

Preporuke



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

Preporuke 01/2020 o mjerama kojima se dopunjuju alati za prijenos podataka kako bi se osigurala usklađenost s razinom zaštite osobnih podataka u EU-u

Doneseno 10. studenoga 2020.

Izvršni sažetak

Opća uredba o zaštiti podataka EU-a (Opća uredba) donesena je kako bi služila dvostrukoj svrsi: olakšavanju slobodnog kretanja osobnih podataka unutar Europske unije uz istovremeno očuvanje temeljnih prava i sloboda pojedinaca, posebno njihova prava na zaštitu osobnih podataka.

U svojoj nedavnoj presudi C-311/18 (Schrems II) Sud Europske unije (SEU) podsjetio je da se zaštita koja se dodjeljuje osobnim podatcima u Europskom gospodarskom prostoru (EGP) mora primjenjivati na podatke neovisno o tome gdje se prenose. Prijenos osobnih podataka u treće zemlje ne može biti sredstvo narušavanja ili umanjivanja zaštite koja im se pruža u EGP-u. Sud to također potvrđuje objašnjavajući da razina zaštite u trećim zemljama ne mora biti identična zaštiti zajamčenoj u EGP-u, nego mora biti u načelu istovjetna. Sud također potvrđuje valjanost standardnih ugovornih klauzula kao alata za prijenos kojim se može ugovorno osigurati u načelu istovjetna razina zaštite podataka koji se prenose u treće zemlje.

Standardne ugovorne klauzule i drugi alati za prijenos navedeni u članku 46. Opće uredbe ne primjenjuju se izolirano. Sud navodi da je na voditeljima ili izvršiteljima obrade podataka, koji djeluju kao izvoznici, da u svakom slučaju zasebno i, ako je potrebno, u suradnji s uvoznikom u trećoj zemlji, provjere dovode li pravo ili praksa treće zemlje u pitanje učinkovitost odgovarajućih zaštitnih mjera sadržanih u alatima za prijenos iz članka 46. Opće uredbe. U tim slučajevima Sud i dalje ostavlja mogućnost izvoznicima da provedu dodatne mjere kojima se nadoknađuju nedostaci u zaštiti i kojima se zaštita podiže na razinu propisanu pravom Unije. Sud ne precizira koje bi to mjere mogle biti. Međutim, Sud naglašava da će ih izvoznici morati utvrditi zasebno u svakom slučaju. To je u skladu s načelom odgovornosti iz članka 5. stavka 2. Opće uredbe kojim se propisuje da su voditelji obrade podataka odgovorni za usklađenost s načelima iz Opće uredbe koja se odnose na obradu osobnih podataka i da moraju biti u mogućnosti dokazati tu usklađenost.

Europski odbor za zaštitu podataka usvojio je ove preporuke kako bi pomogao izvoznicima (bilo da se radi o voditeljima ili izvršiteljima obrade, privatnim subjektima ili javnim tijelima koja obrađuju osobne podatke u okviru primjene Opće uredbe) u složenoj zadaći procjenjivanja trećih zemalja i, prema potrebi, utvrđivanja odgovarajućih dodatnih mjera. U ovim se preporukama izvoznicima pruža niz koraka koje mogu slijediti, mogući izvori informacija i neki primjeri dodatnih mjera koje se mogu provesti.

Kao **prvi korak**, Europski odbor za zaštitu podataka vama izvoznicima savjetuje da **budete upoznati sa svojim prijenosima podataka**. Mapiranje svih prijenosa osobnih podataka u treće zemlje može biti teško. Međutim, svijest o tome gdje se osobni podatci prenose nužno je kako bi se osiguralo da ti podatci imaju u načelu istovjetnu razinu zaštite neovisno o tome gdje se obrađuju. Usto morate provjeriti da su podatci koje prenosite primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se podatci prenose u treću zemlju i u njoj obrađuju.

Drugi je korak provjeriti alat za prijenos na koji se oslanjate, među onima navedenima u poglavlju V. Opće uredbe. Ako je Europska komisija već proglasila određenu zemlju, regiju ili sektor u koje prenosite podatke primjerenima jednom od svojih odluka o primjerenosti na temelju članka 45. Opće uredbe ili na temelju prethodne Direktive 95/46, sve dok je odluka i dalje na snazi, nećete morati poduzimati dodatne korake osim praćenja je li odluka o primjerenosti i dalje valjana. Ako Europska komisija nije donijela odluku o primjerenosti, morate se osloniti na jedan od alata za prijenos navedenih u članku 46. Opće uredbe za prijenose koji su redoviti i koji se ponavljaju. Samo u nekim slučajevima povremenih prijenosa koji se ne ponavljaju možda ćete se moći osloniti na jedno od odstupanja predviđenih u članku 49. Opće uredbe, ako ispunite uvjete za to.

Treći korak jest **procijeniti** postoji li išta u **pravu ili praksi treće zemlje** što može dovesti u pitanje učinkovitost odgovarajućih zaštitnih mjera iz alata za prijenos na koje se oslanjate, u kontekstu konkretnog prijenosa. Vaša se procjena treba prvenstveno usredotočiti na zakonodavstvo treće zemlje koje je relevantno za vaš prijenos i za alat za prijenos iz članka 46. Opće uredbe na koji se oslanjate, i koje može narušiti razinu zaštite tog alata. Za ocjenjivanje elemenata koje je potrebno uzeti u obzir prilikom procjene zakona treće zemlje koji se bave pristupom podacima od strane javnih tijela za potrebe nadzora, pogledajte preporuke o Europskim ključnim jamstvima Europskog odbora za zaštitu podataka. To se treba posebno pažljivo razmotriti kad je zakonodavstvo kojim se uređuje pristup podacima od strane javnih tijela dvosmisleno ili nije javno dostupno. Ako zakonodavstvo kojim se uređuju okolnosti u kojima tijela javne vlasti mogu pristupiti osobnim podacima ne postoji te ako i dalje želite prenijeti podatke, trebali biste istražiti druge relevantne i objektivne čimbenike, a ne se oslanjati na subjektivne čimbenike poput toga koliko je vjerojatno da će javna tijela pristupiti vašim podacima na način koji nije u skladu sa standardima EU-a. Tu biste procjenu trebali provesti s dužnom pažnjom i temeljito je dokumentirati jer ćete snositi odgovornost za odluku koji donesete na temelju te procjene.

Četvrti korak jest **utvrditi i usvojiti dodatne mjere** koje su nužne kako bi se razina zaštite prenesenih podataka podigla na razinu standarda EU-a o načelnoj istovjetnosti zaštite. Taj je korak nužan samo ako vaša procjena pokaže da zakonodavstvo treće zemlje dovodi u pitanje učinkovitost alata za prijenos iz članka 46. Opće uredbe na koji se oslanjate ili na koji se namjeravate osloniti u kontekstu vašeg prijenosa. Preporuke sadrže (u prilogu 2.) ogledni popis primjera dodatnih mjera i neke uvjete za njihovu učinkovitost. Kao što je to slučaj s odgovarajućim zaštitnim mjerama sadržanima u alatima za prijenos iz članka 46., neke dodatne mjere mogu biti učinkovite u nekim zemljama, ali ne moraju nužno biti učinkovite u nekim drugim zemljama. Snosit ćete odgovornost za procjenjivanje njihove učinkovitosti u kontekstu prijenosa i s obzirom na zakone treće zemlje i na alat za prijenos na koji se oslanjate te ćete snositi odgovornost za odluku koju donesete. Možda ćete morati kombinirati nekoliko dodatnih mjera. U konačnici se može dogoditi da utvrdite da nijedna dodatna mjera ne može osigurati u načelu istovjetnu razinu zaštite za određeni prijenos. U slučajevima u kojima nijedna dodatna mjera nije primjerena, morate izbjeći, obustaviti ili prekinuti prijenos kako biste izbjegli ugrožavanje razine zaštite osobnih podataka. Tu procjenu dodatnih mjera također trebate provesti s dužnom pažnjom i dokumentirati.

Peti korak jest **provesti sve formalne postupovne korake** koji su potrebni za usvajanje vaše dodatne mjere, ovisno o alatu za prijenos iz članka 46. Opće uredbe na koji se oslanjate. Ove preporuke preciziraju te formalnosti. Možda ćete se morati savjetovati s nadležnim nadzornim tijelima o nekima od njih.

Šesti i posljednji korak jest da u odgovarajućim vremenskim razmacima ponovno procijenite razinu zaštite podataka koje prenosite u treće zemlje i da nadzirete jesu li se pojavile kakve okolnosti ili hoće li se pojaviti kakve okolnosti koje mogu utjecati na tu razinu zaštite. Načelo odgovornosti zahtijeva stalni oprez u pogledu razine zaštite osobnih podataka.

Nadzorna tijela nastaviti će obnašati svoj mandat za praćenje primjene Opće uredbe i za njezinu provedbu. Nadzorna tijela posvetit će dužnu pažnju radnjama koje izvoznici poduzimaju kako bi osigurali da podatci koje prenose imaju u načelu istovjetnu razinu zaštitu. Kao što Sud podsjeća, nadzorna će tijela obustaviti ili zabraniti prijenose podataka u onim slučajevima u kojima, nakon istrage ili pritužbe, utvrde da se ne može osigurati u načelu istovjetna razina zaštite.

Nadzorna tijela nastaviti će razvijati smjernice za izvoznike i koordinirati svoje aktivnosti unutar Europskog odbora za zaštitu podataka u svrhu osiguravanja dosljedne primjene prava Unije o zaštiti podataka.

Sadržaj

1	Odgovornost pri prijenosima podataka	7
2	Plan djelovanja: primjena načela odgovornosti na prijenose podataka u praksi	8
2.1	1. korak: budite upoznati sa svojim prijenosima podataka.....	8
2.2	2. korak: utvrdite na koje se alate za prijenos oslanjate	9
2.3	3. korak: procijenite je li alat za prijenos iz članka 46. na koji se oslanjate učinkovit s obzirom na sve okolnosti prijenosa	12
2.4	4. korak: donesite dodatne mjere	15
2.5	5. korak: postupovni koraci ako ste utvrdili učinkovite dodatne mjere	17
2.6	6. korak: ponovna procjena u odgovarajućim vremenskim razmacima	19
3	Zaključak.....	20
	PRILOG 1.: DEFINICIJE.....	21
	PRILOG 2.: PRIMJERI DODATNIH MJERA	22
	Tehničke mjere	22
	Dodatne ugovorne mjere	29
	Organizacijske mjere	35
	PRILOG 3.: MOGUĆI IZVORI INFORMACIJA ZA PROCJENU TREĆE ZEMLJE	39

Europski odbor za zaštitu podataka

uzimajući u obzir članak 70. stavak 1. točku (e) Uredbe 2016/679/EU 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 (dalje u tekstu: Opća uredba),

uzimajući u obzir Sporazum o Europskom gospodarskom prostoru (EGP), a posebno njegov Prilog XI. i Protokol 37., kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.¹,

uzimajući u obzir članak 12. i članak 22. svojeg Poslovnika,

budući da:

(1) je Sud Europske unije (SEU) zaključio u svojoj presudi od 16. srpnja 2020. *Data Protection Commissioner protiv Facebook Ireland LTD, Maximilliana Schremsa*, C-311/18 da se članak 46. stavak 1. i članak 46. stavak 2. točka (c) Opće uredbe moraju tumačiti na način da odgovarajuće zaštitne mjere, provediva prava i učinkoviti pravni lijekovi propisani tim odredbama moraju osigurati da se ispitanicima čiji se osobni podatci prenose u treću zemlju u skladu sa standardnim klauzulama o zaštiti podataka pruži razina zaštite koja je u načelu istovjetna razini zaštite zajamčenoj tom uredbom u Europskoj uniji, tumačenom u vezi s Poveljom Europske unije o temeljnim pravima,²

(2) kao što je naglasio Sud, razina zaštite pojedinaca koja je u načelu istovjetna razini zajamčenoj unutar Europske unije Općom uredbom, tumačenom u vezi s Poveljom, mora se jamčiti bez obzirom na odredbu poglavlja V. na temelju koje se izvršava prijenos osobnih podataka u treću zemlju. Odredbe poglavlja V. imaju za cilj osigurati kontinuirano visoku razinu zaštite osobnih podataka kada se ti podatci prenose u treću zemlju,³

(3) uvodna izjava 108. i članak 46. stavak 1. Opće uredbepredviđaju da, ako nije donesena odluka o primjerenosti EU-a, voditelj obrade ili izvršitelj obrade trebaju poduzeti mjere kojima će se nadomjestiti nedostatak zaštite podataka u trećoj zemlji primjenom odgovarajućih zaštitnih mjera za ispitanika. Voditelj obrade ili izvršitelj obrade mogu poduzeti odgovarajuće zaštitne mjere, bez potrebe za ikakvim posebnim ovlaštenjem nadzornog tijela, uporabom jednog od alata za prijenos navedenih u članku 46. stavku 2. Opće uredbe, kao što su standardne klauzule o zaštiti podataka,

(4) Sud pojašnjava da je svrha standardnih klauzula o zaštiti podataka koje je donijela Komisija isključivo pružiti voditeljima obrade ili njihovim izvršiteljima s poslovnim nastanom u Uniji ugovorne zaštitne mjere koje se ujednačeno primjenjuju u svim trećim zemljama. Zbog njihove ugovorne naravi standardne klauzule o zaštiti podataka ne mogu obvezivati javna tijela trećih zemalja jer ona nisu ugovorna stranka. Stoga će izvoznici podataka možda morati dopuniti zaštitne mjere sadržane u tim

¹ Upućivanja na „države članice” u ovom dokumentu treba tumačiti kao upućivanja na „države članice EGP-a”.

² Presuda SEU-a od 16. srpnja 2020., *Data Protection Commissioner protiv Facebook Ireland Ltd, Maximilliana Schremsa*, (u daljnjem tekstu: C-311/18 (Schrems II)), drugo utvrđenje.

³ C-311/18 (Schrems II), stavci 92. i 93.

standardnim klauzulama o zaštiti podataka dodatnim mjerama kako bi osigurali usklađenost s razinom zaštite koja se zahtijeva pravom Unije u određenoj trećoj zemlji. Sud upućuje na uvodnu izjavu 109. Opće uredbe u kojoj se spominje ta mogućnost i potiče voditelj obrade i izvršitelje obrade da je iskoriste,⁴

(5) Sud je naveo da je prije svega na izvozniku podataka da u svakom slučaju zasebno i, ako je potrebno, u suradnji s uvoznikom podataka, provjeri osigurava li pravo treće zemlje odredišta u načelu istovjetnu razinu zaštite, s obzirom na pravo Unije, osobnih podataka prenesenih na temelju standardnih klauzula o zaštiti podataka, tako da prema potrebi osigura dodatne zaštitne mjere uz one ponuđene tim klauzulama,⁵

(6) ako voditelj obrade ili njegov izvršitelj s poslovnim nastanom u Uniji ne može donijeti dodatne mjere koje bi bile dostatne da se osigura u načelu istovjetna razina zaštite na temelju prava Unije, oni ili, podredno, nadležno nadzorno tijelo moraju obustaviti ili okončati prijenos osobnih podataka predmetnoj trećoj zemlji,⁶

(7) Opća uredba i Sud ne definiraju ni preciziraju „dodatne zaštitne mjere” ili „dodatne mjere” uz zaštitne mjere alata za prijenos navedenih u članku 46. stavku 2. Opće uredbe koje voditelji obrade i izvršitelji obrade mogu usvojiti kako bi osigurali usklađenost s razinom zaštite propisanom pravom Unije u određenoj trećoj zemlji,

(8) Europski odbor za zaštitu podataka na vlastitu je inicijativu odlučio ispitati ovo pitanje te voditeljima i izvršiteljima obrade koji djeluju kao izvoznici pružiti preporuke o postupku koji mogu slijediti kako bi utvrdili i usvojili dodatne mjere. Ovim se preporukama nastoji pružiti metodologija kojom se izvoznici mogu služiti kako bi odredili je li za njihove prijenose potrebno usvojiti dodatne mjere i koje bi dodatne mjere trebali usvojiti. Prvenstvena je odgovornost izvoznika da osiguraju da se prenesenim podacima u trećoj zemlji pruži razina zaštite koja je u načelu istovjetna razini zaštite zajamčenoj unutar EU-a. Ovim preporukama Europski odbor za zaštitu podataka nastoji potaknuti dosljednu primjenu Opće uredbe i presude Suda, u skladu sa svojim mandatom,⁷

DONIO JE SLJEDEĆU PREPORUKU:

⁴ C-311/18 (Schrems II), stavci 132. i 133.

