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

Verzija 2.0

Doneseno 18. lipnja 2021.

Povijest inačica

Verzija 2.0	18. lipnja 2021.	Donošenje preporuka nakon javnog savjetovanja
Inačica 1.0	10. studenog 2020.	Donošenje preporuka za javno savjetovanje

Sažetak

Opća uredba o zaštiti podataka EU-a (OUZP) 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 (Sud EU-a) podsjetio je da se zaštita koja se dodjeljuje osobnim podatcima u Europskom gospodarskom prostoru (EGP) mora primjenjivati na podatke neovisno o tome kamo 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. OUZP-a 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. OUZP-a. U tim slučajevima Sud i dalje ostavlja mogućnost izvoznicima da provedu dodatne mjere kojima se nadoknađuju nedostatci 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. OUZP-a kojim se propisuje da su voditelji obrade podataka odgovorni za usklađenost s načelima iz OUZP-a koja se odnose na obradu osobnih podataka i da moraju biti u mogućnosti dokazati tu usklađenost.

Europski odbor za zaštitu podataka donio 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 OUZP-a) 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 obrađuju.

Drugi je korak **provjeriti alat za prijenos na koji se oslanjate**, među onima navedenima u poglavlju V. OUZP-a. 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. OUZP-a 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. OUZP-a. Samo ćete se u nekim slučajevima možda moći osloniti na jedno od odstupanja predviđenih u članku 49. OUZP-a ako za to ispunjavate uvjete. Odstupanja ne mogu postati „pravilo" u praksi, nego se moraju ograničiti na specifične situacije.

Treći korak jest **procijeniti** postoji li išta u pravu i/ili praksi koji su na snazi u trećoj zemlji što može dovesti u pitanje učinkovitost odgovarajućih zaštitnih mjera iz alata za prijenos na koje se oslanjate, u kontekstu konkretnog prijenosa. Vaša se procjena prije svega treba usredotočiti na zakonodavstvo treće zemlje koje je mjerodavno za vaš prijenos i za alat za prijenos iz članka 46. OUZP-a na koji se oslanjate. Proučavanje i prakse tijela javne vlasti treće zemlje omogućit će vam da provjerite mogu li

zaštitne mjere sadržane u alatu za prijenos u praksi osigurati učinkovitu zaštitu osobnih podataka koji se prenose. Proučavanje tih praksi bit će posebno važno za vašu procjenu:

(i.) ako se zakonodavstvo u trećoj zemlji koje formalno ispunjava standarde EU-a očito ne primjenjuje/poštuje u praksi

(ii.) ako postoje prakse koje nisu kompatibilne s obvezama alata za prijenos ako u trećoj zemlji nedostaje relevantno zakonodavstvo

(iii.) ako vaši preneseni podatci i/ili uvoznik potpadaju ili bi mogli potpadati u područje problematičnog zakonodavstva (tj. narušavanje ugovornog jamstva alata za prijenos suštinski jednakovrijedne razine zaštite i neispunjavanje standarda EU-a o temeljnim pravima, nužnosti i razmjernosti).

U prva dva slučaja morat ćete obustaviti prijenos ili provesti odgovarajuće dodatne mjere ako želite nastaviti s njim.

U trećoj situaciji, u svjetlu neizvjesnosti s potencijalnom primjenom problematičnog zakonodavstva na vaš prijenos, možete odlučiti: obustaviti prijenos; provesti dodatne mjere za nastavak prijenosa; ili alternativno, možete odlučiti nastaviti prijenos bez provedbe dodatnih mjera ako smatrate i u mogućnosti ste dokazati i dokumentirati da nemate razloga vjerovati da će se relevantno i problematično zakonodavstvo tumačiti i/ili u praksi primjenjivati na način da se primjenjuje na vaše prenesene podatke i uvoznika.

Za ocjenjivanje elemenata koje je potrebno uzeti u obzir prilikom procjene zakona treće zemlje koji se bave pristupom podatcima od strane javnih tijela za potrebe nadzora, pogledajte preporuke Europskog odbora za zaštitu podataka o europskim temeljnim jamstvima.

Tu procjenu dodatnih mjera trebate provesti s dužnom pažnjom i temeljito je dokumentirati. Vaša nadležna nadzorna i/ili pravosudna tijela mogu to zatražiti i smatrati vas odgovornim za svaku odluku koju donesete na toj osnovi.

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 i/ili prakse treće zemlje dovode u pitanje učinkovitost alata za prijenos iz članka 46. OUZP-a 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 i prakse treće zemlje i na alat za prijenos na koji se oslanjate jer ćete snositi odgovornost za sve odluke koje donesete na toj osnovi. 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. OUZP-a na koji se oslanjate. U ovim preporukama preciziraju se neke od tih 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 osobnih podataka koje prenosite u treće zemlje i da nadzirete jesu li se pojavile 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 nastavit će obnašati svoj mandat za praćenje primjene OUZP-a 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, na temelju provedene istrage ili pritužbe, utvrde da se ne može osigurati u načelu istovjetna razina zaštite.

