamči u okviru Unije".

17. U skladu s člankom 36. stavkom 4. Direktive o zaštiti podataka, Europska komisija mora kontinuirano pratiti razvoj događaja koji bi mogli utjecati na djelovanje odluka o primjerenosti.

18. Člankom 36. stavkom 3. Direktive o zaštiti podataka propisuje se da se periodično preispitivanje provodi najmanje svake četiri godine. Tu je, naime, riječ o općenitom vremenskom okviru koji se mora prilagoditi svakoj trećoj zemlji ili međunarodnoj organizaciji za koju se izdaje odluka o primjerenosti. Ovisno o postojanju posebnih okolnosti može se odobriti kraći ciklus preispitivanja. Osim toga, neočekivani događaji ili druge informacije o pravnom okviru predmetne treće zemlje ili međunarodne organizacije ili promjene tog pravnog okvira 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.

19. S obzirom na njegovu zadaću da Europskoj komisiji dostavi mišljenje o tome jesu li treća zemlja, područje ili jedan 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 Komisijinim praćenjem relevantnog razvoja događaja u toj trećoj zemlji ili međunarodnoj organizaciji. Stoga bi Europski odbor za zaštitu podataka trebalo redovito obavješćivati o svim postupcima preispitivanja i misijama preispitivanja u trećoj zemlji ili međunarodnoj organizaciji. Europski odbor za zaštitu podataka preporučuje da ga se pozove na sudjelovanje u tim postupcima i misijama preispitivanja, kako je bilo predviđeno u odluci o sustavu zaštite privatnosti i kako je predviđeno u odluci o primjerenosti koja se odnosi na Japan.

20. Treba napomenuti i da Europska komisija, u skladu s člankom 36. stavkom 5. Direktive o zaštiti podataka, ima ovlasti staviti izvan snage, izmijeniti ili suspendirati postojeće odluke o primjerenosti ako treća zemlja ili međunarodna organizacija više ne osigurava primjerenu razinu zaštite. Europski odbor za zaštitu podataka sudjeluje u postupku stavljanja izvan snage, izmjene ili suspenzije jer se u skladu s člankom 51. stavkom 1. točkom (g) Direktive o zaštiti podataka mora zatražiti njegovo mišljenje.

21. Nadalje, ne dovodeći u pitanje ovlasti tijela kaznenog progona, nadzorna tijela također bi trebala imati ovlast za obavješćivanje pravosudnih tijela o kršenjima ove Direktive ili za sudjelovanje u pravnim postupcima[13]. Iz presude Suda EU-a u predmetu Schrems I. posebno proizlazi da tijela za zaštitu podataka moraju moći sudjelovati u pravnom postupku pred nacionalnim sudovima ako smatraju da je zahtjev neke osobe protiv odluke o primjerenosti osnovan.[14] Presudom u predmetu Schrems II. potvrđena je ta procjena.[15]

[13] Vidjeti članak 47. stavak 5. Direktive o zaštiti podataka i njezinu uvodnu izjavu 82.

[14] Vidjeti predmet Schrems I., t.65.: „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."

[15] Vidjeti predmet Schrems II., t. 120.: „[...] čak i kada postoji Komisijina odluka o primjerenosti, nadležno nacionalno nadzorno tijelo, kojem je osoba podnijela pritužbu u vezi sa zaštitom svojih prava i sloboda u odnosu na obradu osobnih podataka koji se na nju odnose, mora biti u mogućnosti potpuno neovisno ispitati poštuje li prijenos tih podataka zahtjeve iz GDPR-a i, prema potrebi, pokrenuti postupak pred nacionalnim sudovima kako bi potonji, ako dijele sumnje tog tijela u valjanost odluke o primjerenosti, uputili zahtjev za prethodnu odluku u svrhu ispitivanja te valjanosti [...]".

4. STANDARDI EU-A ZA PRIMJERENOST U POLICIJSKOJ I PRAVOSUDNOJ SURADNJI U KAZNENIM STVARIMA

22. Kad je riječ o sadržaju, u odlukama o primjerenosti trebalo bi se usredotočiti na procjenu postojećeg zakonodavstva treće zemlje u cjelini, u teoriji i praksi, s obzirom na kriterije za procjenu utvrđene u članku 36. Direktive o zaštiti podataka. Sustav koji postoji u trećoj zemlji ili međunarodnoj organizaciji mora sadržavati sljedeća osnovna opća, postupovna i provedbena načela i mehanizme zaštite podataka.

23. Člankom 36. stavkom 2. Direktive o zaštiti podataka utvrđeni su elementi koje Europska komisija uzima u obzir pri procjeni primjerenosti razine zaštite u trećoj zemlji i međunarodnoj organizaciji.