⁵ C-311/18 (Schrems II), stavak 134.

⁶ C-311/18 (Schrems II), stavak 135.

⁷ Članak 70. stavak 1. točka (e) Opće uredbe.

1 ODGOVORNOST PRI PRIJENOSIMA PODATAKA

1. U primarnom pravu Unije pravo na zaštitu osobnih podataka smatra se temeljnim pravom.⁸ U skladu s time, pravo na zaštitu osobnih podataka pruža se visoka razina zaštite i ograničenja pri ostvarivanju prava mogu se primijeniti samo ako su predviđena zakonom, poštuju bit tog prava, proporcionalna su, potrebna i zaista odgovaraju ciljevima od općeg interesa koje priznaje Unije ili potrebi zaštite prava i sloboda drugih osoba.⁹ Pravo na zaštitu osobnih podataka nije apsolutno pravo; mora ga se razmatrati u vezi s njegovom funkcijom u društvu te ga treba ujednačiti s drugim temeljnim pravima u skladu s načelom proporcionalnosti.¹⁰
2. Razina zaštite koja je u načelu istovjetna onoj zajamčenoj u EU-u mora se primijeniti na podatke kada se prenose u treće zemlje izvan EGP-a kako bi se osiguralo da razina zaštite zajamčena Općom uredbom nije narušena.
3. Pravo na zaštitu podataka aktivne je naravi. Od izvoznika i uvoznika (neovisno o tome jesu li voditelji obrade i/ili izvršitelji obrade) zahtijeva angažman na razini višoj od samog priznavanja ili pasivnog poštovanja ovog prava.¹¹ Voditelji obrade i izvršitelji obrade moraju nastojati osigurati poštovanje prava na zaštitu podataka na aktivan i kontinuiran način provedbom zakonskih, tehničkih i organizacijskih mjera kojima se osigurava učinkovitost tog prava. Voditelji obrade i izvršitelji obrade također moraju moći prikazati te napore ispitanicima, općoj javnosti i nadzornim tijelima za zaštitu podataka. To je takozvano načelo odgovornosti.¹²
4. Načelo odgovornosti koje je nužno za osiguravanje učinkovite primjene razine zaštite koju jamči Opća uredba primjenjuje se i na prijenose podataka u treće zemlje¹³ jer su oni sami po sebi oblik obrade osobnih podataka.¹⁴ Kao što je Sud naglasio u svojoj presudi, razina zaštite koja je u načelu istovjetna razini zajamčenoj unutar Europske unije Općom uredbom, tumačenom u vezi s Poveljom, mora se jamčiti bez obzirom na odredbu tog poglavlja na temelju koje se izvršava prijenos osobnih podataka u treću zemlju.¹⁵
5. U presudi Schrems II, Sud naglašava odgovornosti izvoznika i uvoznika da osiguraju da se obrada osobnih podataka obavlja i da će se obavljati u skladu s razinom zaštite propisanom pravom Unije o zaštiti podataka i da obustave prijenos i/ili raskinu ugovor kad uvoznik podataka ne može ili više ne može poštovati standardne klauzule o zaštiti podataka koje su dio relevantnog ugovora između izvoznika i uvoznika.¹⁶ Voditelj ili izvršitelj obrade koji djeluje kao izvoznik mora osigurati da uvoznici surađuju s izvoznikom, prema potrebi, u izvršavanju tih odgovornosti tako što će ga, primjerice, informirati o svim razvojem događaja koji utječu na razinu zaštite osobnih podataka koji se primaju u

⁸ Članak 8. stavak 1. Povelje o temeljnim pravima i članak 16. stavak 1. Ugovora o funkcioniranju Europske unije, preambula 1., članak 1. stavak 2. Opće uredbe.

⁹ Članak 52. stavak 1. Povelje Europske unije o temeljnim pravima.

¹⁰ Uvodna izjava 4. Opće uredbe i presuda C-507/17 Google LLC, pravni sljednik Googlea Inc. protiv Commission nationale de l'informatique et des libertés (CNIL), stavak 60.

¹¹ C-92/09 i C-93/02, Volker und Markus Schecke GbR protiv Land Hessen, Opinion of Advocate General Sharpston (Mišljenje nezavisne odvjetnice Sharpston), 17. lipnja 2010., stavak 71.

¹² Članak 5. stavak 2. i članak 28. stavak 3. točka (h) Opće uredbe.

¹³ Članak 44. i uvodna izjava 101. Opće uredbe o zaštiti podataka, kao i članak 47. stavak 2. točka (d) Opće uredbe o zaštiti podataka.

¹⁴ Presuda SEU-a od 6. listopada 2015., *Maximillian Schrems protiv Data Protection Commissioner*, (u daljnjem tekstu: C-362/14 (Schrems I)), stavak 45.

¹⁵ C-311/18 (Schrems II), stavci 92. i 93.

¹⁶ C-311/18 (Schrems II), stavci 134, 135, 139, 140, 141, 142.

državi uvoznika.¹⁷ Te odgovornosti predstavljaju primjenu načela odgovornosti iz Opće uredbe na prijenose podataka.¹⁸

2 PLAN DJELOVANJA: PRIMJENA NAČELA ODGOVORNOSTI NA PRIJENOSE PODATAKA U PRAKSI

6. U nastavku je opisan plan djelovanja i koraci koje je potrebno poduzeti kako biste saznali trebate li vi (izvoznik podataka) uvesti dodatne mjere kako biste mogli zakonski prenositi podatke izvan EGP-a. Izraz „vi” u ovom dokumentu odnosi se na voditelja ili izvršitelja obrade koji djeluje kao izvoznik podataka i koji obrađuje osobne podatke u okviru primjene Opće uredbe – uključujući obradu od strane privatnih subjekata i javnih tijela prilikom prijenosa podataka privatnim tijelima.¹⁹ Što se tiče prijenosa osobnih podataka između javnih tijela, konkretne smjernice navedene su u dokumentu *Smjernice 2/2020 o članku 46. stavku 2. točki (a) i članku 46. stavku 3. točki (b) Uredbe 2016/679 za prijenose osobnih podataka između tijela javne vlasti i javnih tijela EGP-a i izvan EGP-a*.²⁰
7. Tu procjenu i dodatne mjere koje odaberete i provedete trebate dokumentirati i tu dokumentaciju staviti na raspolaganje nadležnom nadzornom tijelu na zahtjev.²¹

2.1 1. korak: budite upoznati sa svojim prijenosima podataka

8. Da biste znali što može biti potrebno da biste vi (izvoznik podataka) mogli nastaviti s postojećim prijenosima ili vršiti nove prijenose osobnih podataka²², u prvom koraku morate osigurati da ste u potpunosti svjesni svojih prijenosa (budite upoznati sa svojim prijenosima podataka). Evidentiranje i mapiranje svih prijenosa može biti kompleksan zadatak za subjekte koji vrše višestruke, raznolike i redovite prijenose u treće zemlje i koji upotrebljavaju usluge više izvršitelja i podizvršitelja obrade. Upoznatost s prijenosima ključan je prvi korak u ispunjavanju vaših obveza na temelju načela odgovornosti.

¹⁷ C-311/18 (Schrems II), stavak 134.

¹⁸ Članak 5. stavak 2. i članak 28. stavak 3. točka (h) Opće uredbe o zaštiti podataka.

¹⁹ Vidjeti Smjernice Europskog odbora za zaštitu podataka 3/2018 o teritorijalnom području primjene Opće uredbe (članak 3.) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en

²⁰ Smjernice Europskog odbora za zaštitu podataka 2/2020 o članku 46. stavku 2. točki (a) i članku 46. stavku 3. točki (b) Uredbe 2016/679 za prijenose osobnih podataka između tijela javne vlasti i javnih tijela EGP-a i izvan EGP-a, vidjeti https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en

²¹ Članak 5. stavak 2. i članak 24. stavak 1. Opće uredbe.

²² Imajte na umu da se pristup na daljinu podacima koji se nalaze unutar EGP-a od strane subjekta iz treće zemlje također smatra prijenosom podataka.

9. Da biste se potpuno upoznali sa svojim prijenosima, kao početnu točku možete upotrijebiti evidenciju aktivnosti obrade koju možda morate voditi kao voditelj ili izvršitelj obrade na temelju članka 30. Opće uredbe.²³ Mogu vam pomoći i prethodne aktivnosti u svrhu ispunjavanja obveza o informiranju ispitanika na temelju članka 13. stavka 1. točke (f) i članka 14. stavka 1. točke (f) Opće uredbe vašim prijenosima njihovih osobnih podataka u treće zemlje.²⁴
10. Prilikom mapiranja prijenosa nemojte zaboraviti uzeti u obzir daljnje prijenose, primjerice vrše li vaši izvršitelji obrade izvan EGP-a prijenose osobnih podataka koje ste im povjerili podizvršitelju u nekoj drugoj trećoj zemlji ili u istoj trećoj zemlji²⁵.
11. U skladu s načelom „smanjenja količine podataka” iz Opće uredbe o zaštiti podataka,²⁶ morate provjeriti da su podatci koje prenosite primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se podatci prenose u treću zemlju i u njoj obrađuju.
12. Te se aktivnosti moraju provesti prije bilo kakvog prijenosa i moraju se ažurirati prije nastavka prijenosa nakon obustave postupaka prijenosa podataka: morate znati gdje se osobni podatci koje ste izvezli nalaze ili gdje ih uvoznici obrađuju (kartica odredišta).
13. Imajte na umu da se pristup na daljinu iz treće zemlje (primjerice, u situacijama pružanja podrške) i/ili pohrana na oblaku koji se nalazi izvan EGP-a također smatraju prijenosom podataka.²⁷ Konkretno, ako upotrebljavate međunarodnu infrastrukturu oblaka, morate procijeniti hoće li se vaši podatci prenositi u treće zemlje i koje, osim ako pružatelj usluga u oblaku jasno navede u ugovoru da se podatci uopće neće obrađivati u trećim zemljama.

2.2 2. korak: utvrdite na koje se alate za prijenos oslanjate

14. U drugom koraku morate utvrditi alate za prijenos na koje se oslanjate među alatima navedenima i predviđenima u poglavlju V. Opće uredbe.

²³ Vidjeti članak 30. Opće uredbe, posebno stavak 1. točku (e) i stavak 2. točku (c). Štoviše, vaša evidencija obrade treba sadržavati opis vaših aktivnosti obrade (uključujući, ali bez ograničavanja na, kategorije ispitanika, kategorije osobnih podataka, svrhe obrade i konkretne informacije o prijenosima podataka). Neki voditelji i izvršitelji obrade izuzeti su od obveze evidentiranja obrade (članak 30. stavak 5. Opće uredbe). Smjernice o tom izuzeću potražite u Dokumentu o stajalištu Radne skupine iz članka 29. o odstupanjima od obveze evidentiranja aktivnosti obrade u skladu s člankom 30. stavkom 5. Opće uredbe o zaštiti podataka (odobrio Europski odbor za zaštitu podataka 25. svibnja 2018.).

²⁴ Na temelju pravila o transparentnosti iz Opće uredbe, ispitanike morate obavijestiti o prijenosima osobnih podataka u treće zemlje (članak 13. stavak 1. točka (f) i članak 14. stavak 1. točka (f) Opće uredbe). Konkretno, morate ih obavijestiti o postojanju ili nepostojanju odluke Komisije o primjerenosti, ili u slučaju prijenosa iz članka 46. ili 47. Opće uredbe, ili članka 49. stavka 1. drugog podstavka Opće uredbe, uputiti na prikladne ili odgovarajuće zaštitne mjere i načine pribavljanja njihove kopije ili mjesta na kojem su stavljene na raspolaganje. Informacije koje se daju ispitanicima moraju biti točne i aktualne, posebno s obzirom na sudsku praksu Suda u vezi s prijenosima.

²⁵ Kad je voditelj obrade dao prethodno posebno ili opće pisano odobrenje u skladu s člankom 28. stavkom 2. Opće uredbe.

²⁶ Članak 5. stavak 1. točka (c) Opće uredbe.

²⁷ Vidjeti Često postavljana pitanja br. 11 „*treba imati na umu da čak i pružanje pristupa podatcima iz neke treće zemlje, primjerice u administrativne svrhe, također ima učinak prijenosa podataka*”, Često postavljana pitanja Europskog odbora za zaštitu podataka o presudi Suda Europske unije u predmetu C-311/18 – Data Protection Commissioner protiv Facebook Ireland Ltd i Maximilliana Schremsa, 23. srpnja 2020.

Odluke o primjerenosti

15. Europska komisija može **odlukama o primjerenosti** koje se odnose na neke ili sve treće zemlje u koje prenosite osobne podatke priznati da te zemlje pružaju primjerenu razinu zaštite osobnih podataka.²⁸
16. Učinak takve odluke o primjerenosti jest da se osobni podatci mogu kretati iz EGP-a u tu treću zemlju bez potrebe za primjenom alata za prijenos iz članka 46. Opće uredbe.
17. Odluke o primjerenosti mogu obuhvaćati cijelu zemlju ili samo jedan njezin dio. Odluke o primjerenosti mogu obuhvaćati sve prijenose podataka u neku zemlju ili samo neke vrste prijenosa (npr. u jednom sektoru).²⁹
18. Europska komisija objavljuje popis odluka o primjerenosti na svojem mrežnom mjestu.³⁰
19. Ako prenosite osobne podatke u treće zemlje, regije ili sektore obuhvaćene odlukom Komisije o primjerenosti (u mjeri u kojoj je ona primjenjiva), **ne morate poduzimati nikakve daljnje korake opisane u ovim preporukama.**³¹ Međutim, morate i dalje pratiti jesu li odluke o primjerenosti relevantne za vaše prijenose ukinute ili nevaljane.³²
20. Međutim, odluke o primjerenosti ne sprječavaju ispitanike u podnošenju pritužbe. Jednako tako ne sprječavaju nadzorna tijela u pokretanju postupka pred nacionalnim sudom ako imaju sumnje u valjanost odluke kako bi nacionalni sud mogao uputiti zahtjev za prethodnu odluku SEU-u u svrhu ispitivanja te valjanosti.³³

²⁸ Europska komisija ima ovlasti utvrditi, na temelju članka 45. Opće uredbe, pruža li zemlja izvan EU-a primjerenu razinu zaštite podataka. Jednako tako Europska komisija ima ovlasti utvrditi da međunarodna organizacija pruža primjerenu razinu zaštite.

²⁹ Članak 45. stavak 1. Opće uredbe.

³⁰ https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

³¹ Pod uvjetom da se vi i uvoznik podataka provedli mjere u svrhu ispunjavanja drugih obveza iz Opće uredbe; u suprotnom provedite te mjere.

³² Europska komisija mora s vremena na vrijeme preispitati sve odluke o primjerenosti i nadzirati osiguravaju li treće zemlje koje ostvaruju korist od odluka o primjerenosti i dalje primjerenu razinu zaštite (vidjeti članak 45. stavke 3. i 4. Opće uredbe). Osim toga, SEU može proglasiti odluke o primjerenosti nevaljanima (vidjeti presude Suda u predmetima C-362/14 (Schrems I) i C-311/18 (Schrems II)).

³³ C-311/18 (Schrems II), stavci 118. – 120. Nadzorna tijela ne mogu odbaciti odluku o primjerenosti i obustaviti ili zabraniti prijenose osobnih podataka u takve zemlje pozivajući se samo na neprimjerenost razine zaštite. Svoje ovlasti za obustavu ili zabranu prijenosa osobnih podataka u tu treću zemlju mogu izvršiti samo pozivajući se na druge osnove (npr. nedostatne sigurnosne mjere koje krše članak 32. Opće uredbe, nijedna pravna osnova nije valjan temelj za obradu podataka kao takva, a da se time krši članak 6. Opće uredbe o zaštiti podataka). Nadzorna tijela mogu potpuno samostalno ispitati je li prijenos tih podataka u skladu sa zahtjevima utvrđenima u Općoj uredbi i, prema potrebi, mogu pokrenuti postupak pred nacionalnim sudovima kako bi ti sudovi, ako sumnjaju u valjanost odluke Komisije o primjerenosti, uputili zahtjev za prethodnu odluku Sudu Europske unije u svrhu ispitivanja valjanosti odluke.