Nadzorna tijela nastavit 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

Europski odbor za zaštitu podataka

uzimajući u obzir članak 70. stavak 1. točku (e) Uredbe (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 (u daljnjem tekstu: Opća uredba o zaštiti podataka),

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. Poslovnika,

budući da:

(1) Sud Europske unije (Sud EU-a) zaključio je 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) OUZP-a 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 OUZP-om, 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. OUZP-a predviđaju 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. OUZP-a, 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

[1] Upućivanja na „države članice" u ovom dokumentu trebaju se tumačiti kao upućivanja na „države članice EGP-a".
[2] Presuda Suda EU-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.

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 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. OUZP-a 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) OUZP i Sud ne definiraju ni preciziraju „dodatne zaštitne mjere" ili „dodatne mjere" uz zaštitne mjere alata za prijenos navedenih u članku 46. stavku 2. OUZP-a 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 dati 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 podatcima u trećoj zemlji pruži razina zaštite koja je u načelu istovjetna razini zaštite zajamčenoj unutar EGP-a. Ovim preporukama Europski odbor za zaštitu podataka nastoji potaknuti dosljednu primjenu OUZP-a i presude Suda, u skladu sa svojim mandatom,[7]

DONIO JE SLJEDEĆE PREPORUKE:

[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) OUZP-a.

1 ODGOVORNOST PRI PRIJENOSIMA PODATAKA

1. U primarnom pravu Unije pravo na zaštitu osobnih podataka smatra se temeljnim pravom.[8] U skladu s time, pravu 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 OUZP-om nije narušena ni tijekom ni nakon prijenosa.

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 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 OUZP primjenjuje se i na prijenose podataka u treće zemlje[13] 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 OUZP-om, 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 obavljala 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,

---

[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. OUZP-a.
[9] Članak 52. stavak 1. Povelje Europske unije o temeljnim pravima.
[10] Uvodna izjava 4. OUZP-a 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) OUZP-a.
[13] Članak 44. i uvodna izjava 101. OUZP-a, kao i članak 47. stavak 2. točka (d) OUZP-a.
[14] Presuda Suda EU-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.

primjerice, informirati o svim kretanjima koja utječu na razinu zaštite osobnih podataka koji se primaju u državi uvoznika.[17] Te odgovornosti predstavljaju primjenu načela odgovornosti iz OUZP-a 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[19] i koji obrađuje osobne podatke u okviru primjene OUZP-a – uključujući obradu od strane privatnih subjekata i javnih tijela prilikom prijenosa podataka privatnim tijelima.[20] 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.*[21]

7. Tu procjenu i dodatne mjere koje odaberete i provedete trebate dokumentirati i tu dokumentaciju staviti na raspolaganje nadležnom nadzornom tijelu na zahtjev.[22]

2.1 Prva faza: 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 podataka[23], 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) OUZP-a.
[19] Stoga se, na primjer, nećete smatrati izvoznikom podataka ako ste ispitanik koji svoje osobne podatke pruža putem mrežnog upitnika voditelju obrade s poslovnim nastanom u trećoj zemlji.
[20] Vidjeti Smjernice Europskog odbora za zaštitu podataka 3/2018 o teritorijalnom području primjene OUZP-a (članak 3.) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en
[21] 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
[22] Članak 5. stavak 2. i članak 24. stavak 1. OUZP-a.
[23] Imajte na umu da se pristup na daljinu podatcima 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. OUZP-a.[24] 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) OUZP-a vašim prijenosima njihovih osobnih podataka u treće zemlje.[25]

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 zemlji.[26]

11. U skladu s načelom „smanjenja količine podataka" iz OUZP-a,[27] morate provjeriti da su podatci koje prenosite primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se podatci 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 u oblaku koji se nalazi izvan EGP-a i koji nudi pružatelj usluga također smatraju prijenosom podataka.[28] 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 ima poslovni nastan u EGP-u i 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. OUZP-a.

---

[24] Vidjeti članak 30. OUZP-a, 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. OUZP-a). 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. OUZP-a o zaštiti podataka (odobrio Europski odbor za zaštitu podataka 25. svibnja 2018.).

[25] Na temelju pravila o transparentnosti iz OUZP-a, ispitanike morate obavijestiti o prijenosima osobnih podataka u treće zemlje (članak 13. stavak 1. točka (f) i članak 14. stavak 1. točka (f) OUZP-a). Konkretno, morate ih obavijestiti o postojanju ili nepostojanju odluke Komisije o primjerenosti, ili u slučaju prijenosa iz članaka 46. ili 47. OUZP-a, ili članka 49. stavka 1. drugog podstavka OUZP-a, 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.

[26] Kad je voditelj obrade dao prethodno posebno ili opće pisano odobrenje u skladu s člankom 28. stavkom 2. OUZP-a.

[27] Članak 5. stavak 1. točka (c) OUZP-a.