24. Konkretno, Komisija uzima u obzir vladavinu prava, poštovanje ljudskih prava i temeljnih sloboda[16], relevantno zakonodavstvo te provedbu takvog zakonodavstva, djelotvorna i provediva prava ispitanika te djelotvornu administrativnu i sudsku zaštitu ispitanika čiji se osobni podaci prenose, postojanje i djelotvorno funkcioniranje jednog neovisnog nadzornog tijela ili više njih i međunarodne obveze koje je treća zemlja ili međunarodna organizacija preuzela.

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

26. Srž općih načela te postupovnih i 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 (Povelja) i Direktive o zaštiti podataka. 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 koje se konkretno odnose na pravo na zaštitu podataka u području izvršavanja zakonodavstva. Treća bi zemlja trebala ponuditi jamstva kojima se osigurava primjerena razina zaštite, u osnovi istovjetna onoj koja je osigurana u Uniji. Te odredbe moraju biti provedive.

27. Nadalje, u pogledu načela proporcionalnosti[17], Sud EU-a presudio je da u pogledu zakona država članica mogućnost da se opravda ograničenje prava na privatnost i zaštitu podataka treba, s jedne strane, ocijeniti tako da se odmjeri **ozbiljnost zadiranja** takvog ograničenja[18] i, s druge strane,

[16] Pri procjeni pravnog okvira treće zemlje trebalo bi uzeti u obzir mogućnost izricanja smrtne kazne ili bilo kojeg oblika okrutnog i nečovječnog postupanja na temelju podataka prenesenih iz EU-a. Konkretno, ako je takva kazna ili postupanje predviđeno pravom treće zemlje, trebalo bi pronaći dodatne zaštitne mjere u pravnom okviru treće zemlje kako bi se osiguralo da se podaci preneseni iz EU-a ne upotrebljavaju za traženje, izricanje ili izvršenje smrtne kazne ili bilo kakvog oblika okrutnog i nečovječnog postupanja (npr. međunarodni sporazum kojim se određuju uvjeti za prijenos, obveza treće zemlje da neće izreći smrtnu kaznu ili upotrijebiti bilo kakav oblik okrutnog i nečovječnog postupanja na temelju podataka prenesenih iz EU-a, ili moratorij na izvršavanje smrtne kazne).

[17] Članak 52. stavak 1. Povelje.

[18] Sud je, na primjer, primijetio da „za zadiranje, koje podrazumijeva prikupljanje podataka u stvarnom vremenu koji omogućuju određivanje lokacije terminalne opreme, proizlazi da je osobito ozbiljno jer se tim podacima daje nacionalnim nadležnim tijelima precizno i trajno sredstvo za praćenje kretanja korisnika prijenosnih telefona [...]” (spojeni predmeti C-511/18, C-512/18 i C-520/18, La Quadrature du Net i drugi, 6. listopada 2020., ECLI:EU:C:2020:791, t. 187., uključujući navedenu sudsku praksu).

provjeri da je **važnost cilja od općeg interesa** koji se nastoji postići tim ograničenjem povezana s tom ozbiljnošću[19].

28. Prema sudskoj praksi Suda EU-a, pravna osnova kojom se dopušta zadiranje u temeljna prava mora, u skladu s načelom proporcionalnosti, definirati doseg ograničenja ostvarivanja dotičnog prava[20]. Odstupanja od zaštite osobnih podataka i njezina ograničenja moraju biti u granicama onog što je strogo nužno[21]. Kako bi se ispunio taj zahtjev, osim predviđanja jasnih i preciznih pravila kojima se uređuju doseg i primjena predmetne mjere, predmetnim propisom moraju se naložiti minimalne zaštitne mjere, tako da osobe čiji su podaci preneseni raspolažu dostatnim jamstvima koja omogućuju djelotvornu zaštitu njihovih osobnih podataka od rizika zlouporabe. U njemu se mora osobito navesti u kojim se okolnostima i pod kojim uvjetima može donijeti mjera kojom se predviđa obrada takvih podataka, na taj način osiguravajući da zadiranje bude ograničeno na ono što je strogo nužno. Nužnost posjedovanja takvih jamstava još je značajnija kad su osobni podaci podvrgnuti automatskoj obradi[22].

29. Europski odbor za zaštitu podataka donio je preporuke kojima se utvrđuju ključna jamstva koja odražavaju sudsku praksu Suda EU-a i Europskog suda za ljudska prava (ESLJP) u području nadzora i koja treba pronaći u pravu treće zemlje pri procjeni zadiranja takvih nadzornih mjera treće zemlje u prava ispitanika u slučaju prijenosa podataka u tu treću zemlju u skladu s Općom uredbom o zaštiti podataka.[23] Da bi se procijenilo jesu li ispunjeni uvjeti iz članka 36. stavka 2. točke (a) Direktive o zaštiti podataka, Europski odbor za zaštitu podataka smatra da se jamstva utvrđena u tim preporukama moraju uzeti u obzir pri procjeni primjerenosti treće zemlje u skladu s Direktivom o zaštiti podataka u području nadzora, imajući na umu dodatne posebne uvjete u području nadzora u tom kontekstu.