Primjer: G. Schrems, građanin Unije, uputio je pritužbu u lipnju 2013. irskom Povjerenstvu za zaštitu podataka i od tog nadzornog tijela zatražio da zabrani ili obustavi prijenos njegovih osobnih podataka iz poduzeća Facebook Ireland u Sjedinjene Američke Države jer je smatrao da pravo i praksa u toj zemlji ne jamče dovoljnu razinu zaštite osobnih podataka pohranjenih na njezinu državnom području od nadzornih aktivnosti koje tamo provode javna tijela. Povjerenstvo za zaštitu podataka odbacilo je pritužbu pozivajući se posebno na činjenicu da je Europska komisija u svojoj Odluci 2000/520 utvrdila da SAD osigurava primjerenu razinu zaštite prenesenih osobnih podataka u sklopu sustava „sigurne luke” (Odluka o „sigurnoj luci”). G. Schrems je osporio odluku Povjerenstva za zaštitu podataka i irski Visoki sud uputio je zahtjev za prethodnu odluku o valjanosti Odluke 2000/520 Sudu Europske unije (SEU). SEU je naknadno odlučio proglasiti Odluku 2000/520 Europske komisije o primjerenosti zaštite koju pružaju načela „sigurne luke” nevaljanom.³⁴

Alati za prijenos iz članka 46. Opće uredbe

21. Članak 46. Opće uredbe o zaštiti podataka navodi niz alata za prijenos koji sadrže „odgovarajuće zaštitne mjere” kojima se izvoznici mogu služiti za prijenos osobnih podataka u treće zemlje ako ne postoje relevantne odluke o primjerenosti. Glavne vrste alata za prijenos iz članka 46. Opće uredbe:
- standardne klauzule o zaštiti podataka;
 - obvezujuća korporativna pravila;
 - kodeksi ponašanja;
 - mehanizmi certificiranja;
 - *ad hoc* ugovorne klauzule.
22. Neovisno o tome koji alat za prijenos iz članka 46. Opće uredbe o zaštiti podataka odaberete, morate osigurati da će preneseni podatci u cjelini uživati u načelu istovjetnu razinu zaštite.
23. Alati za prijenos iz članka 46. Opće uredbe uglavnom sadrže odgovarajuće zaštitne mjere ugovorne naravi koje se mogu primijeniti na prijenose u sve treće zemlje. Situacija u trećoj zemlji u koju prenosite podatke može od vas i dalje zahtijevati da dopunite te alate za prijenos i u njima sadržane zaštitne mjere dodatnim mjerama kako biste osigurali u načelu istovjetnu razinu zaštite.³⁵

Odstupanja

24. Osim odluka o primjerenosti i alata za prijenos iz članka 46., Opća uredba sadrži i treći način kojim se dopuštaju prijenosi osobnih podataka u posebnim situacijama. Možda možete prenijeti osobne podatke na temelju odstupanja navedenih u članku 49. Opće uredbe, podložno posebnim uvjetima.
25. Članak 49. Opće uredbe posebne je naravi. Odstupanja sadržana u tom članku moraju se tumačiti restriktivno i uglavnom se odnose na aktivnosti obrade koje su povremene i ne ponavljaju se. Europski odbor za zaštitu podataka objavio je svoje Smjernice 2/2018 o odstupanjima iz članka 49. prema Uredbi 2016/679.³⁶
26. Prije nego što se pozovete na odstupanje iz članka 49. Opće uredbe, morate provjeriti ispunjava li vaš prijenos stroge uvjete koje ova odredba predviđa za svaki od njih.

³⁴ Predmet C-362/14 (Schrems I).

³⁵ C-311/18 (Schrems II), stavci 130. i 133. Vidjeti i točku 2.3. u nastavku.

³⁶ Za dodatne informacije vidjeti https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.

27. Ako se vaš prijenos ne može zakonito temeljiti na odluci o primjerenosti ili na odstupanju iz članka 49., nastavite s 3. korakom.

2.3 3. korak: procijenite je li alat za prijenos iz članka 46. na koji se oslanjate učinkovit s obzirom na sve okolnosti prijenosa

28. Nije dovoljno odabrati alat za prijenos iz članka 46. Opće uredbe. Alatom za prijenos mora se osigurati da razina zaštite zajamčena Općom uredbom nije narušena prijenosom.³⁷ Drugim riječima, alat za prijenos koji upotrebljavate mora biti učinkovit u praksi.
29. Učinkovit znači da se prenesenim osobnim podacima u trećoj zemlji pruža razina zaštite koja je u načelu istovjetna razini zaštite zajamčenoj u EGP-u.³⁸ To nije slučaj kad je uvoznik podataka spriječen u ispunjavanju obveza na temelju odabranog alata za prijenos iz članka 46. zbog zakonodavstva i praksi treće zemlje primjenjivih na prijenos.
30. Stoga morate procijeniti, prema potrebi u suradnji s uvoznikom, postoji li išta u pravu ili praksi treće zemlje što može dovesti u pitanje učinkovitost odgovarajućih zaštitnih mjera alata za prijenos iz članka 46. Opće uredbe na koji se oslanjate, u kontekstu konkretnog prijenosa. Prema potrebi, uvoznik podataka trebao bi vam dati na raspolaganje relevantne izvore i informacije u vezi s trećom zemljom u kojoj ima poslovni nastan i navesti zakone koji su mjerodavni za prijenos. Možete provjeriti i druge izvore informacija poput onih navedenih na ogleđnom popisu u prilogu 3.³⁹
31. Vaša bi procjena u obzir trebala uzeti sve dionike koji sudjeluju u prijenosu (npr. voditelje obrade, izvršitelje obrade i podizvršitelje koji obrađuju podatke u trećoj zemlji), koje ste utvrdili tijekom mapiranja prijenosa. Što je više voditelja obrade, izvršitelja obrade ili uvoznika uključeno, to će vaša procjena biti kompleksnija. U procjenu ćete morati uračunati i sve daljnje prijenose do kojih možete doći.
32. U tu svrhu trebate istražiti karakteristike svakog prijenosa i odrediti kako se domaći pravni poredak zemlje u koju se podatci prenose (ili dalje prenose) primjenjuje na te prijenose.
33. Mjerodavni pravni kontekst ovisit će o okolnostima prijenosa, konkretno:
- svrhama u koje se podatci prenose i obrađuju (npr. trgovanje, ljudski potencijali, pohrana, informatička podrška, klinička ispitivanja);
 - vrstama subjekata uključenih u obradu (javni/privatni; voditelj/izvršitelj obrade);
 - sektoru u kojem se prijenos odvija (npr. reklamna tehnologija, telekomunikacije, financije itd.);
 - kategorijama prenesenih osobnih podataka (npr. osobni podatci koji se odnose na djecu mogu biti obuhvaćeni područjem primjene posebnog zakonodavstva u trećoj zemlji);
 - pohranjuju li se podatci u trećoj zemlji ili se radi samo o pristupu na daljinu podacima pohranjenima u EU-u/EGP-u;
 - formatu podataka koji će se prenijeti (tj. nešifrirani/pseudonimizirani ili šifrirani podatci⁴⁰);

³⁷ Članak 44. Opće uredbe.

³⁸ C-311/18 (Schrems II), stavak 105. i drugo utvrđenje.

³⁹ Vidjeti i stavak 43. u nastavku.

⁴⁰ Neke treće zemlje ne dopuštaju uvoz šifriranih podataka.

- mogućnosti da će se podatci dalje prenositi iz te treće zemlje u neku drugu treću zemlju.⁴¹

34. Morat ćete procijeniti dovodi li neki od propisa iz mjerodavnog zakonodavstva u pitanje obveze sadržane u alatu za prijenos iz članka 46. koji ste odabrali. Trebate provjeriti mogu li se obveze koje ispitanicima omogućuju da ostvaruju svoja prava u kontekstu međunarodnih prijenosa (poput zahtjeva za pristup, ispravljanje i brisanje prenesenih podataka) učinkovito primijeniti u praksi i uvjeriti se da pravo treće zemlje odredišta ne priječi ispunjavanje tih obveza.
35. Morat ćete procijeniti relevantna opća pravila u mjeri u kojoj ona utječu na učinkovitu primjenu zaštitnih mjera sadržanih u alatu za prijenos iz članka 46. Opće uredbe i na temeljna prava pojedinaca (posebice pravo ispitanika na pravnu zaštitu u slučaju da javna tijela treće zemlje pristupe prenesenim podacima).
36. U svakom biste slučaju trebali obratiti posebnu pozornost na sve relevantne zakone, posebno zakone kojima se utvrđuju zahtjevi za otkrivanje osobnih podataka javnim tijelima ili kojima se takvim javnim tijelima daju ovlasti za pristup osobnim podacima (primjerice, u svrhe kaznenog progona, regulatornog nadzora i nacionalne sigurnosti). Ako su ti zahtjevi ili ovlasti ograničeni na ono što je nužno i razmjerno u demokratskom društvu,⁴² ne mogu dovoditi u pitanje obveze sadržane u alatu za prijenos iz članka 46. na koji se oslanjate.
37. Standardi EU-a, kao što su članci 47. i 52. Povelje Europske unije o temeljnim pravima, moraju se upotrebljavati kao referentna norma za procjenu je li takav pristup od strane tijela vlasti ograničen na ono što je nužno i razmjerno u demokratskom društvu i je li ispitanicima omogućena učinkovita pravna zaštita.
38. Tijekom provedbe te procjene bitni su i različiti elementi pravnog sustava te treće zemlje, npr. elementi navedeni u članku 45. stavku 2. Opće uredbe.⁴³ Na primjer, situacija u vezi s vladavinom prava u trećoj zemlji može biti relevantna za procjenu učinkovitosti dostupnih mehanizama kojima pojedinci mogu ostvariti pravnu zaštitu od neovlaštenog pristupa vlasti njihovim osobnim podacima. Postojanje sveobuhvatnog zakona za zaštitu osobnih podataka ili neovisnog nadležnog tijela za zaštitu podataka, kao i postupanje u skladu s međunarodnim instrumentima koji predviđaju mjere za zaštitu podataka, može pridonijeti osiguravanju razmjernosti zadiranja vlasti.⁴⁴
- ***
39. U preporukama Europskog odbora za zaštitu podataka iz Europskih ključnih jamstava navode se elementi koje je potrebno procijeniti kako bi se utvrdilo može li se pravni okvir kojim se regulira pristup osobnim podacima od strane javnih tijela u trećoj zemlji, odnosno agencija za nacionalnu sigurnost ili tijela kaznenog progona, smatrati opravdanim zadiranjem (koje tako ne dovodi u pitanje obveze preuzete primjenom alata za prijenos iz članka 46. Opće uredbe) ili ne. To se treba posebno pažljivo

⁴¹ Kad je voditelj obrade dao prethodno posebno ili opće pisano odobrenje u skladu s člankom 28. stavkom 2. Opće uredbe.

⁴² Vidjeti članke 47. i 52. Povelje Europske unije o temeljnim pravima, članak 23. stavak 1. Opće uredbe o zaštiti podataka, i Preporuke Europskog odbora za zaštitu podataka 02/2020 o Europskim ključnim jamstvima za mjere nadzora, 10. studenoga 2020., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

⁴³ C-311/18 (Schrems II), stavak 104.

⁴⁴ Primjerice: Konvencija 108 (Konvencija za zaštitu osoba glede automatizirane obrade osobnih podataka, ETS br. 108) ili Konvencija 108+ (Modernizirana konvencija za zaštitu osoba glede obrade osobnih podataka, CETS br. 223) predviđaju izvršive međunarodne pravne lijekove u slučaju povrede prava na zaštitu podataka i doprinose osiguravanju minimalne razine zaštite osobnih podataka i poštovanja privatnog života.

razmotriti kad je zakonodavstvo kojim se uređuje pristup podacima od strane javnih tijela dvosmisleno ili nije javno dostupno.

40. Kad se primjenjuju na situacije prijenose podataka na temelju alata za prijenos iz članka 46., Preporuke Europskog odbora za zaštitu podataka o Europskim ključnim jamstvima mogu usmjeravati izvoznika podataka i uvoznika podataka prilikom procjene zadiru li takve ovlasti neopravdano u obveze uvoznika podataka da osigura u načelu istovjetnu zaštitu.
41. Izostanak u načelu istovjetne razine zaštite bit će posebno očit kad zakonodavstvo ili praksa treće zemlje relevantna za vaš prijenos ne ispunjava zahtjeve Europskih ključnih jamstava.
42. Vaša se procjena prije svega treba temeljiti na javno dostupnom zakonodavstvu. Međutim, to u nekim situacijama neće biti dovoljno jer je zakonodavstvo u trećim zemljama možda nedostatno. U tom slučaju, ako i dalje želite prenijeti podatke, trebali biste istražiti druge relevantne i objektivne čimbenike⁴⁵, a ne se oslanjati na subjektivne čimbenike poput toga koliko je vjerojatno da će javna tijela pristupiti vašim podacima na način koji nije u skladu sa standardima EU-a. Tu biste procjenu trebali provesti s dužnom pažnjom i temeljito je dokumentirati jer ćete snositi odgovornost za odluku koji donesete na temelju te procjene.⁴⁶
43. Svoju procjenu možete upotpuniti informacijama dobivenima iz drugih izvora⁴⁷, kao što su:
 - elementi koji pokazuju da će tijelo vlasti treće zemlje nastojati pristupiti podacima neovisno o tome je li uvoznik podataka s time upoznat, s obzirom na prijavljene presedane, zakonodavstvo i praksu,
 - elementi koji pokazuju da će tijelo vlasti treće zemlje moći pristupiti podacima putem uvoznika podataka ili neizravnim presretanjem komunikacijskog kanala, s obzirom na prijavljene presedane, zakonske ovlasti i tehničke, financijske i ljudske resurse koji su mu na raspolaganju.
44. Svojom procjenom u konačnici možete utvrditi da alat za prijenos iz članka 46. Opće uredbe na koji se oslanjate i u njemu sadržane odgovarajuće zaštitne mjere:
 - učinkovito osiguravaju da se prenesenim osobnim podacima u trećoj zemlji pruža razina zaštite koja je u načelu istovjetna razini zaštite zajamčenoj u EGP-u. Zakonodavstvo i prakse treće zemlje primjenjive na prijenos uvozniku podataka omogućuju da ispuni svoje obveze na temelju odabranog alata za prijenos. Taj biste zaključak trebali ponovno procijeniti u odgovarajućim vremenskim razmacima ili kad dođe do značajnih promjena (vidjeti 6. korak),
 - ne osiguravaju učinkovito u načelu istovjetnu razinu zaštite. Uvoznik podataka ne može ispuniti svoje obveze zbog zakonodavstva i/ili praksi treće zemlje primjenjivih na prijenos. SEU je naglasio da u slučajevima u kojima su alati za prijenos iz članka 46. Opće uredbe manjkavi, izvoznik podataka snosi odgovornost da provede učinkovite dodatne mjere ili da ne prenosi osobne podatke.⁴⁸

⁴⁵ Vidjeti stavak 43. u nastavku i prilog 3.

⁴⁶ Članak 5. stavak 2. Opće uredbe.

⁴⁷ Također vidjeti prilog 3.

⁴⁸ SEU C-311/18 (Schrems II), stavci 134. – 135.

SEU je, na primjer, zaključio da članak 702. FISA-e (zakon Sjedinjenih Američkih Država) ne poštuje minimalne zaštitne mjere koje proizlaze iz načela proporcionalnosti na temelju prava Unije i da se ne može smatrati da je taj zakon ograničen na ono što je strogo nužno. To znači da razina zaštite programa ovlaštenih na temelju članka 702. FISA-e nije u načelu istovjetna zaštitnim mjerama propisanim na temelju prava Unije. Kao posljedica toga, ako se na uvoznika podataka ili bilo kojeg daljnjeg primatelja kojem uvoznik podataka može otkriti podatke primjenjuje članak 702. FISA-e⁴⁹, standardne klauzule o zaštiti podataka ili drugi alati za prijenos iz članka 46. Opće uredbe mogu se upotrebljavati za takav prijenos samo ako se pristup prenesenim podacima učini nemogućim ili neučinkovitim primjenom dodatnih tehničkih mjera.