[28] 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.[29]

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. OUZP-a.

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).[30]

18. Europska komisija objavljuje popis odluka o primjerenosti na svojem mrežnom mjestu.[31]

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**.[32] Međutim, morate i dalje pratiti jesu li odluke o primjerenosti relevantne za vaše prijenose ukinute ili nevaljane.[33]

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 Sudu EU-a u svrhu ispitivanja te valjanosti.[34]

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

[29] Europska komisija ima ovlasti utvrditi, na temelju članka 45. OUZP-a, pruža li zemlja izvan EU-a primjerenu razinu zaštite podataka. Jednako tako Europska komisija ima ovlasti utvrditi da međunarodna organizacija pruža primjerenu razinu zaštite.

[30] Članak 45. stavak 1. OUZP-a.

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

[32] Pod uvjetom da se vi i uvoznik podataka proveli mjere u svrhu ispunjavanja drugih obveza iz OUZP-a; u suprotnom provedite te mjere.

[33] 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. OUZP-a). Osim toga, Sud EU-a može proglasiti odluke o primjerenosti nevaljanima (vidjeti presude Suda u predmetima C-362/14 (Schrems I) i C-311/18 (Schrems II)).

[34] 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. OUZP-a, 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 OUZP-u 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.

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 te je irski Visoki sud uputio zahtjev za prethodnu odluku o valjanosti Odluke 2000/520 Sudu Europske unije (Sudu EU-a). Sud EU-a naknadno je odlučio proglasiti Odluku 2000/520 Europske komisije o primjerenosti zaštite koju pružaju načela „sigurne luke" nevaljanom.[35]

[35] Predmet C-362/14 (Schrems I).

Alati za prijenos iz članka 46. OUZP-a

21. U članku 46. OUZP-a navodi se 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 su vrste alata za prijenos iz članka 46. OUZP-a:

- 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. OUZP-a odaberete, morate osigurati da će preneseni podatci u načelu u cjelini uživati istovjetnu razinu zaštite.

23. Alati za prijenos iz članka 46. OUZP-a 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.[36]

Odstupanja

24. Osim odluka o primjerenosti i alata za prijenos iz članka 46., OUZP 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. OUZP-a, podložno posebnim uvjetima.

25. Članak 49. OUZP-a posebne je naravi. Odstupanja koja sadrži moraju se tumačiti na način koji ne proturječi samoj prirodi odstupanja kao iznimke od pravila da se osobni podatci ne smiju prenositi u treću zemlju ako država ne osigura odgovarajuću razinu zaštite podataka ili, alternativno, ako se ne uspostave odgovarajuće mjere zaštite. Odstupanja ne mogu postati „pravilo" u praksi, nego se moraju ograničiti na specifične situacije. Europski odbor za zaštitu podataka objavio je svoje Smjernice 2/2018 o odstupanjima iz članka 49. prema Uredbi 2016/679. [37]

26. Prije nego što se pozovete na odstupanje iz članka 49. OUZP-a, morate provjeriti ispunjava li vaš prijenos stroge uvjete koje ova odredba predviđa za svaki od njih.

***

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

[36] C-311/18 (Schrems II), stavci 130. i 133. Vidjeti i pododjeljak 2.3. u nastavku.
[37] Za dodatne informacije vidjeti https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.

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. Odabrani alat za prijenos iz članka 46. OUZP-a mora biti učinkovit u osiguranju toga da razina zaštite zajamčena OUZP-om u praksi nije narušena prijenosom.[38]

29. Posebno, zaštita prenesenih osobnih podataka u trećoj zemlji mora biti u načelu istovjetna onoj koja je u EGP-u zajamčena OUZP-om, tumačenom u svjetlu Povelje o temeljnim pravima EU-a.[39] 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, uključujući i tijekom prijenosa podataka od izvoznika do zemlje uvoznika.[40]

30. Stoga prvo morate procijeniti, prema potrebi u suradnji s uvoznikom, postoji li išta u pravu i/ili praksi koji su na snazi[41] u trećoj zemlji što može dovesti u pitanje učinkovitost odgovarajućih zaštitnih mjera alata za prijenos iz članka 46. OUZP-a na koji se oslanjate, u kontekstu konkretnog prijenosa. To podrazumijeva utvrđivanje toga je li vaš prijenos obuhvaćen područjem primjene zakona i/ili praksi koji mogu dovesti u pitanje učinkovitost vašeg alata za prijenos iz članka 46. OUZP-a. Potrebna procjena treba se prije svega temeljiti na javno dostupnom zakonodavstvu.