30. U pogledu zahtjeva iz članka 36. stavka 2. točke (b), treća zemlja ne bi trebala samo osigurati učinkovit neovisan nadzor zaštite podataka, nego i mehanizme suradnje s tijelima država članica za zaštitu podataka.[24]

31. U pogledu zahtjeva iz članka 36. stavka 2. točke (c), osim međunarodnih obveza koje su treća zemlja ili međunarodna organizacija preuzele, također bi trebalo uzeti u obzir obveze koje proizlaze iz sudjelovanja treće zemlje ili međunarodne organizacije u multilateralnim ili regionalnim sustavima, posebno u odnosu na zaštitu osobnih podataka, kao i provedbu tih obveza. Posebno bi trebalo uzeti u obzir pristupanje treće zemlje drugim međunarodnim sporazumima o zaštiti podataka, npr. Konvenciji Vijeća Europe od 28. siječnja 1981. o zaštiti pojedinaca vezanoj uz automatsku obradu osobnih podataka te njezinu Dodatnom protokolu (Konvenciji 108[25] i njezinoj ažuriranoj verziji, Konvenciji 108+). Osim toga, u obzir se može uzeti i usklađenost treće zemlje s načelima sadržanima u međunarodnim dokumentima kao što je Praktični vodič Vijeća Europe o upotrebi osobnih podataka u sektoru policije – Kako zaštititi osobne podatke u borbi protiv kriminala (*Practical Guide on the use of personal data in the police sector: how to protect personal data while combatting crime*).

32. Odlukom o primjerenosti trebalo bi se osigurati da strani sustav u cjelini putem sadržaja prava na privatnost i zaštitu podataka te u okviru njihove učinkovite provedbe, nadzora i izvršenja pruža

[19] La Quadrature du Net i drugi, t. 131.
[20] Predmet Schrems II., t. 180.
[21] Predmet Schrems II., t. 176, uključujući navedenu sudsku praksu.
[22] Predmet Schrems II., t. 176, uključujući navedenu sudsku praksu.
[23] Preporuke Europskog odbora za zaštitu podataka 02/2020 o europskim temeljnim jamstvima za mjere nadzora, donesene 10. studenoga 2020.
[24] Uvodna izjava 67. Direktive o zaštiti podataka.
[25] Uvodna izjava 68. Direktive o zaštiti podataka.

potrebnu razinu zaštite, uključujući za podatke u tranzitu u tu treću zemlju. Kako je Sud EU-a istaknuo u presudi u predmetu Schrems II., visoka razina zaštite osobnih podataka treba se osigurati i pri prijenosu tih podataka u treću zemlju.[26]

33. Konačno, pri donošenju odluke o primjerenosti samo u vezi s područjem ili posebnim sektorom u trećoj zemlji, Europska komisija trebala bi uzeti u obzir jasne i objektivne kriterije, kao što su upućivanje na specifične aktivnosti obrade ili područje primjene mjerodavnih zakonskih standarda i zakonodavstva koji su na snazi u trećoj zemlji.[27]

A. Opća načela i zaštitne mjere

a) Pojmovi

34. Trebali bi postojati osnovni pojmovi u vezi sa zaštitom podataka. Ne moraju biti istovjetni terminologiji iz Direktive o zaštiti podataka, ali trebali bi odražavati pojmove sadržane u europskom pravu o zaštiti podataka i biti usklađeni s njima. Na primjer, u Direktivi o zaštiti podataka javljaju se sljedeći važni pojmovi: „osobni podaci", „obrada osobnih podataka", „nadležna tijela", „voditelj obrade podataka", „izvršitelj obrade podataka", „primatelj", „osjetljivi podaci", „točnost", „izrada profila", „tehnička i integrirana zaštita podataka", „nadzorno tijelo" i „pseudonimizacija".

b) Obrada osobnih podataka – zakonita i poštena (članak 4. i uvodna izjava 26.)

35. U skladu s člankom 8. stavkom 2. Povelje osobni podaci trebali bi se, među ostalim, obrađivati „u utvrđene svrhe i na temelju suglasnosti osobe o kojoj je riječ, ili na nekoj drugoj legitimnoj osnovi utvrđenoj zakonom".[28] Međutim, u kontekstu izvršavanja zakonodavstva, treba napomenuti da obavljanje zadaća sprečavanja, istraživanja, otkrivanja ili kaznenog progona kaznenih djela institucionalno zakonom dodijeljenih nadležnim tijelima omogućuje tim tijelima da od pojedinaca smiju zatražiti da ispune zahtjeve ili to im narediti. U takvom slučaju privola ispitanika ne bi smjela biti pravna osnova za obradu osobnih podataka od strane nadležnih tijela.[29]