2.4 4. korak: donesite dodatne mjere

45. Ako je procjenom iz 3. koraka otkriveno da alat za prijenos iz članka 46. Opće uredbe koji upotrebljavate nije učinkovit, trebate razmotriti, prema potrebi u suradnji s uvoznikom, postoje li dodatne mjere koje bi, kad bi se njima dopunile zaštitne mjere sadržane u alatima za prijenos, mogle osigurati da se prenesenim podacima u trećoj zemlji pruži razina zaštite koja je u načelu istovjetna razini zajamčenoj unutar EU-a.⁵⁰ „Dodatne mjere” po definiciji dopunjuju zaštitne mjere koje već pruža alat za prijenos iz članka 46. Opće uredbe.⁵¹
46. U svakom slučaju zasebno morate utvrditi koje bi dodatne mjere mogle biti učinkovite za skup prijenosa u određenu treću zemlju kada upotrebljavate određeni alat za prijenos iz članka 46. Opće uredbe. Moći ćete se nadovezati na prethodne procjene iz drugih koraka (prethodno opisani 1., 2. i 3. korak) i na temelju zaključaka iz tih koraka provjeriti potencijalnu učinkovitost dodatnih mjera u pogledu osiguravanja potrebne razine zaštite.
47. U načelu dodatne mjere mogu biti ugovorne, tehničke ili organizacijske naravi. Kombiniranjem različitih mjera na način da se one podupiru i nadopunjuju možete povećati razinu zaštite i time pridonijeti dostizanju standarda EU-a.
48. Ugovorne i organizacijske mjere same po sebi neće spriječiti pristup osobnim podacima od strane javnih tijela treće zemlje (kada to neopravdano zadire u obveze uvoznika podataka da osigura u načelu istovjetnu razinu zaštite). Doista, javit će se situacije u kojima će samo tehničke mjere moći spriječiti pristup osobnim podacima od strane javnih tijela u trećim zemljama ili ga učiniti neučinkovitim, posebno kada se podacima nastoji pristupiti u nadzorne svrhe.⁵² U takvim situacijama ugovornim i

⁴⁹ Članak 702. FISA-e primjenjiv je ako se podatci dobiju „od pružatelja usluga elektroničke komunikacije ili uz njegovu pomoć” (članak 702. FISA-e = glava 50. USC-a članak 1881.a, pod (h)(2)(A)(vi)), koji je definiran u glavi 50. USC-a članku 1881. pod (b)(4) kao

„(A) telekomunikacijski operater kako je taj izraz definiran u članku 153. glave 47.;

(B) pružatelj usluga elektroničke komunikacije, kako je taj izraz definiran u članku 2510. glave 18.;

(C) pružatelj usluga računarstva na daljinu, kako je taj izraz definiran u članku 2711. glave 18.;

(D) bilo koji drugi pružatelj komunikacijskih usluga koji ima pristup žičanim ili elektroničkim komunikacijama bilo u prijenosu ili u pohrani takvih komunikacija; ili

(E) službenik, zaposlenik ili posrednik subjekta opisanog u podstavku (A), (B), (C) ili (D).”

⁵⁰ C-311/18 (Schrems II), stavak 96.

⁵¹ Uvodna izjava 109. Opće uredbe i C-311/18 (Schrems II), stavak 133.

⁵² Kada takav pristup nadilazi ono što je nužno i razmjerno u demokratskom društvu; vidjeti članke 47. i 52. Povelje Europske unije o temeljnim pravima, članak 23. stavak 1. Opće uredbe, i Preporuke Europskog odbora za zaštitu podataka 02/2020 o Europskim ključnim jamstvima za mjere nadzora, 10. studenoga 2020., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

organizacijskim mjerama mogu se dopuniti tehničke mjere i može se ojačati sveukupna razina zaštite podataka, primjerice stvaranjem prepreka za pokušaje javnih tijela da pristupe podatcima na način koji nije u skladu sa standardima EU-a.

49. Prema potrebi u suradnji s uvoznikom podataka možete provjeriti sljedeći (ogledni) popis čimbenika kako biste utvrdili koje bi dodatne mjere bile najučinkovitije u zaštiti prenesenih podataka:

- format podataka koji će se prenijeti (tj. nešifrirani/pseudonimizirani ili šifrirani podatci),
- narav podataka,
- duljina i složenost tijeka rada obrade podataka, broj dionika uključenih u obradu i njihovi međusobni odnosi (npr. je li u prijenose uključeno više voditelja obrade ili i voditelji i izvršitelji obrade, jesu li uključeni izvršitelji obrade koji će prenijeti podatke od vas vašem uvozniku podataka (uzimajući u obzir mjerodavne odredbe koje se na njih primjenjuju na temelju zakonodavstva treće zemlje odredišta)),⁵³
- mogućnost da će se podatci dalje prenositi unutar te treće zemlje ili čak u neku drugu treću zemlju (npr. kad su uključeni podizvršitelji obrade uvoznika podataka⁵⁴).

Primjeri dodatnih mjera

50. Neke primjere tehničkih, ugovornih i organizacijskih mjera za razmatranje možete pronaći u oglednom popisu opisanom u prilogu 2.

51. Ako ste uspostavili učinkovite dodatne mjere koje u kombinaciji s odabranim alatom za prijenos iz članka 46. Opće uredbe dostižu razinu zaštite koja je sada u načelu istovjetna razini zaštite zajamčenoj unutar EGP-a, možete vršiti prijenose.
52. Ako ne možete pronaći ili provesti učinkovite dodatne mjere kojima se može osigurati da preneseni osobni podatci imaju u načelu istovjetnu razinu zaštite,⁵⁵ ne smijete početi prenositi osobne podatke u predmetnu treću zemlju na temelju alata za prijenos iz članka 46. Opće uredbe na koji se oslanjate. Ako već vršite prijenose, morate obustaviti ili potpuno prekinuti prijenos osobnih podataka.⁵⁶ U skladu sa zaštitnim mjerama sadržanima u alatu za prijenos iz članka 46. Opće uredbe na koji se oslanjate, podatci koje ste već prenijeli u tu treću zemlju i svi primjerci tih podataka trebaju vam biti vraćeni ili ih uvoznik treba u cijelosti uništiti.⁵⁷

⁵³ Opća uredba o zaštiti podataka određuje različite obveze za voditelje obrade i izvršitelje obrade. Prijenosi se mogu vršiti od voditelja obrade do voditelja obrade, između zajedničkih voditelja obrade, od voditelja obrade do izvršitelja obrade i, uz odobrenje voditelja obrade, od izvršitelja obrade do voditelja obrade ili od izvršitelja obrade do izvršitelja obrade.

⁵⁴ Vidjeti bilješku 25.

⁵⁵ Kada takav pristup nadilazi ono što je nužno i razmjerno u demokratskom društvu; vidjeti članke 47. i 52. Povelje Europske unije o temeljnim pravima, članak 23. stavak 1. Opće uredbe, i Preporuke Europskog odbora za zaštitu podataka 02/2020 o Europskim ključnim jamstvima za mjere nadzora, 10. studenoga 2020., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

⁵⁶ C-311/18 (Schrems II), stavak 135.

⁵⁷ Vidjeti klauzulu 12. u prilogu Odluke 87/2010 o standardnim ugovornim klauzulama; vidjeti (izbornu) Dodatnu klauzulu o raskidu u prilogu B Odluke 2004/915/EZ o standardnim ugovornim klauzulama.

Primjer: pravo treće zemlje zabranjuje dodatne mjere koje se utvrdili (npr. zabranjuje uporabu šifriranja) ili na drugi način sprječava njihovu učinkovitost. Ne smijete početi prenositi osobne podatke u tu zemlju ili morate zaustaviti postojeće prijenose u tu zemlju koji su u tijeku.

53. Ako odlučite nastaviti prijenos bez obzira na to što uvoznik nije u mogućnosti ispuniti obveze preuzete na temelju alata za prijenos iz članka 46. Opće uredbe, o tome trebate obavijestiti nadležno nadzorno tijelo u skladu s posebnim odredbama umetnutima u relevantni alat za prijenos iz članka 46. Opće uredbe.⁵⁸ Nadležno nadzorno tijelo obustavit će ili zabraniti prijenose podataka u onim slučajevima u kojima utvrdi da se ne može osigurati u načelu istovjetna razina zaštite.⁵⁹
54. Nadležno nadzorno tijelo može nametnuti bilo kakve druge korektivne mjere (npr. novčanu kaznu) ako, unatoč činjenici da ne možete dokazati u načelu istovjetnu razinu zaštite u trećoj zemlji, započnete ili nastavite prijenos podataka.

2.5 5. korak: postupovni koraci ako ste utvrdili učinkovite dodatne mjere

55. Postupovni koraci koje ćete možda morati provesti ako ste utvrdili učinkovite dodatne mjere koje treba uspostaviti, a koje se mogu razlikovati ovisno o alatu za prijenos iz članka 46. Opće uredbe koji upotrebljavate ili planirate upotrebljavati.

2.5.1 Standardne klauzule o zaštiti podataka (članak 46. stavak 2. točke (c) i (d) Opće uredbe)

56. Kada namjeravate uspostaviti dodatne mjere uz standardne ugovorne klauzule, ne morate tražiti ovlaštenje nadležnog nadzornog tijela da biste dodali takve klauzule ili dodatne zaštitne mjere pod uvjetom da utvrđene dodatne mjere izravno ili neizravno ne proturječe standardnim ugovornim klauzulama i da su dostatne da bi se osiguralo da razina zaštite zajamčena Općom uredbom nije narušena.⁶⁰ Izvoznik i uvoznik podataka moraju osigurati da se dodatne klauzule ne mogu protumačiti na način da ograničavaju prava i obveze iz standardnih ugovornih klauzula ili na način da umanjuju razinu zaštite podataka. To biste trebali moći dokazati, uključujući nedvosmislenost svih klauzula, u skladu s načelom odgovornosti i svojom obvezom da osigurate dostatnu razinu zaštite podataka. Nadležna nadzorna tijela imaju ovlasti preispitati te dodatne klauzule kad je to potrebno (npr. u slučaju pritužbe ili istrage na vlastitu inicijativu).

⁵⁸ Vidjeti Često postavljana pitanja Europskog odbora za zaštitu podataka o presudi Suda Europske unije u predmetu C-311/18 – Data Protection Commissioner protiv Facebook Ireland Ltd i Maximilliana Schremsa donesena 23. srpnja 2020., posebno pitanja br. 5, 6 i 9. Također vidjeti klauzulu 4. točku (g) Odluke Komisije 2010/87/EU, klauzulu 5. točku (a) Odluke Komisije 2001/497/EZ i Prilog „Skup II.” klauzula II(c) Odluke Komisije 2004/915/EZ.

⁵⁹ C-311/18 (Schrems II), stavci 113. i 121.

⁶⁰ Uvodna izjava 109. Opće uredbe navodi: „Mogućnost da se voditelj obrade ili izvršitelj obrade koristi standardnim klauzulama o zaštiti podataka koje je donijela Komisija ili nadzorno tijelo ne bi trebala sprečavati mogućnost voditelja obrade ili izvršitelja obrade ni da uključe standardne klauzule o zaštiti podataka u širi ugovor, kao što je ugovor između izvršitelja obrade i drugog izvršitelja obrade, ni da dodaju druge klauzule ili dodatne zaštitne mjere pod uvjetom da one izravno ili neizravno ne proturječe standardnim ugovornim klauzulama koje je donijela Komisija ili nadzorno tijelo ili ne dovode u pitanje temeljna prava ili slobode ispitanika.” Slične su odredbe navedene u skupovima standardnih ugovornih klauzula koje je usvojila Europska komisija na temelju Direktive 95/45/EZ.

57. Ako namjeravate izmijeniti standardne klauzule o zaštiti podataka ili ako dodatne mjere koje ste primijenili izravno ili neizravno „proturječe” standardnim ugovornim klauzulama, više se ne smatra da se oslanjate na standardne ugovorne klauzule⁶¹ i morate zatražiti odobrenje nadležnog nadzornog tijela u skladu s člankom 46. stavkom 3. točkom (a) Opće uredbe.

2.5.2 Obvezujuća korporativna pravila (članak 46. stavak 2. točka (b) Opće uredbe o zaštiti podataka)

58. Obrazloženje izneseno u presudi Schrems II primjenjuje se i na druge instrumente za prijenos u skladu s člankom 46. stavkom 2. Opće uredbe jer su svi ti instrumenti u osnovi ugovorne naravi, stoga u njima predviđena jamstva i obveze koje su preuzele ugovorne strane ne mogu obvezivati javna tijela treće zemlje.⁶²
59. Presuda Schrems II relevantna je za prijenose osobnih podataka na temelju obvezujućih korporativnih pravila jer zakoni trećih zemalja mogu utjecati na zaštitu koju pružaju takvi instrumenti. Još uvijek se vode rasprave o točnom utjecaju presude Schrems II na obvezujuća korporativna pravila. Europski odbor za zaštitu podataka objavit će u referentnim dokumentima WP 256/257 što je prije moguće više detalja o tome je li u obvezujuća korporativna pravila potrebno uključiti kakve dodatne obveze.⁶³
60. Sud je istaknuo da izvoznik podataka i uvoznik podataka imaju odgovornost procijeniti poštuje li se u predmetnoj trećoj zemlji razina zaštite propisana pravom Unije kako bi utvrdili mogu li se u praksi poštovati jamstva dana standardnim ugovornim klauzulama ili obvezujućim korporativnim pravilima. Ako to nije slučaj, trebate procijeniti možete li pružiti dodatne mjere da bi se osigurala razina zaštite koja je u načelu istovjetna onoj koja se pruža u EGP-u i narušavaju li propisi ili praksa treće zemlje te dodatne mjere tako da sprječavaju njihovu učinkovitost.

2.5.3 *Ad hoc* ugovorne klauzule (članak 46. stavak 3. točka (a) Opće uredbe)

61. Obrazloženje izneseno u presudi Schrems II primjenjuje se i na druge instrumente za prijenos u skladu s člankom 46. stavkom 2. Opće uredbe jer su svi ti instrumenti u osnovi ugovorne naravi, stoga u njima predviđena jamstva i obveze koje su preuzele ugovorne strane ne mogu obvezivati javna tijela treće zemlje.⁶⁴ Presuda Schrems II stoga je relevantna za prijenose osobnih podataka na temelju *ad hoc* ugovornih klauzula jer zakoni trećih zemalja mogu utjecati na zaštitu koju pružaju takvi instrumenti. Još uvijek se vode rasprave o točnom utjecaju presude Schrems II na *ad hoc* ugovorne klauzule. Europski odbor za zaštitu podataka objavit će više detalja što je prije moguće.

⁶¹ Vidjeti, po analogiji, Mišljenje Europskog odbora za zaštitu podataka 17/2020 o nacrtu standardnih ugovornih klauzula koje je predalo slovensko nadzorno tijelo (članak 28. stavak 8. Opće uredbe) o članku 28. o već donesenim standardnim ugovornim klauzulama, koje mišljenje sadrži sličnu odredbu („Uz to, Odbor podsjeća da mogućnost uporabe standardnih ugovornih klauzula koje je donijelo nadzorno tijelo ne sprječava strane da dodaju druge klauzule ili dodatne zaštitne mjere pod uvjetom da one izravno ili neizravno ne proturječe donesenim standardnim ugovornim klauzulama ili da ne narušavaju temeljna prava ili slobode ispitanika. Nadalje, ako se standardne klauzule o zaštiti podataka izmijene, više se neće smatrati da su strane primijenile donesene standardne ugovorne klauzule.”), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28scs_si_en.pdf.

⁶² SEU, C-311/18 (Schrems II), stavak 132.

⁶³ Radna skupina iz članka 29., Radni dokument kojim se utvrđuje tablica s elementima i načelima koji se nalaze u obvezujućim korporativnim pravilima, kako je posljednji put revidiran i donesen 6. veljače 2018., WP 256 rev.01; Radna skupina iz članka 29., Radni dokument kojim se utvrđuje tablica s elementima i načelima koji se nalaze u obvezujućim korporativnim pravilima, kako je posljednji put revidiran i donesen 6. veljače 2018., WP 257 rev.01.

⁶⁴ SEU, C-311/18 (Schrems II), stavak 132.

2.6 6. korak: ponovna procjena u odgovarajućim vremenskim razmacima

62. Morate nazirati, kontinuirano i prema potrebi u suradnji s uvoznicima podataka, promjene u trećoj zemlji u koju ste prenijeli osobne podatke, a koje bi mogli utjecati na vašu izvornu procjenu razine zaštite i na odluke koje ste možda donijeti na temelju te procjene u vezi s prijenosima. Odgovornost je kontinuirana obveza (članak 5. stavak 2. Opće uredbe).
63. Trebali biste uspostaviti dovoljno dobre mehanizme kako biste osigurali da ćete odmah obustaviti ili prekinuti prijenose osobnih podataka u sljedećim situacijama:
 - uvoznik je prekršio obveze koje je preuzeo na temelju alata za prijenos iz članka 46. Opće uredbe ili ih ne može ispuniti, ili
 - dodatne mjere više nisu učinkovite u toj trećoj zemlji.