31. Ova procjena mora sadržavati elemente koji se odnose na pristup podatcima tijela javne vlasti treće zemlje vašeg uvoznika kao što su:

    - elementi koji pokazuju hoće li tijela javne vlasti treće zemlje vašeg uvoznika nastojati pristupiti podatcima neovisno o tome je li uvoznik podataka s time upoznat, s obzirom na zakonodavstvo, praksu i prijavljene presedane;
    - elementi koji pokazuju hoće li tijela vlasti treće zemlje vašeg uvoznika moći pristupiti podatcima putem uvoznika podataka ili putem pružatelja telekomunikacijskih usluga ili komunikacijskih kanala, s obzirom na zakone, zakonske ovlasti i tehničke, financijske i ljudske resurse koji su im na raspolaganju i prijavljene presedane.

Utvrđivanje zakona i praksi relevantnih s obzirom na sve okolnosti prijenosa

32. Trebat ćete istražiti karakteristike svakog prijenosa i odrediti primjenjuju li se domaći pravni poredak i/ili prakse koji su na snazi u zemlji u koju se podatci prenose (ili dalje prenose) na te prijenose. Opseg vaše procjene stoga je ograničen na zakonodavstvo i prakse koji su relevantni za zaštitu specifičnih podataka koje prenosite, za razliku od općih i širokih sveobuhvatnih ocjena primjerenosti koje Europska komisija provodi u skladu s člankom 45. OUZP-a.

33. Mjerodavni pravni kontekst i/ili prakse ovisit će o okolnostima vašeg prijenosa, konkretno:

    - svrhama u koje se podatci prenose i obrađuju (npr. trgovanje, ljudski potencijali, pohrana, informatička podrška, klinička ispitivanja);

---

[38] Članak 44. OUZP-a i stavci 126., 137. i 148. presude C-311/18 (Schrems II).
[39] C-311/18 (Schrems II), stavak 105. i drugo utvrđenje.
[40] C-311/18 (Schrems II), stavak 183. u vezi sa stavkom 184.
[41] Vidjeti stavak 126. presude C-311/18 (Schrems II) u kojoj Sud izričito navodi „zakone i prakse koji su na snazi u predmetnoj trećoj zemlji" i zahtijeva „(...) da se osigura, u praksi, učinkovita zaštita osobnih podataka prenesenih u predmetnu treću zemlju." (isticanje naknadno dodano) i stavak 158.

- 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);[42]
- pohranjuju li se podatci u trećoj zemlji ili se radi o pristupu na daljinu podatcima pohranjenima u EU-u/EGP-u;
- formatu podataka koji će se prenijeti (tj. nešifrirani/pseudonimizirani ili šifrirani podatci[43]);
- mogućnosti da će se podatci dalje prenositi iz te treće zemlje u neku drugu treću zemlju.[44]

34. 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 predviđene daljnje prijenose.

35. 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 javnim tijelima daju ovlasti za pristup osobnim podatcima (primjerice, u svrhe kaznenog progona, regulatornog nadzora ili nacionalne sigurnosti). Ako se tim zahtjevima ili ovlastima ograničavaju temeljna prava ispitanika, a istovremeno poštuje njihova suština te su nužne i razmjerne mjere u demokratskom društvu za zaštitu važnih ciljeva koji su također priznati u pravu Unije ili država članica EU-a,[45] njima se ne mogu dovoditi u pitanje obveze sadržane u alatu za prijenos iz članka 46. OUZP-a na koji se oslanjate.

36. Morat ćete procijeniti relevantna opća pravila i prakse u mjeri u kojoj ona utječu na učinkovitu primjenu zaštitnih mjera sadržanih u alatu za prijenos iz članka 46. OUZP-a.

37. Tijekom provedbe te procjene bitni su i različiti elementi pravnog sustava te treće zemlje, npr. elementi navedeni u članku 45. stavku 2. OUZP-a. 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 podatcima. Postojanje sveobuhvatnog zakona za zaštitu osobnih podataka ili neovisnog nadležnog

[42] Prijenos osobnih podataka je postupak obrade (čl. 4., st. 2. OUZP-a) Ako želite prenijeti osjetljive podatke koji potpadaju pod članke 9. i 10. OUZP-a, prijenos možete izvršiti samo ako potpada u jedno od odstupanja i uvjeta navedenih u člancima 9. i 10. OUZP-a i zakonima država članica EU-a. U skladu s člankom 32. OUZP-a, također ćete morati provesti, s uvoznikom koji djeluje kao voditelj obrade ili izvršitelj obrade, odgovarajuće tehničke i organizacijske mjere kako biste osigurali razinu sigurnosti primjerenu rizicima za prava i slobode ispitanika koje predstavlja moguća povreda prenesenih osobnih podataka (čl. 4., st. 12. OUZP-a). Kategorije prenesenih podataka i njihova osjetljivost bit će relevantne za ocjenu rizika i primjerenost mjera.

[43] Neke treće zemlje ne dopuštaju uvoz šifriranih podataka.

[44] Kad je voditelj obrade dao prethodno posebno ili opće pisano odobrenje u skladu s člankom 28. stavkom 2. OUZP-a.