36. Tom sudskom praksom trebala bi se predvidjeti jasna i precizna pravila kojima se uređuju doseg i primjena relevantnih aktivnosti obrade podataka i određuju i nalažu minimalni zahtjevi.[30] Osim toga, Sud EU-a podsjetio je da „[propis] mora biti zakonski obvezujuć u unutarnjem pravu".[31]

37. Da bi bila zakonita, obrada podataka[32] treba biti nužna za izvršavanje zadaće koju obavlja nadležno tijelo u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja

[26] Vidjeti t. 93.
[27] Uvodna izjava 67. Direktive o zaštiti podataka.
[28] Vidjeti predmet Schrems II., t. 173.
[29] U uvodnoj izjavi 35. Direktive o zaštiti podataka navodi se i da „[a]ko ispitanik mora ispuniti pravnu obvezu, on nema pravi i slobodan izbor, stoga se reakcija ispitanika ne bi mogla smatrati dovoljno slobodnim izrazom njegovih želja. To ne bi smjelo spriječiti države članice da zakonski predvide da ispitanik može pristati na obradu svojih osobnih podataka za potrebe iz ove Direktive, poput DNK testiranja u kaznenim istragama ili praćenja svoje lokacije pomoću elektroničkih oznaka za izvršavanje kaznenih sankcija."
[30] Vidjeti predmet Schrems II., t. 175 i 180 te Mišljenje 1/15, t. 139. i navedenu sudsku praksu.
[31] Vidjeti predmet C-623/17, Privacy International protiv Secretary of State for Foreign and Commonwealth Affairs i dr., 6. listopada 2020., ECLI:EU:C:2020:790, t. 68. – Treba napomenuti i da u presudi na francuskom jeziku Sud EU-a koristi riječ *réglementation*, koja je šira i ne obuhvaća samo akte Parlamenta.
[32] Obrada osobnih podataka koja se u cijelosti ili djelomično obavlja automatizirano te neautomatizirana obrada osobnih podataka koji čine dio sustava pohrane ili su namijenjeni tomu da budu dio sustava pohrane.

kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje.[33] Te svrhe trebalo bi predvidjeti u nacionalnom pravu.

38. Osobni podaci moraju se pošteno obrađivati. Načelo zaštite podataka u pogledu poštene obrade odvojeno je od pojma prava na pošteno suđenje, kako je utvrđeno u članku 47. Povelje i u članku 6. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda.[34]

c) Načelo ograničavanja svrhe (članak 4.)

39. Posebne svrhe obrade osobnih podataka osobito bi trebale biti izričite i legitimne te utvrđene u trenutku prikupljanja osobnih podataka.[35]

40. Podaci bi se trebali obrađivati u posebne, izričite i zakonite svrhe u okviru svrha sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija[36], uključujući zaštitu od prijetnji javnoj sigurnosti unutar treće zemlje i njihovo sprečavanje, te potom upotrebljavati u bilo koju od tih svrha ako to nije protivno izvornoj svrsi obrade (npr. za paralelne postupke izvršenja ili u svrhe arhiviranja u javnom interesu, u znanstvene, statističke ili povijesne svrhe) i podložno odgovarajućim zaštitnim mjerama u pogledu prava i sloboda ispitanika. Ako osobne podatke obrađuje isti ili drugi voditelj obrade (nadzorno tijelo[37]) u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija za koje nisu prikupljeni, takva bi obrada trebala biti dopuštena pod uvjetom da je takva obrada odobrena u skladu s primjenjivim pravnim odredbama te da je nužna za tu drugu svrhu i razmjerna toj drugoj svrsi[38]. Trebalo bi uzeti u obzir i postojanje mehanizma za obavješćivanje relevantnih nadležnih tijela država članica o takvoj daljnjoj obradi podataka.[39] Nadalje, u svakom slučaju ne bi trebalo narušiti razinu zaštite pojedinaca koju u Uniji pruža Direktiva o zaštiti podataka, uključujući u onim slučajevima u kojima se osobni podaci iz treće zemlje prenose voditeljima obrade ili izvršiteljima obrade u istoj trećoj zemlji.[40]

d) Posebni uvjeti za daljnju obradu u druge svrhe (članak 9.)

41. Za daljnju obradu ili otkrivanje podataka prenesenih iz EU-a u druge svrhe osim za potrebe izvršavanja zakonodavstva, kao što su potrebe nacionalne sigurnosti, također bi trebalo zakonom propisati da trebaju biti nužni i proporcionalni. Trebalo bi uzeti u obzir i postojanje mehanizma za