3 ZAKLJUČAK

64. Opća uredba o zaštiti podataka propisuje pravila o obradi osobnih podataka u EGP-u i na taj način omogućuje sloboda kretanja osobnih podataka unutar EGP-a. Poglavlje V. Opće uredbe o zaštiti podataka uređuje prijenose osobnih podataka u treće zemlje i postavlja stroge kriterije: prijenos ne smije narušiti razinu zaštite pojedinaca zajamčenu Općom uredbom o zaštiti podataka (članak 44. Opće uredbe. Presuda SEU C-311/18 (Schrems II) naglašava potrebu da se osigura kontinuitet u razini zaštite koju pruža Opća uredba o zaštiti podataka kad su u pitanju osobni podatci preneseni u treću zemlju.⁶⁵
65. Kako biste osigurali u načelu istovjetnu razinu zaštite podataka, prvo morate detaljno poznavati svoje prijenose. Usto morate provjeriti da su podatci koje prenosite primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se podatci prenose u treću zemlju i u njoj obrađuju.
66. Također morate utvrditi na koje se alate za prijenos oslanjate u svojim prijenosima podataka. Ako alat za prijenos nije odluka o primjerenosti, morate u svakom slučaju zasebno provjeriti narušava li pravo ili praksa treće zemlje odredišta zaštitne mjere sadržane u alatu za prijenos iz članka 46. Opće uredbe o zaštiti podataka u kontekstu vaših prijenosa. Ako sam alat za prijenos iz članka 46. Opće uredbe ne uspije postići u načelu istovjetnu razinu zaštite za osobne podatke koje prenosite, možete ga dopuniti dodatnim mjerama.
67. Ako ne možete pronaći ili provesti učinkovite dodatne mjere kojima se može osigurati da preneseni osobni podatci imaju u načelu istovjetnu razinu zaštite, ne smijete početi prenositi osobne podatke u predmetnu treću zemlju na temelju odabranoga alata za prijenos. Ako već vršite prijenose, morate odmah obustaviti ili potpuno prekinuti prijenos osobnih podataka.
68. Nadležno nadzorno tijelo ima ovlasti obustaviti ili prekinuti prijenose osobnih podataka u treću zemlju ako nije osigurana zaštita prenesenih podataka koja je propisana pravom Unije, posebno člancima 45. i 46. Opće uredbe i Poveljom o temeljnim pravima.

Za Europski odbor za zaštitu podataka

Predsjednica

(Andrea Jelinek)

⁶⁵ C-311/18 (Schrems II), stavak 93.

PRILOG 1.: DEFINICIJE

- „Treća zemlja” znači bilo koja zemlja koja nije država članica EGP-a.
- „EGP” znači Europski gospodarski prostor i uključuje sve države članice Europske unije i Island, Norvešku i Lihtenštajn. Opća uredba o zaštiti podataka primjenjuje se na potonje na temelju Sporazuma o Europskom gospodarskom prostoru, posebno njegovih priloga XI. i protokola 37.
- „Opća uredba o zaštiti podataka” znači Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka).
- „Povelja” znači Povelja Europske unije o temeljnim pravima, SL C 326, 26. 10. 2012., str. 391. – 407.
- „SEU” ili „Sud” znači Sud Europske unije. Predstavlja pravosudno tijelo Europske unije i u suradnji sa sudovima država članica osigurava jedinstvenu primjenu i tumačenje prava Unije.
- „Izvoznik podataka” znači voditelj obrade ili izvršitelj obrade unutar EGP-a koji prenosi osobne podatke voditelju obrade ili izvršitelju obrade u trećoj zemlji.
- „Uvoznik podataka” znači voditelj obrade ili izvršitelj obrade u trećoj zemlji koji prima ili ostvaruje pristup osobnim podacima prenesenima iz EGP-a.
- „Alat za prijenos iz članka 46. Opće uredbe o zaštiti podataka” odnosi se na odgovarajuće zaštitne mjere iz članka 46. Opće uredbe o zaštiti podataka koje izvoznici podataka uspostavljaju prilikom prijenosa osobnih podataka u treću zemlju u izostanku odluke o primjerenosti u skladu s člankom 45. stavkom 3. Opće uredbe o zaštiti podataka. Članak 46. stavci 2. i 3. Opće uredbe o zaštiti podataka sadrže popis alata za prijenos iz članka 46. Opće uredbe o zaštiti podataka koje voditelji obrade i izvršitelji obrade mogu upotrebljavati.
- „Standardne ugovorne klauzule” znači standardne klauzule o zaštiti podataka (ili „standardne ugovorne klauzule”) koje je Europska komisija usvojila za prijenose osobnih podataka između voditelja obrade ili izvršitelja obrade u EGP-u i voditelja obrade ili izvršitelja obrade izvan EGP-a. Standardne ugovorne klauzule koje je usvojila Europska komisija alat su za prijenos na temelju Opće uredbe, u skladu s člankom 46. stavkom 2. točkom (c) i člankom 46. stavkom 5. Opće uredbe o zaštiti podataka.

PRILOG 2.: PRIMJERI DODATNIH MJERA

69. Sljedeće mjere predstavljaju primjere dodatnih mjera koje možete razmotriti kad dosegnete 4. korak „Donesite dodatne mjere”. Popis ne sadrži sve moguće mjere. Odabir i provedba jedne ili više ovih mjera neće nužno i sustavno osigurati da vaš prijenos zadovoljava standard u načelu istovjetne zaštite propisan pravom Unije. Trebate odabrati one dodatne mjere kojima se može učinkovito osigurati ta razina zaštite u odnosu na vaše prijenose.
70. Bilo koja dodatna mjera može se smatrati učinkovitom u smislu presude SEU-a „Schrems II” ako otklanja određene nedostatke koje ste utvrdili u svojoj procjeni pravne situacije u trećoj zemlji i samo u mjeri u kojoj otklanja te nedostatke. Ako u konačnici ne možete osigurati u načelu istovjetnu razinu zaštite, ne smijete prenositi osobne podatke.
71. Kao voditelj obrade ili izvršitelj obrade možda već morate provesti neke mjere opisane u ovom prilogu čak i ako se na vašeg uvoznika podataka primjenjuje odluka o primjerenosti, kao što ih možda morate provesti i kad obrađujete podatke unutar EGP-a.⁶⁶

Tehničke mjere

72. U ovom se odjeljku opisuju ogledni primjeri tehničkih mjera kojima se mogu dopuniti zaštitne mjere sadržane u alatima za prijenos iz članka 46. Opće uredbe kako bi se osigurala usklađenost s razinom zaštite koju propisuje pravo Unije u kontekstu prijenosa osobnih podataka u treću zemlju. Te su mjere posebno potrebe u slučajevima u kojima pravo te države uvozniku podataka nameće obveze koje su protivne zaštitnim mjerama sadržanima u alatima za prijenos iz članka 46. Opće uredbe i koje, posebice, mogu ugroziti ugovorno jamstvo o načelu istovjetne razine zaštite od pristupa javnih tijela treće zemlje tim podacima⁶⁷.
73. Kako bi se postigla veća jasnoća, u ovom se odjeljku prvo navode tehničke mjere koje bi potencijalno mogle biti učinkovite u određenim scenarijima / slučajevima uporabe kako bi se osigurala u načelu istovjetna razina zaštite. U nastavku odjeljka navode se neki scenariji / slučajevi uporabe za koje nije utvrđena nijedna tehnička mjera kojom bi se mogla osigurati ta razina zaštite.

Scenariji za koje bi se mogle utvrditi učinkovite mjere

74. Mjere navedene u nastavku namijenjene su osiguravanju da pristup prenesenim podacima od strane javnih tijela u trećim zemljama ne ugrozi učinkovitost odgovarajućih zaštitnih mjera sadržanih u alatima za prijenos iz članka 46. Opće uredbe. Te se mjere primjenjuju čak i ako je pristup javnih tijela u skladu sa zakonom zemlje uvoznika, ako takav pristup nadilazi ono što je nužno i razmjerno u demokratskom društvu⁶⁸. Cilj je ovih mjera onemogućiti pristup podacima koji može uzrokovati povredu tako što sprječavaju javna tijela u identificiranju ispitanika, izvođenju informacija o njima, izdvajanju ispitanika u drugom kontekstu ili povezivanju prenesenih podataka s drugim skupovima podataka koje javna

⁶⁶ Članak 5. stavak 2. i članak 32. Opće uredbe.

⁶⁷ C-311/18 (Schrems II), stavak 135.

⁶⁸ Vidjeti članke 47. i 52. Povelje Europske unije o temeljnim pravima, članak 23. stavak 1. Opće uredbe o zaštiti podataka i Preporuke Europskog odbora za zaštitu podataka o Europskim ključnim jamstvima za mjere nadzora.

tijela možda posjeduju, a koji mogu sadržavati, među ostalim podacima, mrežne identifikatore koje pružaju uređaji, aplikacije, alati i protokoli koje ispitanici upotrebljavaju u drugim kontekstima.

75. Javna tijela u trećim zemljama mogu nastojati pristupiti prenesenim podacima
- a) u postupku provoza pristupanjem komunikacijskim putovima koji se upotrebljavaju kako bi se podatci prenijeli u zemlju primateljicu. Taj pristup može biti pasivan u kojem se slučaju sadržaj komunikacije, moguće nakon postupka odabira, jednostavno kopira. Međutim, taj pristup može biti i aktivan u smislu da se javna tijela umiješaju u komunikacijski postupak ne samo čitanjem sadržaja, već manipuliranjem dijelovima komunikacije ili njihovim potiskivanjem,
 - b) dok su u posjedu predviđenog primatelja podataka, bilo da sami pristupe opremi za obradu podataka bilo da od primatelja podataka zahtijevaju da locira i izdvoji podatke od interesa i preda ih javnim tijelima.
76. U ovom se odjeljku razmatraju scenariji u kojima se primjenjuju mjere koje su učinkovite u oba slučaja. Ako je samo jedna vrsta pristupa predviđena pravom države primateljice, mogu se primijeniti različite dodatne mjere koje mogu biti dostatne u danoj okolnosti konkretnog prijenosa. Stoga izvoznik podataka mora pažljivo analizirati, uz pomoć uvoznika podataka, koje se obveze nameću potonjem.

Na primjer, uvoznici podataka u SAD-u na koje se primjenjuje glava 50. USC-a, članak 1881.a (članak 702. FISA-e) imaju izravnu obvezu omogućiti pristup podacima koje posjeduju, čuvaju ili nadziru ili predati takve uvezene osobne podatke. To se može odnositi i na sve kriptografske ključeve koji su potrebni da bi se podatke učinilo razumljivima.

77. Scenariji opisuju posebne okolnosti i poduzete mjere. Sve promjene u scenariju mogu dovesti do drugačijih zaključaka.
78. Voditelji obrade možda će morati primijeniti neke ili sve ovdje opisane mjere neovisno o razini zaštite koju pružaju zakoni primjenjivi na uvoznika podataka jer su one potrebne kako bi se ispunili zahtjevi članaka 25. i 32. Opće uredbe u konkretnim okolnostima prijenosa. Drugim riječima, izvoznici će možda morati provesti mjere opisane u ovom dokumentu čak i ako se na uvoznike njihovih podataka primjenjuje odluka o primjerenosti, kao što ih voditelji obrade i izvršitelji obrade možda moraju provesti i kad se podatci obrađuju unutar EGP-a.

1. slučaj uporabe: pohrana podataka za izradu sigurnosne kopije i u druge svrhe za koje nije potreban pristup nešifriranim podacima

79. Izvoznik podataka upotrebljava usluge pružatelja smještaja informacija na poslužitelju u trećoj zemlji kako bi pohranio osobne podatke, npr. u svrhe izrade sigurnosne kopije.

Ako vrijedi sljedeće:

1. osobni podatci obrađuju se uz primjenu snažnog šifriranja prije prijenosa,
2. algoritam šifriranja i njegova parametrizacija (npr. duljina ključa, način rada, ako je primjenjivo) u skladu su s najnovijim dostignućima i mogu se smatrati snažnima u odnosu na kriptanalizu koju provode javna tijela u zemlji primateljici, uzimajući u obzir resurse i tehničke mogućnosti (npr. računalna snaga potrebna za napade grubom silom) koji su im na raspolaganju,
3. snaga šifriranja uzima u obzir određeno vremensko razdoblje tijekom kojeg se mora očuvati povjerljivost šifriranih osobnih podataka,

4. algoritam šifriranja besprijekorno je primijenjen pravilno održavanim softverom čija je usklađenost sa specifikacijama odabranog algoritma provjerena, npr. certificiranjem,
5. ključevima se pouzdano upravlja (stvaranje, upravljanje, pohranjivanje te, ako je potrebno, povezivanje s identitetom namjeravanog primatelja, opoziv), i
6. ključevi ostaju pod isključivom kontrolom izvoznika podataka ili drugih subjekata kojima je taj zadatak povjeren, a koji se nalaze u EGP-u ili trećoj zemlji, na državnom području ili u jednom ili više određenih sektora unutar treće zemlje, ili u međunarodnoj organizaciji za koju je Komisija utvrdila u skladu s člankom 45. Opće uredbe da se osigurava primjerena razina zaštite,

Europski odbor za zaštitu podataka smatra da provedeno šifriranje predstavlja učinkovitu dodatnu mjeru.

2. slučaj uporabe: prijenos pseudonimiziranih podataka

80. Izvoznik podataka prvo pseudonimizira podatke koje posjeduje, a zatim ih prenosi u treću zemlju na analizu, npr. u svrhu istraživanja.

Ako vrijedi sljedeće:

1. izvoznik podataka prenosi osobne podatke koji su obrađeni na način da se osobni podatci više ne mogu pripisati određenom ispitaniku i ne mogu se upotrijebiti da bi se ispitanika izdvojilo u većoj skupini bez uporabe dodatnih informacija⁶⁹,
2. dodatne informacije posjeduje isključivo izvoznik podataka i drže se odvojeno u državi članici ili u trećoj zemlji, na državnom području ili u jednom ili više određenih sektora unutar treće zemlje, ili u međunarodnoj organizaciji za koju je Komisija utvrdila u skladu s člankom 45. Opće uredbe da se osigurava primjerena razina zaštite,
3. otkrivanje ili neovlaštena uporaba tih dodatnih informacija spriječena je odgovarajućim tehničkim ili organizacijskim zaštitnim mjerama, osigurano je da izvoznik podataka zadržava isključivu kontrolu nad algoritmom ili repozitorijem koji omogućuje ponovno utvrđivanje identiteta s pomoću dodatnih informacija, i
4. voditelj obrade utvrdio je temeljitom analizom podataka u pitanju, uzimajući u obzir sve informacije koje javna tijela zemlje primateljice možda posjeduju, da se pseudonimizirani osobni podatci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi čak i ako se usporede s takvim informacijama,

Europski odbor za zaštitu podataka smatra da provedena pseudonimizacija predstavlja učinkovitu dodatnu mjeru.

⁶⁹ U skladu s člankom 4. stavkom 5. Opće uredbe: „pseudonimizacija’ znači obrada osobnih podataka na način da se osobni podatci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podatci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi;”.

81. Imajte na umu da u brojnim situacijama čimbenici svojstveni za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet pojedinca, njihov fizički položaj ili njihova interakcija s internetskom uslugom u određenim trenucima⁷⁰ mogu omogućiti utvrđivanje identiteta te osobe čak i ako se ime, adresa ili drugi jednostavni identifikatori osobe izostave.
82. To osobito vrijedi kad se podatci odnose na uporabu informacijskih usluga (vrijeme pristupa, redoslijed značajki kojima se pristupilo, karakteristike upotrijebljenog uređaja itd.). Pružatelji tih usluga, kao i uvoznik osobnih podataka, mogu biti obvezni omogućiti pristup istim javnim tijelima u njihovoj jurisdikciji, koja će javna tijela zatim vjerojatno posjedovati podatke o uporabi tih informacijskih usluga od strane ciljanih osoba.
83. Štoviše, s obzirom na to da je uporaba nekih informacijskih usluga po svojoj naravi javna ili s obzirom na to da ih subjekti sa značajnim resursima mogu iskoristiti, voditelji obrade moraju biti posebno oprezni s obzirom na to da javna tijela u njihovoj jurisdikciji vjerojatno posjeduju podatke o uporabi informacijskih usluga od strane ciljane osobe.

3. slučaj uporabe: šifrirani podatci koji se samo provozе kroz treće zemlje

84. Izvoznik podataka želi prenijeti podatke u odredište za koje je priznato da nudi primjerenu zaštitu u skladu s člankom 45. Opće uredbe. Podatci se usmjeravaju preko treće zemlje.