[45] Vidjeti članke 47. i 52. Povelje Europske unije o temeljnim pravima, članak 23., stavak 1. OUZP-a i Preporuke Europskog odbora za zaštitu podataka 02/2020 o europskim temeljnim jamstvima za mjere nadzora, 10. studenoga 2020. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

tijela za zaštitu podataka, kao i postupanje u skladu s međunarodnim instrumentima koji predviđaju mjere za zaštitu podataka, može pridonijeti osiguravanju razmjernosti zadiranja vlasti.

38. Smatrat će se da obveze ili ovlasti koje proizlaze iz takvih zakona i praksi narušavaju ili nisu u skladu s obvezama alata za prijenos iz članka 46. OUZP-a ako[46]:

- ne poštuju suštinu temeljnih prava i sloboda Povelje EU-a o temeljnim pravima ili
- premašuju ono što je potrebno i razmjerno u demokratskom društvu kako bi se zaštitio jedan od važnih ciljeva koji su također priznati u pravu Unije ili države članice, poput onih navedenih u čl. 23., st. 1. OUZP-a.

39. Trebate provjeriti mogu li se obveze uvoznika podataka koje ispitanicima omogućuju da ostvaruju svoja prava, kako su navedena u alatu za prijenos iz članka 46. OUZP-a (poput zahtjeva za pristup, ispravljanje i brisanje prenesenih podataka, kao i (sudske) zaštite) učinkovito primijeniti u praksi i uvjeriti se da pravo i/ili praksa treće zemlje odredišta ne priječi ispunjavanje tih obveza.

40. Standardi EU-a, kao što su članci 47. i 52. Povelje Europske unije o temeljnim pravima, moraju se upotrebljavati kao referentna norma, posebno za procjenu je li pristup tijela vlasti ograničen na ono što je nužno i razmjerno u demokratskom društvu i je li ispitanicima omogućena učinkovita pravna zaštita.

41. U preporukama Europskog odbora za zaštitu podataka o europskim temeljnim jamstvima[47] navode se objašnjenja elemenata koje je potrebno procijeniti kako bi se utvrdilo može li se pravni okvir kojim se regulira pristup osobnim podatcima javnih tijela u trećoj zemlji, odnosno agencija za nacionalnu sigurnost ili tijela kaznenog progona, smatrati opravdanim zadiranjem[48] ili ne. To se treba posebno pažljivo razmotriti kad je zakonodavstvo kojim se uređuje pristup podatcima od strane javnih tijela dvosmisleno ili nije javno dostupno. Prvi je zahtjev europskih temeljnih jamstava da treba postojati pravni okvir za takav pristup, kada je predviđen, koji je javno dostupan i dovoljno jasan.

42. Kad se primjenjuju na situacije prijenosa podataka na temelju alata za prijenos iz članka 46., Preporuke Europskog odbora za zaštitu podataka o europskim temeljnim jamstvima mogu usmjeravati izvoznika podataka i uvoznika podataka prilikom procjene zadiru li takve ovlasti neopravdano u obveze izvoznika i uvoznika podataka da osigura u načelu istovjetnu zaštitu u skladu s OUZP-om ili obvezama sadržanima u alatu za prijenos. Izostanak u načelu istovjetne razine zaštite bit će posebno očit kad zakonodavstvo i/ili praksa treće zemlje koji su relevantni za vaš prijenos ne ispunjavaju zahtjeve europskih temeljnih jamstava. Europski odbor za zaštitu podataka ponavlja da su europska temeljna jamstva referentne norme tijekom procjene zadiranja koja proizlaze iz mjera nadzora trećih zemalja u kontekstu međunarodnih prijenosa podataka. Te

[46] Vidjeti članke 47. i 52. Povelje Europske unije o temeljnim pravima, članak 23., stavak 1. OUZP-a, stavke 174. i 187. presude C-311/18 (Schrems II) i Preporuke Europskog odbora za zaštitu podataka 02/2020 o europskim temeljnim jamstvima za mjere nadzora, 10. studenoga 2020.,

[47] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020.

[48] Pa stoga ne dovodi u pitanje obveze preuzete u alatu za prijenos iz čl. 46. OUZP-a.

norme proizlaze iz prava Unije i sudske prakse Suda Europske unije i Europskog suda za ljudska prava koji su obvezujući za države članice EU-a.

43. Vaša se procjena prije svega treba temeljiti na javno dostupnom zakonodavstvu. Proučavanje i prakse tijela javne vlasti treće zemlje omogućit će vam da provjerite mogu li zaštitne mjere sadržane u alatu za prijenos iz članka 46. OUZP-a u praksi biti dovoljna sredstva osiguravanja učinkovite zaštite osobnih podataka koji se prenose.[49] Proučavanje praksi koje su na snazi u trećoj zemlji bit će posebno važno za vašu procjenu u situacijama opisanima u nastavku.