[33] Nadležna tijela su svako javno tijelo nadležno za te svrhe ili bilo koje drugo tijelo ili subjekt kojemu je zakonom povjereno izvršavanje javnih ovlasti u te svrhe.
[34] Uvodna izjava 26. Direktive o zaštiti podataka.
[35] Uvodna izjava 26. Direktive o zaštiti podataka.
[36] Uključuje „policijske aktivnosti bez prethodnog znanja o tome je li incident kazneno djelo. Takve aktivnosti mogu obuhvaćati i izvršavanje ovlasti uporabom mjera prisile poput policijskih aktivnosti na prosvjedima, velikim sportskim događanjima ili u neredima. One također uključuju održavanje zakona i reda, kao zadaće dodijeljene policiji ili drugim tijelima za izvršavanje zakonodavstva ako je potrebna zaštita od prijetnji javnoj sigurnosti i njihovo sprečavanje te prijetnji temeljnim interesima društva zaštićenima zakonom, što može dovesti do kaznenog djela." (uvodna izjava 12. Direktive o zaštiti podataka). To treba razlikovati od svrhe u vezi s nacionalnom sigurnosti ili od djelatnosti obuhvaćenih glavom V. poglavljem 2. Ugovora o Europskoj uniji (UEU) (uvodna izjava 14. Direktive o zaštiti podataka).
[37] Vidjeti bilješku 33.
[38] Uvodna izjava 29. Direktive o zaštiti podataka.
[39] Takav mehanizam mogli bi biti, na primjer, uzajamno dogovorene oznake za postupanje, obveza obavješćivanja u okviru međunarodnog instrumenta, uključujući moguće automatske obavijesti, ili druge slične mjere transparentnosti.
[40] Uvodna izjava 64. Direktive o zaštiti podataka.

obavješćivanje relevantnih nadležnih tijela država članica o takvoj daljnjoj obradi podataka.[41] I u tom slučaju, nakon daljnje obrade ili otkrivanja podaci bi trebali imati istu razinu zaštite kao kad ih je prvotno obradilo nadležno tijelo koje ih je zaprimilo.

e) Načelo smanjenja količine podataka

42. Podaci bi trebali biti primjereni, relevantni i ne preopsežni u odnosu na svrhu u koju se obrađuju. Konkretno, trebalo bi uzeti u obzir primjenu tehničke i integrirane zaštite podataka, kao što su ograničena ulazna polja (strukturirana komunikacija) ili automatizirane i neautomatizirane provjere kvalitete.

f) Načelo točnosti podataka

43. Podaci bi trebali biti točni i, prema potrebi, ažurirani. Međutim, načelo točnosti podataka trebalo bi primijeniti uzimajući u obzir prirodu i svrhu predmetne obrade. Izjave koje sadržavaju osobne podatke temelje se, osobito u sudskim postupcima, na subjektivnoj percepciji pojedinaca i ne mogu se uvijek provjeriti. Stoga se zahtjev za točnošću ne bi trebao odnositi na točnost izjave, već samo na činjenicu da je određena izjava dana.[42]

44. Trebalo bi osigurati da se osobni podaci koji su netočni, nepotpuni ili više nisu ažurni ne prenose i ne stavljaju na raspolaganje[43] te da se predvide postupci za ispravljanje ili brisanje netočnih podataka. Konkretno, trebalo bi uzeti u obzir svaki sustav klasifikacije obrađenih informacija, u pogledu pouzdanosti izvora i razine provjere činjenica[44].

g) Načelo zadržavanja podataka

45. Podaci se ne bi trebali čuvati dulje nego što je potrebno za svrhe u koje se obrađuju. Trebalo bi uspostaviti odgovarajuće mehanizme za brisanje osobnih podataka; to može biti određeno razdoblje ili periodično preispitivanje potrebe za pohranom osobnih podataka (ili njihova kombinacija: određeno najdulje razdoblje i periodično preispitivanje u određenim vremenskim razmacima).[45] Na osobne podatke koji se pohranjuju na dulja razdoblja u svrhe arhiviranja u javnom interesu, u znanstvene, statističke ili povijesne svrhe, trebale bi se primjenjivati odgovarajuće zaštitne mjere (npr. u pogledu pristupa)[46].

h) Načelo sigurnosti i povjerljivosti (članak 29., uvodne izjave 28. i 71.)

46. Svaki subjekt koji obrađuje osobne podatke trebao bi osigurati da se podaci obrađuju na način kojim se jamči sigurnost osobnih podataka, uključujući sprečavanjem neovlaštenog pristupa osobnim podacima i opremi za obradu ili njihove neovlaštene uporabe. To uključuje zaštitu od nezakonite obrade i od slučajnog gubitka, uništenja ili oštećenja te odgovarajuće mjere za rješavanje tih problema primjenom odgovarajućih tehničkih i organizacijskih mjera. Pri utvrđivanju razine sigurnosti trebalo bi uzeti u obzir najnovija dostignuća i troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različite vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca.

[41] Vidjeti bilješku 39.
[42] Uvodna izjava 30. Direktive o zaštiti podataka.
[43] Uvodna izjava 32. Direktive o zaštiti podataka.
[44] Npr. mreže 4x4 za procjene pouzdanosti i oznake za postupanje.
[45] Članak 5. Direktive o zaštiti podatka.
[46] Uvodna izjava 26. Direktive o zaštiti podataka.