Ako vrijedi sljedeće:

1. izvoznik podataka prenosi osobne podatke uvozniku podataka u jurisdikciji u kojoj je osigurana primjerena zaštita, podatci se šalju putem interneta i mogu se geografski usmjeravati kroz treću zemlju koja ne nudi u načelu istovjetnu razinu zaštite,
2. upotrebljava se šifriranje za slanje i osigurano je da su upotrijebljeni protokoli za šifriranje u skladu s najmodernijim dostignućima i pružaju učinkovitu zaštitu od aktivnih i pasivnih napada resursima za koje je poznato da su dostupni javnim tijelima treće zemlje,
3. dešifriranje je moguće samo izvan treće zemlje u pitanju,
4. subjekti uključeni u komunikaciju suglasni su oko pouzdanog certifikacijskog tijela koje izdaje certifikat javnog ključa ili oko infrastrukture javnog ključa,
5. upotrebljavaju posebne zaštitne i najmodernije mjere protiv aktivnih i pasivnih napada na podatke šifrirane za slanje,
6. u slučaju da šifriranje za slanje samo po sebi ne pruža odgovarajuću zaštitu zbog iskustva s ranjivostima infrastrukture ili softvera koji se upotrebljavaju, osobni podatci također se šifriraju s kraja na kraj na aplikacijskom sloju primjenom najmodernijih metoda šifriranja,
7. algoritam šifriranja i njegova parametrizacija (npr. duljina ključa, način rada, ako je primjenjivo) u skladu su s najnovijim dostignućima i mogu se smatrati snažnima u odnosu na kriptanalizu koju provode javna tijela u zemlji kroz koju podatci prolaze, uzimajući u obzir resurse i tehničke mogućnosti (npr. računalna snaga potrebna za napade grubom silom) koji su im na raspolaganju,
8. snaga šifriranja uzima u obzir određeno vremensko razdoblje tijekom kojeg se mora očuvati povjerljivost šifriranih osobnih podataka,

⁷⁰ Članak 4. stavak 1. Opće uredbe: „osobni podatci” znači svi podatci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik”); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podatci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca;”.

9. algoritam šifriranja besprijekorno je primijenjen pravilno održavanim softverom čija je usklađenost sa specifikacijama odabranog algoritma provjerena, npr. certificiranjem,
10. isključeno je postojanje stražnjih ulaza (u hardver ili softver),
11. ključevima pouzdano upravlja (stvaranje, upravljanje, pohranjivanje te, ako je potrebno, povezivanje s identitetom namjeravanog primatelja, opoziv) izvoznik ili subjekt kojem izvoznik vjeruje u jurisdikciji u kojoj se nudi u načelu istovjetna razina zaštite,

Europski odbor za zaštitu podataka smatra da šifriranje za slanje, po potrebi u kombinaciji sa šifriranjem sadržaja s kraja na kraj, predstavlja učinkovitu dodatnu mjeru.

4. slučaj uporabe: zaštićen primatelj

85. Izvoznik podataka prenosi osobne podatke uvozniku podataka u trećoj zemlji koji je posebno zaštićen pravom te države, npr. u svrhu zajedničkog liječenja bolesnika ili pružanja pravnih usluga klijentu.

Ako vrijedi sljedeće:

1. pravo treće zemlje daje izuzeće uvozniku podataka rezidentu u odnosu na pristup podacima koji može uzrokovati povredu za podatke koje taj primatelj posjeduje u određenu svrhu, npr. na temelju obveze čuvanja poslovne tajne koja se primjenjuje na uvoznika podataka,
2. izuzeće se primjenjuje na sve informacije u posjedu uvoznika podataka koje se mogu upotrijebiti kako bi se zaobišla zaštita povjerljivih informacija (kriptografski ključevi, lozinke, druge vjerodajnice itd.),
3. uvoznik podataka ne upotrebljava usluge izvršitelja obrade na način koji javnim tijelima omogućuje da pristupe podacima dok su u posjedu izvršitelja obrade, te jednako tako ne prosljeđuje podatke drugom subjektu koji nije zaštićen, na temelju alata za prijenos iz članka 46. Opće uredbe,
4. osobni se podatci šifriraju prije prijenosa metodom koja je u skladu s najmodernijim dostignućima i koja jamči da dešifriranje neće biti moguće bez ključa za dešifriranje (šifriranje s kraja na kraj) tijekom cijelog razdoblja u kojem podatci trebaju biti zaštićeni,
5. ključ za dešifriranje posjeduje isključivo zaštićeni uvoznik podataka i ključ je odgovarajuće zaštićen od neovlaštene uporabe ili otkrivanja tehničkim i organizacijskim mjerama koje su u skladu s najmodernijim dostignućima, i
6. izvoznik podataka pouzdano je utvrdio da ključ za šifriranje koji namjerava upotrijebiti odgovara ključu za dešifriranje u posjedu primatelja,

Europski odbor za zaštitu podataka smatra da provedeno šifriranje za slanje predstavlja učinkovitu dodatnu mjeru.

5. slučaj uporabe: podijeljena obrada ili obrada podataka na više strana

86. Izvoznik podataka želi da se osobni podatci obrađuju zajednički ili da ih obrađuju dva ili više neovisnih izvršitelja obrade koji se nalaze u različitim jurisdikcijama bez da im otkrije sadržaj podataka. Prije prijenosa podatke dijeli na način da nijedan dio koji pojedini izvršitelj obrade primi nije dostatan za cijelu ili djelomičnu rekonstrukciju osobnih podataka. Izvoznik podataka prima rezultat obrade zasebno od svakog izvršitelja obrade i spaja primljene dijelove kako bi dobio konačan rezultat koji može predstavljati osobne ili agregirane podatke.

Ako vrijedi sljedeće:

1. izvoznik podataka obrađuje osobne podatke na način da se osobni podatci dijele na dva ili više dijela od kojih se svaki dio više ne može tumačiti ili pripisati određenom ispitaniku bez uporabe dodatnih informacija,
2. svaki se dio prenosi zasebnom izvršitelju obrade u drugoj jurisdikciji,
3. izvršitelji obrade po izboru obrađuju podatke zajedno, npr. upotrebljavaju sigurno višekorisničko računanje na način da se nijednom od njih ne otkrivaju podatci koje nisu posjedovali prije računanja,
4. algoritam koji se upotrebljava za zajedničko računanje zaštićen je od aktivnih napadača,
5. ne postoje dokazi o suradnji između javnih tijela u zasebnim jurisdikcijama u kojem se svaki od izvršitelja obrade nalazi, koja bi im omogućila da pristupe svim skupovima osobnih podataka u posjedu izvršitelja obrade i da rekonstruiraju i iskoriste sadržaj osobnih podataka u nešifriranom obliku u okolnostima u kojima takvo iskorištavanje ne bi poštovalo bit temeljnih prava i sloboda ispitanika. Jednako tako, javna tijela bilo koje od tih zemalja ne bi trebala imati ovlasti pristupiti osobnim podacima u posjedu izvršitelja obrade u svim predmetnim jurisdikcijama,
6. voditelj obrade utvrdio je temeljitom analizom podataka u pitanju, uzimajući u obzir sve informacije koje javna tijela zemalja primateljica možda posjeduju, da se dijelovi osobnih podataka koje prenosi izvršiteljima obrade ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi čak i ako se usporede s takvim informacijama,

Europski odbor za zaštitu podataka smatra da podijeljena obrada predstavlja učinkovitu dodatnu mjeru.

Scenariji u kojima se ne bi mogle utvrditi *učinkovite* mjere

87. Mjere opisane u nastavku u određenim scenarijima ne bi bile učinkovite u osiguravanju u načelu istovjetne razine zaštite za podatke koji se prenose u treću zemlju. Stoga se ne bi mogle okvalificirati kao dodatne mjere.

6. slučaj uporabe: prijenos pružateljima usluga u oblaku ili drugim izvršiteljima obrade koji zahtijevaju pristup nešifriranim podacima

88. Izvoznik podataka upotrebljava usluge pružatelja usluga u oblaku ili drugog izvršitelja za obradu osobnih podataka u trećoj zemlji u skladu s njegovim uputama.

Ako vrijedi sljedeće:

1. voditelj obrade prenosi podatke pružatelju usluga u oblaku ili drugom izvršitelju obrade,
2. pružatelj usluga u oblaku ili drugi izvršitelj obrade treba pristup nešifriranim podacima kako bi izvršio dodijeljeni zadatak, i
3. ovlasti dane javnim tijelima u zemlji primateljici za pristup prenesenim podacima nadilazi ono što je nužno i razmjerno u demokratskom društvu,⁷¹

⁷¹ Vidjeti članke 47. i 52. Povelje Europske unije o temeljnim pravima, članak 23. stavak 1. Opće uredbe i Preporuke Europskog odbora za zaštitu podataka o Europskim ključnim jamstvima za mjere nadzora.

Europski odbor za zaštitu podataka, s obzirom na trenutačna najmodernija dostignuća, ne može predvidjeti učinkovitu tehničku mjeru kojom bi se spriječila povreda prava ispitanika zbog takvog pristupa. Europski odbor za zaštitu podataka ne isključuje mogućnost da daljnja tehnološka dostignuća ponude mjere kojima se ostvaruju namjeravane poslovne svrhe bez potrebe za pristupom nešifriranim podacima.

89. U navedenim scenarijima u kojima su nešifrirani osobni podatci tehnički nužni kako bi izvršitelj obrade pružio svoje usluge, čak i zajednička primjena šifriranja podataka za slanje i šifriranja podataka u mirovanju ne predstavlja dodatnu mjeru kojom bi se osigurala u načelu istovjetna razina zaštite ako uvoznik podataka posjeduje kriptografske ključeve.

7. slučaj uporabe: pristup podacima na daljinu u poslovne svrhe

90. Izvoznik podataka osobne podatke stavlja na raspolaganje subjektima u trećoj zemlji kako bi se upotrebljavali u zajedničke poslovne svrhe. Uobičajena konstelacija subjekata sastoji se od voditelja obrade ili izvršitelja obrade s poslovnim nastanom na državnom području države članice koji prenosi osobne podatke voditelju obrade ili izvršitelju obrade u trećoj zemlji koji je dio iste grupacije poduzeća, ili skupina poduzeća koja se bavi zajedničkom gospodarskom aktivnošću. Uvoznik podataka možete, na primjer, upotrijebiti podatke koje primi kako bi pružio kadrovske usluge izvozniku podataka za što su mu potrebni podatci o osoblju, ili kako bi komunicirao s korisnicima izvoznika podataka koji žive u Europskoj uniji putem telefona ili elektroničke pošte.

Ako vrijedi sljedeće:

1. izvoznik podataka prenosi osobne podatke uvozniku podataka u trećoj zemlji tako što podatke čini dostupnima u informacijskom sustavu koji zajednički upotrebljavaju, na način kojim se uvozniku omogućuje izravan pristup podacima po njegovom izboru, ili tako što izravno prenosi podatke, pojedinačno ili skupno, uporabom komunikacijske usluge,
2. uvoznik upotrebljava nešifrirane podatke u vlastite svrhe,
3. ovlasti dane javnim tijelima u zemlji primateljici za pristup prenesenim podacima nadilazi ono što je nužno i razmjerno u demokratskom društvu,

Europski odbor za zaštitu podataka ne može predvidjeti učinkovitu tehničku mjeru kojom bi se spriječila povreda prava ispitanika zbog takvog pristupa.

91. U navedenim scenarijima u kojima su nešifrirani osobni podatci tehnički nužni kako bi izvršitelj obrade pružio svoje usluge, čak i zajednička primjena šifriranja podataka za slanje i šifriranja podataka u mirovanju ne predstavlja dodatnu mjeru kojom bi se osigurala u načelu istovjetna razina zaštite ako uvoznik podataka posjeduje kriptografske ključeve.

Dodatne ugovorne mjere

92. Te će se mjere općenito sastojati od jednostranih, dvostranih ili višestranih⁷² ugovornih obveza.⁷³ Ako se upotrebljava alat za prijenos iz članka 46. Opće uredbe, u većini će slučajeva već sadržavati određen broj (uglavnom ugovornih) obveza izvoznika podataka i uvoznika podataka koje služe kao zaštitne mjere za osobne podatke.⁷⁴
93. U nekim situacijama te mjere mogu nadopuniti i ojačati zaštitne mjere koje pružaju alat za prijenos i mjerodavni propisi treće zemlje kada, uzimajući u obzir okolnosti prijenosa, one ne ispunjavaju sve uvjete koji su potrebni kako bi se osigurala razina zaštite koja je u načelu istovjetna razini zajamčenoj unutar EU-a. S obzirom na narav ugovornih mjera koje općenito ne mogu obvezivati tijela vlasti te treće zemlje ako ta tijela nisu ugovorna strana⁷⁵, te se mjere trebaju kombinirati s drugim tehničkim i organizacijskim mjerama kako bi se osigurala potrebna razina zaštite podataka. Odabir i provedba jedne ili više ovih mjera neće nužno i sustavno osigurati da vaš prijenos zadovoljava standard u načelu istovjetne zaštite propisan pravom Unije.
94. Ovisno o tome koje su ugovorne mjere već sadržane u alatu za prijenos iz članka 46. Opće uredbe koji se upotrebljava, dodatne ugovorne mjere mogu pridonijeti tome da izvoznici podataka koji se nalaze u EGP-u postanu svjesni novih promjena koje utječu na zaštitu podataka prenesenih u treće zemlje.
95. Kao što je već rečeno, ugovorne mjere neće moći spriječiti primjenu propisa treće zemlje koji ne zadovoljavaju standarde Europskih ključnih jamstava Europskog odbora za zaštitu podataka u onim slučajevima u kojima propisi obvezuju uvoznike da postupe po nalogima za otkrivanje podataka koje prime od javnim tijela.⁷⁶
96. Neki primjeri tih mogućih ugovornih mjera navedeni su u nastavku i razvrstani prema njihovoj naravi:

Predviđanje ugovorne obveze uporabe određenih tehničkih mjera

97. ***Ovisno o posebnim okolnostima prijenosa, ugovorom će se možda morati predvidjeti uspostavljanje posebnih tehničkih mjera da bi se prijenos mogao odviti (vidjeti tehničke mjere predložene ranije u ovom dokumentu).***
98. ***Uvjeti za učinkovitost:***
- Ova bi klauzula mogla biti učinkovita u situacijama u kojima je izvoznik utvrdio potrebu za primjenom tehničkih mjera. Zatim bi se to trebalo navesti u pravnom obliku kako bi se osiguralo da se uvoznik također obveže uspostaviti nužne tehničke mjere, ako je to potrebno.

⁷² Npr., u obvezujućim korporativnim pravilima koja bi u svakom slučaju trebala uređivati neke od mjera navedenih u nastavku.

⁷³ Bit će privatne naravi i neće se smatrati međunarodnim sporazumima na temelju međunarodnog javnog prava. U skladu s time, obično neće obvezivati javna tijela treće zemlje jer nisu ugovorne strane u ugovoru sklopljenom s privatnim tijelima u trećim zemljama, kao što je Sud naglasio u svojoj presudi C-311/18 (Schrems II), stavak 125.

⁷⁴ Vidjeti presudu C-311/18 (Schrems II), stavak 137. u kojoj je Sud stoga priznao da standardna ugovorna klauzula sadrži „učinkovite mehanizme koji u praksi omogućuju osiguranje razine zaštite koja se zahtijeva pravom Unije i obustavu ili zabranu prijenosa osobnih podataka temeljenih na takvim klauzulama u slučaju povrede tih klauzula ili nemogućnosti njihova poštovanja.”, vidjeti također stavak 148.).

⁷⁵ C-311/18 (Schrems II), stavak 125.

⁷⁶ Presuda SEU-a C-311/18 (Schrems II), stavak 132.