43.1 **Relevantno zakonodavstvo u trećoj zemlji može formalno ispunjavati standarde EU-a o temeljnim pravima i slobodama te o nužnosti i razmjernosti njihovih ograničenja.** Međutim, prakse njezinih javnih tijela (npr. pristup osobnim podatcima u posjedu privatnog sektora ili kada provode – ili ne provode – zakone kao nadzorna ili pravosudna tijela) mogu jasno upućivati na to da se obično ne primjenjuju / nisu u skladu sa zakonodavstvom kojim se uređuju, u načelu, njihove aktivnosti. U tom slučaju morate u svojoj procjeni uzeti u obzir te prakse i biti svjesni da alat za prijenos iz članka 46. OUZP-a neće moći učinkovito osigurati, sam po sebi (tj. bez dodatnih mjera), razinu zaštite koja je u načelu istovjetna. U tom slučaju, ako želite nastaviti s prijenosom, morat ćete provesti odgovarajuće dodatne mjere.

43.2 **U trećoj zemlji možda ne postoje relevantni zakoni (npr. o pristupu osobnim podatcima u posjedu privatnog sektora)**. U tom slučaju, iz nepostojanja relevantnih zakona ne možete automatski zaključiti da se vaš alat za prijenos iz članka 46. OUZP-a može učinkovito primijeniti. Morat ćete provjeriti jesu u toj zemlji na snazi prakse koje nisu u skladu s pravom EU-a i obvezama alata za prijenos iz članka 46. OUZP-a. Ako postoje nesukladne prakse, alat za prijenos iz članka 46. OUZP-a neće moći učinkovito osigurati, sam po sebi (tj. bez odgovarajućih dopunskih mjera), razinu zaštite koja je u načelu istovjetna. U tom slučaju, ako želite nastaviti s prijenosom, morat ćete provesti odgovarajuće dodatne mjere.

43.3 **Procjenom se može otkriti da je relevantno zakonodavstvo u trećoj zemlji problematično[50] i da preneseni podatci i/ili uvoznik potpadaju ili bi mogli potpadati pod područje primjene takvog problematičnog zakonodavstva.[51]**

U kontekstu neizvjesnosti oko potencijalne primjene problematičnog zakonodavstva na vaš prijenos, možete odlučiti:

- obustaviti prijenos

[49] C-311/18 (Schrems II), stavak 126.

[50] Pod „problematičnim zakonodavstvom“ podrazumijeva se zakonodavstvo: 1) kojim se primatelju osobnih podataka iz Europske unije nameću obveze i/ili utječe na podatke koji se prenose na način koji može dovesti u pitanje ugovorno jamstvo načelno istovjetne razine zaštite alata za prijenos i 2) kojim se ne poštuje suština temeljnih prava i sloboda priznatih Poveljom o temeljnim pravima EU-a ili premašuje ono što je potrebno i razmjerno u demokratskom društvu za zaštitu jednog od važnih ciljeva priznatih i u pravu Unije ili država članica EU-a, poput onih navedenih u čl. 23., st. 1. OUZP-a.

[51] Može biti nejasno jesu li uvoznik i/ili preneseni podatci obuhvaćeni općim pojmovima koji se često koriste u zakonima o nacionalnoj sigurnosti kako bi se ograničilo njihovo područje primjene, kao što su na primjer „pružatelj elektroničkih komunikacijskih usluga” i „podatci stranih obavještajnih službi”.

- provesti dodatne mjere[52] za sprječavanje rizika potencijalne primjene zakona i/ili prakse treće zemlje uvoznika podataka na vašeg uvoznika i/ili na vaše prenesene podatke koji mogu utjecati na ugovorna jamstva alata za prijenos načelno istovjetne razine zaštite onoj zajamčenoj u EGP-u ili

- Alternativno, možete odlučiti nastaviti s prijenosom bez obveze provedbe dodatnih mjera ako smatrate da nemate razloga vjerovati da će se relevantno i problematično zakonodavstvo primijeniti u praksi na vaše prenesene podatke i/ili uvoznika. Morat ćete dokazati i dokumentirati svojom procjenom, kada je to prikladno u suradnji s uvoznikom, da se zakon ne tumači i/ili ne primjenjuje u praksi na način da se primjenjuje na vaše prenesene podatke i uvoznika, također uzimajući u obzir iskustva drugih dionika koji djeluju unutar istog sektora i/ili su povezani sa sličnim prenesenim osobnim podatcima i dodatnim izvorima informacija koji su dodatno opisani u nastavku.[53]

  Stoga ćete detaljnim izvješćem morati pokazati i dokumentirati[54] da se problematično zakonodavstvo u praksi neće primjenjivati na vaše prenesene podatke i/ili uvoznika, te da, posljedično, neće spriječiti uvoznika u ispunjavanju njegovih obveza prema alatu za prijenos iz članka 46. OUZP-a.[55]

Mogući izvori informacija

44. Vaš 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 i prakse koji su mjerodavni za prijenos.

45. Vi i vaš uvoznik možete svoju procjenu upotpuniti informacijama dobivenima iz drugih izvora, kao što su oni navedeni kao primjeri u Prilogu 3.