47. Trebalo bi osigurati sigurne kanale komunikacije između tijela država članica koja prenose osobne podatke i tijela trećih država koja ih primaju.

i) Načelo transparentnosti (članak 13., uvodne izjave 26., 39., 42., 43., 44. i 46.)

48. Pojedince bi trebalo upoznati s rizicima, pravilima, zaštitnim mjerama i pravima u vezi s obradom njihovih osobnih podataka i načinom ostvarivanja njihovih prava u vezi s obradom.[47]

49. Pojedincima bi trebalo staviti na raspolaganje informacije o svim glavnim elementima obrade njihovih osobnih podataka. Te informacije trebale bi biti lako dostupne i lako razumljive, a jezik jasan i jednostavan. Trebale bi uključivati svrhu obrade, identitet voditelja obrade podataka, prava na raspolaganju[48] i ostale informacije, ako je to potrebno za osiguranje poštene obrade.

50. Mogu postojati neke iznimke od tog prava na informacije. Međutim, takvo bi ograničenje trebalo dopustiti zakonodavnom mjerom te bi ono trebalo biti nužno i razmjerno kako bi se izbjeglo ometanje službenih ili pravnih ispitivanja, istraga ili postupaka te dovođenje u pitanje sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, kako bi se zaštitila javna ili nacionalna sigurnost ili zaštitila prava i slobode drugih, dok god takvo djelomično ili potpuno ograničavanje čini neophodnu i proporcionalnu mjeru u demokratskom društvu uz dužno poštovanje temeljnih prava i legitimnih interesa dotičnog pojedinca. Takva ograničenja također bi trebalo razmotriti i procijeniti uzimajući u obzir mogućnost podnošenja pritužbe nadzornom tijelu ili traženja pravnog lijeka. U svakom slučaju, sva moguća ograničenja trebala bi biti privremena i ne bi trebala biti opća te bi trebala biti uređena uvjetima, zaštitnim mjerama i ograničenjima sličnima onima koji se zahtijevaju u skladu s Poveljom i Europskom konvencijom za zaštitu ljudskih prava i temeljnih sloboda, kako se tumače u sudskoj praksi Suda EU-a odnosno Europskog suda za ljudska prava, a posebno bi trebala poštovati srž tih prava i sloboda.

j) Pravo na pristup, ispravak i brisanje (članci 14. i 16.)

51. Ispitanik bi trebao imati pravo dobiti potvrdu o tome provodi li se neka obrada podataka koja se odnosi na njega te bi, ako je tako, trebao imati pristup svojim podacima. To pravo trebalo bi obuhvaćati barem određene informacije o obradi, kao što su svrha i pravna osnova obrade, pravo na podnošenje pritužbe nadzornom tijelu ili kategorije osobnih podataka o kojima je riječ[49]. To je posebno važno u slučaju da se transparentnost postiže općom obavijesti (npr. informacije na internetskim stranicama nadležnog tijela).

52. Ispitanik bi trebao imati pravo na ispravak svojih podataka iz određenih razloga, na primjer ako se pokaže da su netočni ili nepotpuni. Ispitanik bi trebao imati pravo i na brisanje svojih podataka ako obrada, na primjer, više nije potrebna ili je nezakonita.

53. Iskorištavanje tih prava ne bi trebalo biti pretjerano složeno za ispitanika.

k) Ograničenja prava ispitanika

54. Mogu postojati ograničenja tih prava kako bi se izbjeglo ometanje službenih ili pravnih ispitivanja, istraga ili postupaka te dovođenje u pitanje sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, kako bi se zaštitila javna ili nacionalna sigurnost ili zaštitila

[47] Uvodna izjava 26. Direktive o zaštiti podataka.
[48] I materijalna prava (pravo na pristup, ispravak itd.) i pravo na pravnu zaštitu.
[49] Članak 14. Direktive o zaštiti podatka.

prava i slobode drugih, dok god takvo djelomično ili potpuno ograničavanje čini neophodnu i proporcionalnu mjeru u demokratskom društvu uz dužno poštovanje temeljnih prava i legitimnih interesa dotičnog pojedinca. Takva ograničenja također bi trebalo razmotriti i procijeniti uzimajući u obzir mogućnost podnošenja pritužbe nadzornom tijelu ili traženja pravnog lijeka.

l) Ograničenja daljnjeg prijenosa (članak 35., uvodne izjave 64. – 65.)

55. Daljnji prijenosi osobnih podataka od strane prvotnog primatelja u neku drugu treću zemlju ili međunarodnu organizaciju ne smiju ugroziti razinu zaštite fizičkih osoba čiji se podaci prenose, osiguranu u Uniji. Stoga bi takvi daljnji prijenosi podataka trebali biti dopušteni samo ako je osiguran kontinuitet razine zaštite zajamčene pravom EU-a.[50] Konkretno, daljnji primatelj (tj. primatelj daljnjeg prijenosa) trebalo bi biti nadležno tijelo za potrebe izvršavanja zakonodavstva[51], a takvi daljnji prijenosi podataka mogu se obavljati samo u ograničene i posebne svrhe i pod uvjetom da postoji pravna osnova za takvu obradu.