Obveze transparentnosti:

99. ***Izvoznik može dodati priloge ugovoru s informacijama koje bi pružio uvoznik, koliko god mu je to moguće, o pristupu podacima od strane javnih tijela, uključujući u obavještajnom polju pod uvjetom da je zakonodavstvo u skladu s Europskim ključnim jamstvima Europskog odbora za zaštitu podataka, u zemlji odredišta. To izvozniku podataka može pomoći da ispuní obvezu dokumentiranja svoje procjene razine zaštite u trećoj zemlji.***
100. Od uvoznika bi se na primjer moglo tražiti sljedeće:
- (1) da nabroji zakone i propise u zemlji odredišta koji su primjenjivi na uvoznika ili njegove (pod)izvršitelje obrade, a koji bi javnim tijelima omogućili pristup osobnim podacima koji podliježu prijenosu, posebno u obavještajnom polju, polju kaznenog progona i polju administrativnog i regulatornog nadzora primjenjivog na prenesene podatke;
 - (2) u izostanku zakona kojima se uređuje pristup javnih tijela podacima, da navede informacije i statistike na temelju svojeg iskustva ili izvješća iz različitih izvora (npr. partneri, slobodno dostupni izvori, nacionalna sudska praksa i odluke tijela za nadzor) o pristupu javnih tijela osobnim podacima u situacijama sličnima situaciji predmetnog prijenosa podataka (odnosno u određenom regulatornom području, s obzirom na vrstu subjekta kakav je uvoznik podataka; ...);
 - (3) da navede koje se mjere provode da bi se spriječio pristup prenesenim podacima (ako takve postoje);
 - (4) da pruži dovoljno detaljne informacije o svim zahtjevima za pristup osobnim podacima od strane javnih tijela koje je uvoznik primio tijekom određenom razdoblja,⁷⁷ posebno u područjima navedenima u točki (1) i to informacije o zahtjevima koje je primio, podacima za koje je zatražen pristup, o tijelu koje je zatražilo pristup i o pravnoj osnovi za otkrivanje podataka te o mjeru u kojoj je izvoznik otkrio zatražene podatke;⁷⁸
 - (5) da navede je li i u kojoj mjeri uvozniku zakonski zabranjeno pružiti informacije navedene u točkama (1) – (5).
101. Te bi se informacije mogle pružiti u obliku strukturiranog upitnika koji bi uvoznik podataka ispunio i potpisao i kombinirati s ugovornom obvezom uvoznika da u određenom razdoblju navede sve moguće izmjene tih informacija, kao što je trenutačna praksa za postupke dubinske analize.
102. ***Uvjeti za učinkovitost:***
- Uvoznik mora moći pružiti te vrste informacije izvozniku najbolje što zna i nakon što je uložio maksimalan trud da te informacije pribavi.⁷⁹
 - Ova obveza nametnuta izvozniku sredstvo je kojim se osigurava da izvoznik postane i ostane svjestan rizika koji proizlaze iz prijenosa podataka u treću zemlju. To će izvozniku omogućiti da odustane od sklapanja ugovora, ili ako se informacije promijene nakon sklapanja ugovora, da ispuní svoju obvezu obustave prijenosa i/ili raskida ugovora ako pravo treće zemlje, zaštitne mjere sadržane u upotrijebljenom alatu za prijenos iz članka 46. Opće uredbe i sve dodatne

⁷⁷ Duljina razdoblja trebala bi ovisiti o riziku za prava i slobode ispitanika čiji podatci podliježu prijenosu u pitanju, npr. zadnja godina prije sklapanja instrumenta za izvoz podataka s izvoznikom podataka.

⁷⁸ Ispunjavanje ove obveze samo po sebi ne znači da se pružila odgovarajuća razina zaštite. Istovremeno svako neprimjereno otkrivanje podataka koje se zaista dogodilo stvara potrebu za primjenom dodatnih mjera.

⁷⁹ Vidi stavak 32.5. ovog dokumenta.

zaštitne mjere koje je možda usvojio više ne mogu osigurati razinu zaštite koja je u načelu istovjetna razini zaštite u EU-u. Međutim, ta obaveza ne može opravdati otkrivanje osobnih podataka od strane uvoznika ni stvoriti očekivanje da neće biti daljnjih zahtjeva za pristup.

103. ***Izvoznik također može dodati klauzule kojima uvoznik potvrđuje da (1) nije namjerno stvorio stražnje ulaze ili slične programe koji bi se mogli upotrijebiti za pristup sustavu i/ili osobnim podacima, (2) nije namjerno stvorio ili izmijenio svoje poslovne procese na način koji olakšava pristup osobnim podacima ili sustavima i (3) nacionalno pravo ili vladine politike od uvoznika ne zahtijevaju da stvori ili održava stražnje ulaze ili da olakša pristup osobnim podacima ili sustavima ili da posjeduje ili tijelima vlasti preda ključ za šifriranje.***⁸⁰

104. ***Uvjeti za učinkovitost:***

- Ako postoje propisi ili vladine politike koji uvoznika sprječavaju u otkrivanju tih informacije, to može dovesti do toga da je ova klauzula nevaljana. Uvoznik stoga neće moći sklopiti ugovor ili će trebati obavijestiti izvoznika da nije u mogućnosti dalje ispunjavati svoje ugovorne obveze.⁸¹
- Ugovor mora sadržavati novčane kazne i/ili mogućnost da izvoznik raskine ugovor u kratkom roku u onim slučajevima u kojima uvoznik ne otkrije postojanje stražnjih ulaza ili sličnih programa ili u kojima je izmijenio poslovne procese ili bilo kakve zahtjeve kako bi primijenio stražnje ulaze ili slične programe ili ako ne obavijesti izvoznika čim sazna za postojanje stražnjih ulaza ili sličnih programa.

105. ***Izvoznik bi mogao ojačati svoje ovlasti da provodi revizije⁸² ili inspekcije opreme za obradu podataka uvoznika, na lokaciji i na daljinu, kako bi provjerio jesu li podatci otkriveni javnim tijelima i pod kojim uvjetima (pristup ne nadilazi ono što je nužno i razmjerno u demokratskom društvu), npr. određivanjem kratkog roka najave i mehanizama kojima se osigurava brza intervencija inspekcijskih tijela i jačanjem autonomije izvoznika da odabere inspekcijska tijela.***

106. ***Uvjeti za učinkovitost:***

- Opseg revizije treba zakonski i tehnički obuhvatiti svu obradu od strane izvršitelja ili podizvršitelja obrade uvoznika u odnosu na osobne podatke prenesene u treću zemlju kako bi revizija bila potpuno učinkovita.
- Evidencije pristupa i drugi slični tragovi trebaju biti zaštićeni od neovlaštenih izmjena kako bi revizori mogli pronaći dokaze o otkrivanju podataka. Evidencije pristupa i drugi slični tragovi trebaju također prikazivati razliku između pristupa zbog redovnih poslovnih aktivnosti i pristupa zbog naloga ili zahtjeva za pristup.

⁸⁰ Ova je klauzula važna kako bi se jamčila primjerena razina zaštite prenesenih osobnih podataka i obično bi trebala biti obvezna.

⁸¹ Vidi stavak 32.5. ovog dokumenta.

⁸² Vidjeti na primjer klauzulu 5. točku (f) standardnih ugovornih klauzula između voditelja obrade i izvršitelja obrade u Odluci 2010/87/EU, revizije se mogu predvidjeti u sklopu kodeksa ponašanja ili putem certifikacije.

107. ***Ako su pravo i praksa treće zemlje uvoznika u početku uspješno procijenjene i ako se utvrdilo da pružaju u načelu istovjetnu razinu zaštite kao u EU-u za podatke koje prenosi izvoznik, izvoznik i dalje može ojačati obvezu uvoznika podataka da izvoznika podataka odmah obavijesti ako nije u mogućnosti ispuniti ugovorne obveze i stoga ni propisani standard „u načelu istovjetne razine zaštite podataka“.***^{83.}
108. Ta nemogućnost ispunjavanja obveza može biti rezultata izmjena u zakonodavstvu ili praksi treće zemlje.⁸⁴ Klauzule bi mogle uspostaviti određene i stroge rokove i postupke za brzu obustavu prijenosa podataka i/ili raskid ugovora, te vraćanja ili brisanje primljenih podataka od strane uvoznika. Praćenje primljenih zahtjeva, njihovog opsega i učinkovitosti mjera usvojenih kako bi ih se suzbilo izvozniku bi trebalo dati dovoljno naznaka treba li ispuniti svoju obvezu obustave ili prekida prijenosa i/ili raskida ugovora.
109. ***Uvjeti za učinkovitost:***
- Izvoznika podataka treba obavijestiti prije nego što se odobri pristup podacima. U suprotnom, do trenutka u kojem izvoznik primi obavijest već može doći do povrede prava pojedinaca ako se zahtjev temelji na zakonima te treće zemlje koji nadilaze ono što razina zaštite podataka iz prava Unije dopušta. Obavijest može i dalje poslužiti kako bi se spriječile buduće povrede prava i kako bi izvoznik mogao ispuniti svoju obvezu obustave prijenosa osobnih podataka u treću zemlju i/ili raskida ugovora.
 - Uvoznik podataka mora nadzirati sve promjene propisa ili politika koje bi mogle dovesti do toga da nije u mogućnosti ispuniti svoje obveze i o svim takvim promjenama mora odmah obavijestiti izvoznika podataka, po mogućnosti prije nego što se one provedu kako bi izvoznik podataka mogao uzeti podatke od uvoznika.
 - Klauzule bi trebale predvidjeti brz mehanizam kojim izvoznik podataka ovlašćuje uvoznika podataka da brzo osigura ili vrati podatke izvozniku podataka, a ako to nije moguće, izbriše ili sigurno šifrira podatke bez da nužno čeka upute izvoznika, ako se zadovolji određeni prag koji će izvoznik podataka i uvoznik podataka dogovoriti. Uvoznik treba primijeniti taj mehanizam od početka prijenosa podataka i redovito ga testirati kako bi bio siguran da se mehanizam može primijeniti u kratkom roku.
 - Druge bi klauzule mogle omogućiti izvozniku da nadzire uvoznikovo ispunjavanje tih obveza putem revizija, inspekcija i drugih mjera provjere i da ih izvrši novčanim kaznama nametnutim uvozniku i/ili svojom ovlasti da obustavi prijenos i/ili odmah raskine ugovor.

⁸³ Klauzula 5. točka (a) i klauzula 5. točka (d) podtočka (i) Odluke 2010/87/EU o standardnim ugovornim klauzulama.

⁸⁴ Vidjeti C-311/18 (Schrems II), stavak 139. u kojem Sud navodi da „iako ta klauzula 5. u točkama (d) podtočki (i) omogućuje primatelju osobnih podataka da voditelja obrade s poslovnim nastanom u Uniji ne obavijesti o pravno obvezujućem zahtjevu tijela kaznenog progona za otkrivanje osobnih podataka ako postoji propis koji brani takvo primateljevo postupanje poput zabrane prema kaznenom pravu radi očuvanja povjerljivosti kaznene istrage, primatelj je ipak dužan, u skladu s klauzulom 5. točkom (a) priloga Odluci o standardnim ugovornim klauzulama, obavijestiti voditelja obrade o svojoj nemogućnosti da postupi u skladu sa standardnim klauzulama o zaštiti podataka.“

110. ***U mjeri u kojoj to dopušta nacionalno pravo u trećoj zemlji, ugovorom bi se mogle ojačati obveze transparentnosti uvoznika propisivanjem metode „Warrant Canary” kojom se uvoznik obvezuje redovito objavljivati (npr. najmanje svaka 24 sata) kriptografski potpisanu poruku kojom obavještava izvoznika da do određenog datuma i vremena nije primio nijedan nalog za otkrije osobne podatke ili nešto tome slično. Ako se ta obavijest ne ažurira, to će izvozniku ukazati na to da je uvoznik možda primio takav nalog.***

111. ***Uvjeti za učinkovitost:***

- Propisi treće zemlje moraju dopuštati uvozniku podataka da objavi ovaj oblik pasivne obavijesti izvozniku.
- Izvoznik podataka mora automatski nadzirati obavijesti o nepostojanju naloga.
- Uvoznik podataka mora osigurati da je njegov privatni ključ za potpisivanje takvih obavijesti o nepostojanju naloga sigurno pohranjen i da ga se propisima treće zemlje ne može prisiliti da objavi lažnu obavijest o nepostojanju naloga. U tu bi svrhu moglo biti korisno ako su za obavijest potrebni potpisi nekoliko osoba i/ili ako obavijest objavljuje osoba izvan nadležnosti treće zemlje.

Obveza poduzimanja određenih radnji

112. ***Uvoznik se može obvezati na preispitivanje, na temelju prava zemlje odredišta, zakonitosti bilo kojeg naloga za otkrivanje podataka, prije svega je li to u okviru ovlasti danih javnom tijelu koje podnosi nalog, i na osporavanje naloga ako nakon pažljivog razmatranja zaključi da za to postoje osnove na temelju prava države odredišta. Prilikom osporavanja naloga, uvoznik podataka trebao bi zatražiti privremenu mjeru obustave učinka naloga dok sud ne odluči o njegovoj osnovanosti. Uvoznik bi imao obvezu ne otkriti zatražene osobne podatke dok to ne bude obvezan učiniti na temelju mjerodavnih postupovnih pravila. Uvoznik podataka također bi se obvezao pružiti najmanju moguću dopuštenu količinu informacija kad odgovara na nalog, na temelju razumnog tumačenja naloga.***

113. ***Uvjeti za učinkovitost:***

- Pravni poredak treće zemlje mora pružati učinkovita pravna sredstva za osporavanje naloga za otkrivanje podataka.
- Ova će odredba uvijek nuditi vrlo ograničenu dodatnu zaštitu jer nalog za otkrivanje podataka može biti zakonit u pravnom poretku treće zemlje, no taj pravni poredak možda ne ispunjava standarde EU-a. Ova će ugovorna mjera nužno morati biti samo dopuna drugim dodatnim mjerama.
- Osporavanje naloga mora imati učinak odgode izvršenja na temelju prava treće zemlje. U suprotnom bi javna tijela i dalje imala pristup podacima pojedinaca i svaka daljnja radnja u korist pojedinca imala bi ograničen učinak toga da se pojedincu dopusti da potražuje naknadu štete za negativne posljedice koje proizađu iz otkrivanja podataka.
- Uvoznik će trebati moći dokumentirati i dokazati izvozniku koje je radnje proveo uz ulaganje maksimalnih napora kako bi ispunio ovu obvezu.

114. ***U istoj situaciji kao onoj opisanoj gore, uvoznik se može obvezati obavijestiti javno tijelo koje šalje nalog o nespojivosti naloga sa zaštitnim mjerama sadržanima u alatu za prijenos iz članka 46. Opće uredbe o zaštiti podataka⁸⁵ i sukobu obveza koji iz toga proizlazi za uvoznika. Uvoznik bi istovremeno i što je ranije moguće obavijestio izvoznika i/ili nadležno nadzorno tijelo iz EGP-a u mjeri u kojoj je to moguće u pravnom poretku treće zemlje.***

115. ***Uvjeti za učinkovitost:***

- Takve informacije o zaštiti zajamčenoj pravom Unije i sukobu obveza treba imati neki pravni učinak u pravnom poretku treće zemlje, poput sudskog ili upravnog preispitivanja naloga ili zahtjeva za pristup, uvjeta o postojanju sudskog naloga i/ili privremene obustave naloga kako bi se dodao neki oblik zaštite podataka.
- Pravni sustav zemlje ne smije sprječavati uvoznika u slanju obavijesti izvozniku ili barem nadležnom nadzornom tijelu iz EGP-a o nalogu ili zahtjevu koji je primio.
- Uvoznik će trebati moći dokumentirati i dokazati izvozniku koje je radnje proveo uz ulaganje maksimalnih napora kako bi ispunio ovu obvezu.

Oснаživanje ispitanika da ostvaruju svoja prava

116. ***Ugovorom se može predvidjeti da se osobnim podacima koji se prenose nešifrirani tijekom redovitog poslovanja (uključujući u slučajevima pružanja podrške) može pristupiti samo uz izričitu ili implicitnu privolu izvoznika i/ili ispitanika.***

117. ***Uvjeti za učinkovitost:***

- Ova bi klauzula mogla biti učinkovita u situacijama u kojima uvoznici prime zahtjeve od javnih tijela da surađuju na dobrovoljnoj osnovi, za razliku od, primjerice, pristupa podacima od strane javnih tijela koji se odvije bez znanja uvoznika podataka ili protiv njegove volje.
- U nekim situacijama ispitanik možda neće biti u mogućnosti usprotiviti se pristupu ili dati privolu koja ispunjava sve uvjete propisane na temelju prava Unije (dobrovoljan, poseban, informiran i nedvosmislen pristanak) (npr. u slučaju zaposlenika)⁸⁶.
- Nacionalni propisi ili politike koji prisiljavaju uvoznika da ne otkriva nalog za pristup mogu dovesti do toga da je ova klauzula nevaljana, osim ako se ne može ojačati tehničkim metodama koje dovode do toga da je potrebna intervencija izvoznika ili ispitanika kako bi nešifrirani podatci bili dostupni. Takve tehničke mjere ograničavanja pristupa mogu se predvidjeti posebno kad se pristup daje samo u posebnim slučajevima davanja podrške ili usluga, ali se sami podatci pohranjuju u EGP-u.