46. Uz pravni okvir treće zemlje koji se primjenjuje na prijenos, izvori i informacije trebaju biti relevantni, objektivni, pouzdani, provjerljivi i javno dostupni ili na drugi način dostupni kako bi se utvrdilo može li se vaš alat za prijenos iz članka 46. učinkovito primijeniti[56], a vi ćete morati procijeniti i dokumentirati da jesu.

Relevantne: informacije moraju biti relevantne za određeni prijenos i/ili uvoznika i njihovu sukladnost sa zahtjevima propisanima u pravu EU-a i instrumentu za prijenos iz članka 46. OUZP-a, a ne pretjerano općenite ili apstraktne.

[52] Vidjeti uvodnu izjavu 109. OUZP-a i C-311/18 (Schrems II), stavak 132.
[53] Vidjeti točke 45. do 47.
[54] Izvješća koja ćete sastaviti morat će uključivati sveobuhvatne informacije o pravnoj ocjeni zakona i praksi te o njihovoj primjeni na posebne prijenose, interni postupak za izradu procjene (uključujući informacije o dionicima uključenima u procjenu – npr. odvjetničke tvrtke, konzultante ili interne odjele) i datume provjere. Izvješća treba ovjeriti zakonski predstavnik izvoznika.
[55] Dokazivanje da se problematično zakonodavstvo u praksi ne primjenjuje na vaše prenesene podatke i uvoznika, uzimajući u obzir i iskustvo drugih dionika koji djeluju u istom sektoru i/ili su povezani sa sličnim prenesenim osobnim podatcima, ne oslobađa vas od osiguravanja potrebnih dodatnih mjera za zaštitu osobnih podataka tijekom njihova prijenosa i obrade u trećoj zemlji odredišta (npr. end-to-end enkripcija podataka – vidi primjere dodatnih tehničkih mjera u Prilogu 2.) ako vaša analiza primjenjivog zakonodavstva treće zemlje odredišta navodi da se pristup podatcima također može dogoditi, čak i bez intervencije uvoznika, u tom trenutku prijenosa. Možda ste već predvidjeli takve mjere s uvoznikom koji djeluje kao voditelj obrade ili izvršitelj obrade u skladu s člankom 32. OUZP-a.
[56] Vidjeti Prilog 3. za ogledni popis izvora informacija koje vi i uvoznik možete koristiti.

Objektivne: informacije su potkrijepljene empirijskim dokazima temeljenima na znanju stečenom iz prošlosti, a ne pretpostavkama o mogućim događajima i rizicima.

Pouzdane: izvoznik i uvoznik moraju objektivno procijeniti pouzdanost izvora informacija i samih informacija te ih zasebno ocijeniti.

Provjerljive: informacije i zaključci trebaju biti provjerljivi ili usporedivi s drugim vrstama informacija ili izvora, u okviru ukupne procjene, među ostalim i kako bi se nadležnom nadzornom ili pravosudnom tijelu omogućilo da provjeri objektivnost i pouzdanost tih informacija, ako je to potrebno.

Javno dostupne ili na drugi način dostupne: u idealnim okolnostima, informacije trebaju biti javne ili barem dostupne kako bi se olakšala provjera naprijed navedenih kriterija i osiguralo njihovo moguće dijeljenje s nadzornim tijelima, pravosudnim tijelima i u konačnici s ispitanicima.

47. U obzir možete uzeti i dokumentirano praktično iskustvo uvoznika s relevantnim prethodnim slučajevima zahtjeva za pristup zaprimljenih od javnih tijela u trećoj zemlji. Iskustvo uvoznika moći ćete koristiti samo kao dodatni izvor informacija ako pravni okvir treće zemlje ne zabranjuje uvozniku da pruža informacije o zahtjevima javnih tijela za otkrivanje podataka ili o nepostojanju takvih zahtjeva (i također trebate dokumentirati takvu ocjenu). Međutim, morate imati na umu da se činjenica da uvoznik prethodno nije primio zahtjeve nikada ne može sama po sebi smatrati odlučujućim čimbenikom za učinkovitost alata za prijenos iz članka 46. OUZP-a koji omogućuje da se prijenos nastavi bez dodatnih mjera. Ove informacije, zajedno s drugim vrstama informacija dobivenih iz drugih izvora, moći ćete uzeti u obzir kao dio vaše ukupne procjene zakona i prakse treće zemlje u vezi s vašim prijenosom. Relevantno i dokumentirano iskustvo uvoznika treba biti potkrijepljeno relevantnim, objektivnim, pouzdanim, provjerljivim i javno dostupnim ili na drugi način dostupnim informacijama o praktičnoj primjeni relevantnog zakona i takve mu informacije ne smiju proturječiti (npr. postojanje ili nepostojanje zahtjeva za pristup koji su primili drugi dionici koji djeluju unutar istog sektora i/ili su povezani sa sličnim prenesenim osobnim podatcima[57] i/ili primjenom zakona u praksi, kao što su sudska praksa i izvješća neovisnih nadzornih tijela).