56. Trebalo bi uzeti u obzir i postojanje mehanizma za obavješćivanje relevantnih nadležnih tijela država članica koja bi odobravala takve daljnje prijenose. Prvotni primatelj podataka prenesenih iz EU-a trebao bi biti odgovoran i trebao bi moći dokazati da je relevantno nadležno tijelo države članice odobrilo daljnji prijenos[52] te da su osigurane odgovarajuće zaštitne mjere za daljnje prijenose podataka u slučaju nepostojanja odluke o primjerenosti u pogledu treće zemlje u koju bi se podaci dalje prenosili[53].

m) Načelo odgovornosti (članak 4. stavak 4.)

57. Voditelj obrade trebao bi biti odgovoran za usklađenost s načelima zaštite podataka iz članka 4. Direktive o zaštiti podataka te bi trebao moći dokazati njihovu usklađenost.

[50] Vidjeti i Mišljenje 1/15.
[51] Vidjeti bilješku 33.
[52] U tom kontekstu trebalo bi uzeti u obzir postojanje obveze da se uvedu relevantne oznake za postupanje koje su definirala tijela država članica.
[53] Navedenim zahtjevima ne dovode se u pitanje posebni uvjeti za daljnje prijenose u odgovarajuću zemlju utvrđeni u skladu s Direktivom o zaštiti podataka (članak 35. stavak 1. točke (c) i (e)).

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

a) Posebne kategorije podataka (članak 10. i uvodna izjava 37.)

58. Trebale bi postojati posebne zaštitne mjere ako su obuhvaćene „posebne kategorije podataka”[54] koje se odnose na posebne rizike.[55] Te bi kategorije trebale odgovarati kategorijama iz članka 10. Direktive o zaštiti podataka. Na obradu posebnih kategorija podataka trebale bi se stoga primjenjivati posebne zaštitne mjere te bi ona trebala biti dopuštena samo ako je to nužno potrebno pod određenim uvjetima, na primjer radi zaštite vitalnog interesa pojedinca.

b) Automatizirano donošenje odluka i izrada profila (članak 11. i uvodna izjava 38.)

59. Odluke koje se temelje isključivo na automatiziranoj obradi (automatizirano pojedinačno donošenje odluka), uključujući izradu profila, te koje proizvode štetne pravne učinke ili znatno utječu na ispitanika mogu se dopustiti samo pod određenim uvjetima utvrđenima u pravnom okviru treće zemlje.[56]

60. U okviru Europske unije takvi uvjeti uključuju, na primjer, pružanje posebnih informacija ispitaniku i pravo na izravnu ljudsku intervenciju voditelja obrade, posebno pravo na izražavanje vlastitog stajališta, dobivanje objašnjenja odluke donesene nakon takve procjene i osporavanje te odluke.

61. Zakonodavstvom treće zemlje trebale bi se u svakom slučaju predvidjeti potrebne zaštitne mjere za prava i slobode ispitanika. U tom pogledu trebalo bi uzeti u obzir i postojanje mehanizma za obavješćivanje relevantnih nadležnih tijela države članice o svakoj daljnjoj obradi kao što je upotreba prenesenih podataka za izradu profila velikih razmjera.

c) Tehnička i integrirana zaštita podataka (članak 20.)

62. Pri procjeni primjerenosti trebalo bi obratiti pozornost na postojanje obveze voditelja obrade da donose unutarnje politike i provode mjere koje su u skladu s načelima tehničke i integrirane zaštite podataka, uzimajući u obzir najnovija dostignuća i troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizike različite vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca koji proizlaze iz obrade podataka, i u vrijeme određivanja sredstava obrade i u vrijeme same obrade, te da provode odgovarajuće tehničke i organizacijske mjere, poput pseudonimizacije, za omogućivanje učinkovite primjene načela zaštite podataka, kao što je smanjenje količine podataka, i uključenje zaštitnih mjera u obradu.

[54] U uvodnoj izjavi 37. takve posebne kategorije nazivaju se „osjetljivim podacima”.
[55] Takve dodatne zaštitne mjere mogle bi biti npr. posebne sigurnosne mjere, ograničena prava pristupa za osoblje i ograničenja u pogledu daljnje obrade, automatiziranog donošenja odluka, daljnjeg dijeljenja ili daljnjih prijenosa.
[56] Mišljenje 1/15, t. 173.