⁸⁵ Na primjer, standardne ugovorne klauzule predviđaju da se obrada podataka, uključujući prijenos podataka, provodi i da će se nastaviti provoditi u skladu s „pravom koje se primjenjuje na zaštitu podataka”. To se pravo definira kao „zakonodavstvo, koje štiti temeljna prava i slobode pojedinaca i posebno njihovo pravo na privatnost u pogledu obrade osobnih podataka, koje primjenjuje nadzornik podataka u državi članici u kojoj izvoznik podataka ima poslovni nastan”. SEU potvrđuje da su odredbe Opće uredbe o zaštiti podataka, tumačene u vezi s Poveljom Europske unije o temeljnim pravima, dio tog zakonodavstva, vidjeti SEU C-311/18 (Schrems II), stavak 138.

⁸⁶ Članak 4. stavak 11. Opće uredbe.

118. ***Ugovorom bi se moglo obvezati uvoznika i/ili izvoznika da odmah obavijesti ispitanika o zahtjevu ili nalogu primljenom od javnih tijela treće zemlje, ili o nemogućnosti uvoznika da ispuní ugovorne obveze, kako bi se ispitaniku omogućilo da traži informacije i učinkovitu pravnu zaštitu (npr. podnošenjem zahtjeva svojem nadležnom nadzornom tijelu i/ili pravosudnom tijelu i dokazivanjem procesne legitimacije pred sudovima treće zemlje).***

119. ***Uvjeti za učinkovitost:***

- Tom bi se obavijesti moglo upozoriti ispitanika o potencijalnim pristupima javnih tijela trećih zemalja njegovim podacima. To bi stoga ispitaniku omogućilo da traži dodatne informacije od izvoznika i da podnese zahtjev svojem nadležnom nadzornom tijelu. Ovom bi se klauzulom mogle riješiti neke od poteškoća s kojima se pojedinac može susresti prilikom dokazivanja svoje procesne legitimacije (*locus standi*) pred sudovima treće zemlje kako bi osporio pristup javnih tijela njegovim podacima.

- Nacionalni propisi i politike mogu spriječiti slanje ove obavijesti ispitaniku. Izvoznik i uvoznik mogu se svejedno obvezati obavijestiti ispitanika čim se ukinu ograničenja u odnosu na otkrivanje podataka i uložiti maksimalne napore kako bi pribavili oslobođenje od zabrane otkrivanja. Izvoznik ili nadležno nadzorno tijelo mogu barem obavijestiti ispitanika o obustavi ili prekidu prijenosa njegovih osobnih podataka zbog nemogućnosti uvoznika da ispuní svoje ugovorne obveze jer je primio zahtjev za pristup.

120. ***Ugovorom bi se moglo obvezati izvoznika i uvoznika da ispitaniku pomognu u ostvarivanje njegovih prava u jurisdikciji treće zemlje mehanizmima ad hoc pravne zaštite i pravnim savjetovanjem.***

121. ***Uvjeti za učinkovitost:***

- Nacionalnim propisima i politikama mogu se nametnuti uvjeti koji mogu umanjiti učinkovitost predviđenih mehanizama *ad hoc* pravne zaštite.

- Pravno savjetovanje može biti korisno za ispitanika, osobito kad se uzme u obzir koliko bi razumijevanje pravosudnog sustava treće zemlje i pokretanje pravnog postupka iz inozemstva, moguće na stranom jeziku, moglo biti složeno i skupo za ispitanika. Međutim, ovom će se klauzulom uvijek dati samo ograničena dodatna zaštita jer pružanje pomoći i pravnog savjetovanja ispitanicima ne može samo po sebi ispraviti propust pravnog poretka treće zemlje da osigura razinu zaštite koja je u načelu istovjetna razini zajamčenoj unutar EU-a. Ova će ugovorna mjera nužno morati biti samo dopuna drugim dodatnim mjerama.

Dodatna mjera bila bi učinkovita samo kad bi pravo treće zemlje predviđalo pravnu zaštitu pred svojim nacionalnim sudovima ili kad bi postojao mehanizam *ad hoc* pravne zaštite. To u svakom slučaju ne bi bila učinkovita dodatna mjera protiv mjera nadzora ako ne postoji mehanizam pravne zaštite.

Organizacijske mjere

122. Dodatne organizacijske mjere mogu se sastojati od internih politika, organizacijskih metoda i standarda koje voditelji obrade i izvršitelji obrade mogu primijeniti na sebe i nametnuti uvoznicima podataka u trećim zemljama. One mogu pridonijeti osiguravanju dosljednosti zaštite osobnih podataka tijekom cijelog ciklusa obrade. Organizacijske mjere također mogu povećati svijest izvoznika o opasnostima i pokušajima ostvarivanja pristupa podacima u trećim zemljama i sposobnost izvoznika da reagiraju na

njih. Odabir i provedba jedne ili više ovih mjera neće nužno i sustavno osigurati da vaš prijenos zadovoljava standard u načelu istovjetne zaštite propisan pravom Unije. Ovisno o konkretnim okolnostima prijenosa i procjeni zakonodavstva treće zemlje, organizacijske mjere potrebne su kako bi se njima dopunile ugovorne i/ili tehničke mjere da bi se osigurala razina zaštite osobnih podataka koja je u načelu istovjetna razini zajamčenoj u EU-u.

123. Procjena najprimjerenijih mjera mora se provesti za svaki pojedinačni slučaj imajući na umu potrebu voditelja obrade i izvršitelja obrade da poštuju načelo odgovornosti. U nastavku Europski odbor za zaštitu podataka navodi neke primjere organizacijskih mjera koje izvoznici mogu primijeniti, no popis nije iscrpan te i druge mjere također mogu biti primjerene:

Unutarnje politike upravljanja prijenosima, posebno sa skupinama poduzeća

124. ***Usvajanje odgovarajućih unutarnjih politika s jasnom raspodjelom odgovornosti za prijenose podataka, kanalima prijavljivanja i standardnim operativnim postupcima za slučajeve tajnih ili službenih zahtjeva za pristup podacima od strane javnih tijela. Posebno u slučaju prijenosa među skupinama poduzeća, te politike mogu među ostalim uključivati imenovanje posebnog tima koji bi se trebao nalaziti unutar EGP-a i sastojati se od stručnjaka u području informacijskih tehnologije, zakona o zaštiti podataka i privatnosti, koji bi se bavili zahtjevima koji uključuju osobne podatke prenesene iz EU-a; obavješćavanje višeg pravnog i korporacijskog rukovodstva i izvoznika podataka po primitku takvih zahtjeva; postupovne korake za osporavanje nesrazmjernih ili nezakonitih zahtjeva i pružanje transparentnih informacija ispitanicima.***
125. Razvijanje posebnih postupaka osposobljavanja za osoblje odgovorno za upravljanje zahtjevima za pristup osobnim podacima od strane javnih tijela, koji se postupci trebaju s vremena na vrijeme ažurirati kako bi odražavali nove promjene u zakonima i sudskoj praksi u trećoj zemlji i u EGP-u. Postupci osposobljavanja trebali bi sadržavati zahtjeve iz prava Unije u pogledu pristupa javnih tijela osobnim podacima, posebno kao što proizlazi iz članka 52. stavka 1. Povelje o temeljnim pravima. Potrebno je podići svijest osoblja, posebno procjenom praktičnih primjera zahtjeva javnih tijela za pristup i primjenom standarda koji proizlazi iz članka 52. stavka 1. Povelje o temeljnim pravima na te praktične primjere. Takvo osposobljavanje treba uzeti u obzir posebnu situaciju uvoznika podataka, npr. zakonodavstvo i propise treće zemlje kojima uvoznik podataka podliježe, i treba ga razviti u suradnji s izvoznikom podataka kad je to moguće.
126. ***Uvjeti za učinkovitost:***
- Te se politike mogu predvidjeti samo za one slučajeve u kojima je zahtjev javnih tijela u trećoj zemlji u skladu s pravom Unije.⁸⁷ Kad zahtjev nije u skladu s pravom Unije, te politike nisu dovoljne da bi se osigurala istovjetna razina zaštite osobnih podataka i, kao što je ranije navedeno, prijenosi se moraju zaustaviti ili se moraju uspostaviti odgovarajuće dodatne mjere kako bi se izbjegao pristup podacima.

⁸⁷ Vidjeti predmet C-362/14 (Schrems I), stavak 94.; C-311/18 (Schrems II), stavci 168., 174., 175. i 176.

Mjere transparentnosti i odgovornosti

127. ***Dokumentirajte i evidentirajte zahtjeve za pristup koje primite od javnih tijela i odgovore na te zahtjeve zajedno s pravnim obrazloženjem i uključenim dionicima (npr. je li izvoznik obaviješten i koji je bio njegov odgovor, procjena tima odgovornog za rješavanje takvih zahtjeva itd.). Tu evidenciju trebate staviti na raspolaganje izvozniku podataka koji bi ju trebao, kad je to potrebno, prenijeti ispitanicima u pitanju.***

128. ***Uvjeti za učinkovitost:***

- Nacionalno zakonodavstvo u trećoj zemlji može priječiti otkrivanje zahtjeva ili bitnih informacija o njemu čime ova praksa postaje neučinkovita. Uvoznik podataka trebao bi obavijestiti izvoznika da nije u mogućnosti dostaviti takve dokumente i evidenciju i time izvozniku ponuditi mogućnost da obustavi prijenose ako bi ta nemogućnost izvoznika da dostavi evidenciju uzrokovala smanjenje razine zaštite.

129. ***Redovito objavljivanje izvješća ili sažetaka o transparentnosti u vezi sa zahtjevima javnih tijela za pristup podacima i o vrsti odgovora na zahtjeve, u mjeru kojoj je objavljivanje takvih dokumenata dopušteno lokalnim pravom.***

130. ***Uvjeti za učinkovitost:***

- Pružene informacije trebaju biti relevantne, jasne i što detaljnije. Nacionalno zakonodavstvo u trećoj zemlji može priječiti otkrivanje detaljnih informacija. U tim slučajevima izvoznik podataka treba uložiti maksimalan napor u objavljivanje statističkih podataka ili sličnih vrsta agregiranih podataka.

Organizacijske metode i mjere smanjenja količine podataka

131. ***U kontekstu prijenosa podataka korisnim se mjerama mogu pokazati i već postojeći organizacijski zahtjevi na temelju načela odgovornosti, poput usvajanja politika strogog i djelomičnog pristupa podacima i politika i najboljih praksi u području čuvanja povjerljivosti, na temelju stroge primjene načela otkrivanja samo nužnih informacija, uz nadzor redovnim revizijama i osiguravanje poštovanja politika primjenom disciplinskih mjera. U tom se pogledu treba razmotriti i smanjenje količine podataka kako bi se ograničila izloženost osobnih podataka riziku od neovlaštenog pristupa. Na primjer, u nekim slučajevima možda nije potrebno prenositi određene podatke (npr. u slučaju pristupa podacima u EGP-u na daljinu, kao u slučajevima pružanja podrške kad se odobrava ograničen pristup umjesto potpunog pristupa podacima; ili kad je za pružanje usluge potreban prijenos samo ograničenog skupa podataka, a ne cijele baze podataka).***

132. ***Uvjeti za učinkovitost:***

- Potrebno je uspostaviti redovite revizije i stroge disciplinske mjere kako bi se nadziralo i osiguralo poštovanje mjera smanjenja količine podataka i u kontekstu prijenosa podataka.
- Izvoznik podataka provodi procjenu osobnih podataka koje posjeduje prije prijenosa kako bi utvrdio koji skupovi podataka nisu potrebni za svrhe radi kojih se vrši prijenos i koje stoga neće podijeliti s uvoznikom podataka.

- Mjere smanjenja količine podataka potrebno je dopuniti tehničkim mjerama kako bi se osiguralo da podatci nisu izloženi riziku od neovlaštenog pristupa. Na primjer, primjena sigurnih mehanizama višekorisničkog računanja i raspodjela šifriranih skupova podataka među različitim subjektima od povjerenja može samo po sebi spriječiti situaciju u kojoj bi bilo koji jednostran pristup podacima uzrokovao otkrivanje podataka koji se mogu identificirati.

133. ***Razvoj najboljih praksi za primjereno i pravovremeno uključivanje službenika za zaštitu podataka, ako postoji, te pravnih službi i službi za unutarnju reviziju i davanje pristupa informacijama istima u stvarima povezanim s međunarodnim prijenosima osobnih podataka.***

134. ***Uvjeti za učinkovitost:***

- Službenik za zaštitu podataka, ako postoji, te pravna služba i služba za unutarnju reviziju dobivaju sve relevantne informacije prije prijenosa i provodi se savjetovanje s njima o nužnosti prijenosa i dodatnim zaštitnim mjerama, ako postoje.
- Relevantne informacije trebaju uključivati, na primjer, procjenu nužnosti prijenosa određenih osobnih podataka, pregled primjenjivih zakona treće zemlje i zaštitne mjere koje se uvoznik obvezao provesti.

Usvajanja standarda i najboljih praksi

135. ***Usvajanje strogih politika o sigurnosti i privatnosti podataka, na temelju certifikata i kodeksa ponašanja iz EU-a ili na temelju međunarodnih normi (npr. norme ISO) i najboljih praksi (npr. prakse ENISA-e) uzimajući u obzir najmodernija dostignuća, u skladu s rizicima svojstvenima za kategorije podataka koji se obrađuju i u skladu s time koliko je vjerojatno da će javna tijela pokušati pristupiti podacima.***

Ostalo

136. ***Usvajanje i redovito preispitivanje unutarnjih politika kako bi se ocijenila primjerenost provedenih dopunskih mjera i utvrdila i provela dodatna ili alternativna rješenja kad je to potrebno da bi se održala razina zaštite prenesenih podataka koja je istovjetna razini zaštite zajamčenoj u EU-u.***

137. ***Obvezivanje uvoznika podataka da neće provoditi daljnje prijenose osobnih podataka u istoj ili nekoj drugoj trećoj zemlji, ili da će obustaviti postojeće prijenose, kad se u trećoj zemlji ne može zajamčiti razina zaštite osobnih podataka istovjetna razini zaštite u EU-u.⁸⁸***

⁸⁸ C-311/18 (Schrems II), stavci 135. i 137.

PRILOG 3.: MOGUĆI IZVORI INFORMACIJA ZA PROCJENU TREĆE ZEMLJE

138. Uvoznik podataka trebao bi biti u poziciji staviti vam na raspolaganje relevantne izvore i informacije u vezi s trećom zemljom u kojoj ima poslovni nastan i navesti zakone koji se na njega primjenjuju. Možete provjeriti i više različitih izvora informacija poput onih oglednih navedenih u nastavku:

- sudska praksa Suda Europske unije (SEU) i Europskog suda za ljudska prava (ESLJP)⁸⁹ na koju je upućeno u preporukama o Europskim ključnim jamstvima;⁹⁰
- odluke o primjerenosti u zemlji odredišta ako se prijenos oslanja na drugačiju pravnu osnovu;⁹¹
- rezolucije i izvješća međuvladinih organizacija poput Vijeća Europe,⁹² drugih regionalnih tijela⁹³ i tijela i agencija UN-a (npr. Vijeće Ujedinjenih naroda za ljudska prava,⁹⁴ Odbor za ljudska prava⁹⁵);
- nacionalna sudska praksa ili odluke neovisnih pravosudnih ili administrativnih tijela vlasti nadležnih u području privatnosti i zaštite podataka u trećim zemljama;
- izvješća akademskih institucija i organizacija civilnog društva (npr. nevladine organizacije i trgovinska udruženja).

⁸⁹ Vidjeti informativni članak o sudskoj praksi ESLJP-a o masovnom nadzoru: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

⁹⁰ <https://www.coe.int/en/web/data-protection/reports-studies-and-opinions>

⁹¹ C-311/18 (Schrems II), stavak 141.; vidjeti odluke o primjerenosti u https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

⁹² <https://www.coe.int/en/web/data-protection/reports-studies-and-opinions>

⁹³ Vidjeti, na primjer, izvješća o zemljama Međuameričke komisije za ljudska prava (IACHR), <https://www.oas.org/en/iachr/reports/country.asp>.

⁹⁴ Vidjeti <https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx>

⁹⁵ Vidjeti:

https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5