C. Postupovni i provedbeni mehanizmi

63. Iako se pravna sredstva kojima se koristi treća zemlja za osiguravanje primjerene razine zaštite mogu razlikovati od onih koja se provode u Europskoj uniji[57], sustav koji je usklađen s europskim mora sadržavati elemente u nastavku.

a) Nadležno neovisno nadzorno tijelo (članak 36. stavak 2. točka (b), članak 36. stavak 3. i uvodna izjava 67.)

64. U trećoj bi zemlji trebalo postojati najmanje jedno neovisno nadzorno tijelo čija je zadaća osiguravanje i provedba 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 odgovarajuće provedbene ovlasti radi djelotvornog osiguravanja usklađenosti s pravima na zaštitu podataka i promicanja informiranosti. Trebalo bi isto tako uzeti u obzir osoblje i proračun nadzornog tijela. Nadzorno tijelo ujedno treba moći provoditi istrage na vlastitu inicijativu. Trebalo bi biti zaduženo i za pružanje pomoći ispitanicima i njihovo savjetovanje u ostvarivanju njihovih prava (vidjeti i točku c) u nastavku). U odlukama o primjerenosti trebalo bi, ako je primjenjivo, utvrditi nadzorno tijelo ili tijela i mehanizme suradnje s nadzornim tijelima država članica radi provedbe pravila o zaštiti podataka.

b) Djelotvorna provedba pravila o zaštiti podataka

65. U okviru sustava treće zemlje trebao bi se osigurati visok stupanj informiranosti voditelja obrade podataka i onih koji u njihovo ime obrađuju osobne podatke o njihovim obvezama, zadaćama i odgovornostima te informiranosti ispitanika o njihovim pravima i načinima ostvarivanja tih prava. Postojanje učinkovitih i odvraćajućih sankcija može imati važnu ulogu u osiguravanju poštovanja pravila, a to se može postići i sustavima izravne provjere koju provode nadležna tijela, revizori ili neovisni službenici za zaštitu podataka.

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

c) Sustav zaštite podataka mora olakšati ostvarivanje prava ispitanika (članci 12., 17. i 46. Direktive o zaštiti podataka)

67. Okvirom za zaštitu podataka treće zemlje trebalo bi obvezati voditelje obrade podataka da olakšaju ostvarivanje prava ispitanika iz odjeljka A. točke j) te osigurati da njezino nadzorno tijelo, na zahtjev, obavijesti sve ispitanike o ostvarivanju njihovih prava[58].

d) Sustav zaštite podataka mora osigurati odgovarajuće mehanizme pravne zaštite

68. Iako trenutačno ne postoji sudska praksa u pogledu primjerenosti pravnog sustava treće zemlje u skladu s Direktivom o zaštiti podataka, Sud EU-a tumačio je temeljno pravo na djelotvornu sudsku

[57] Predmet Schrems I., t. 74.
[58] Ostvarivanje prava ispitanika može biti izravno ili neizravno.

zaštitu kako je utvrđeno u članku 47. Povelje. U prvom stavku članka 47. Povelje propisuje se da svatko kome su povrijeđena prava i slobode koji su zajamčeni pravom Unije ima pravo na djelotvoran pravni lijek pred sudom[59], u skladu s uvjetima utvrđenima tim člankom.

69. Prema ustaljenoj sudskoj praksi Suda EU-a, sâmo postojanje djelotvornog sudskog nadzora radi osiguranja poštovanja Unijinih pravnih odredaba svojstveno je postojanju pravne države. Tako propis koji pojedincima ne pruža nikakvu mogućnost korištenja pravnim sredstvima radi pristupa osobnim podacima koji se na njih odnose, ili radi ispravka ili brisanja takvih podataka, ne poštuje bitan sadržaj temeljnog prava na djelotvornu sudsku zaštitu, kao što je to propisano u članku 47. Povelje[60].

70. Pojedinac bi trebao moći koristiti pravne lijekove kako bi brzo i djelotvorno ostvario svoja prava, i to bez prevelikih troškova, ali i kako bi se osigurala usklađenost.

71. 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 prava na poštovanje privatnog života utvrde i kazne u praksi.

72. Ako se pravila ne poštuju, ispitaniku čiji se osobni podaci prenose u treću zemlju trebalo bi i u trećoj zemlji pružiti djelotvornu upravnu i sudsku zaštitu, uključujući naknadu štete nastale kao rezultat nezakonite obrade njegovih osobnih podataka. Riječ je o ključnom aspektu za koji je karakterističan sustav neovisnog sudskog odlučivanja ili arbitraže kojim se, prema potrebi, omogućava plaćanje naknade i određivanje kazni.

[59] Sud EU-a smatra da djelotvornu sudsku zaštitu osim suda može osigurati i tijelo koje pruža zaštitne mjere bitno ekvivalentne onima koje se zahtijevaju člankom 47. Povelje (vidjeti predmet Schrems II., t. 197.). To bi moglo biti posebno važno za međunarodne organizacije.
[60] Predmet Schrems II., t. 187. i 194., uključujući navedenu sudsku praksu.