Rezultati vaše procjene

48. Ovu opću procjenu zakona i prakse treće zemlje vašeg uvoznika koji se primjenjuju na vaš prijenos trebate provesti s dužnom pažnjom i to temeljito dokumentirati. Tu procjenu mogu zatražiti vaša nadležna nadzorna i/ili pravosudna tijela i smatrati vas odgovornim za svaku odluku koju donesete na toj osnovi.[58]

49. Svojom procjenom u konačnici možete utvrditi da alat za prijenos iz članka 46. OUZP-a na koji se oslanjate:

    - učinkovito osigurava da se prenesenim osobnim podatcima 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

[57] Iskustvo može biti iskustvo drugih subjekata koje izravno poznajete zbog prethodnih prijenosa iste vrste koje ste izvršili ili koji su navedeni u relevantnoj sudskoj praksi, izvješćima nevladinih organizacija itd. (vidjeti Prilog 3.).
[58] Članak 5. stavak 2. OUZP-a.

temelju odabranog alata za prijenos. Taj biste zaključak trebali ponovno procijeniti u odgovarajućim vremenskim razmacima ili kad dođe do značajnih promjena (vidjeti 6. korak); ili

- ne osigurava učinkovito u načelu istovjetnu razinu zaštite. Uvoznik podataka ne može ispuniti svoje obveze zbog toga što zakonodavstvo i/ili prakse treće zemlje koji se primjenjuju na prijenos ne udovoljavaju standardima EU-a o temeljnim pravima i slobodama te nužnosti i razmjernosti ograničenja za zaštitu legitimnih ciljeva od javnog interesa. Sud EU-a naglasio je da u slučajevima u kojima su alati za prijenos iz članka 46. OUZP-a manjkavi, izvoznik podataka snosi odgovornost da provede učinkovite dodatne mjere ili da ne prenosi osobne podatke[59].

Primjer:

Osnovne informacije
Sud EU-a zaključio je da članak 702. FISA-e (zakon Sjedinjenih Američkih Država) ne poštuje minimalne zaštitne mjere koje proizlaze iz načela razmjernosti 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 propisanima na temelju prava Unije.

Ocjena:
Ako vas vaša procjena relevantnog zakonodavstva SAD-a navede na pretpostavku da bi vaš prijenos mogao potpasti u područje primjene članka 702. FISA-e, ali niste sigurni potpada li u područje njegove praktične primjene, možete odlučiti:

1. zaustaviti prijenos;
2. donijeti odgovarajuće dodatne mjere kojima se učinkovito osigurava razina zaštite prenesenih podataka koja je u načelu istovjetna onoj zajamčenoj u EGP-u; ili
3. u obzir uzeti druge objektivne, pouzdane, relevantne, provjerljive i po mogućnosti javno dostupne informacije (koje mogu uključivati informacije koje vam je dostavio vaš uvoznik podataka) kako biste razjasnili opseg primjene u praksi članka 702. FISA-e na vaš prijenos. Ove informacije trebaju pružiti odgovore na neka relevantna pitanja, kao što su sljedeća:

- Pokazuju li javno dostupne informacije da postoji zakonska zabrana obavještavanja o konkretnom zahtjevu za pristup zaprimljenim podatcima i široka ograničenja pružanja općih informacija o zaprimljenim zahtjevima za pristup podatcima ili nepostojanju zaprimljenih zahtjeva?

- Je li vaš uvoznik podataka potvrdio da je u prošlosti primao zahtjeve za pristup podatcima od tijela javne vlasti SAD-a? Ili je vaš uvoznik podataka potvrdio da u prošlosti nije primao zahtjeve za pristup podatcima od tijela javne vlasti SAD-a i da mu nije zabranjeno pružati informacije o takvim zahtjevima ili njihovom nepostojanju?

[59] Sud EU-a C-311/18 (Schrems II), stavci 134. i 135.

- Otkrivaju li javno dostupne informacije koje ste dobili o sudskoj praksi SAD-a i izvješća nadzornih tijela, organizacija civilnog društva i akademskih ustanova[60] da su uvoznici podataka iz istog sektora kao i vaš uvoznik u prošlosti primali zahtjeve za pristup podatcima za slične prenesene podatke?

Odgovori na ova pitanja koje dobijete svojom cjelokupnom procjenom navode vas na zaključak da:

- članak 702. FISA-e primjenjuje se u praksi na vaš određeni prijenos i stoga dovodi u pitanje učinkovitost vašeg alata za prijenos iz članka 46. OUZP-a. Prema tome, ako želite nastaviti prijenos, morate razmotriti, kada je to prikladno u suradnji s uvoznikom, možete li donijeti dodatne mjere koje učinkovito osiguravaju razinu zaštite prenesenih podataka koja je u načelu istovjetna onoj zajamčenoj u EGP-u. Ako ne možete pronaći učinkovite dodatne mjere, ne smijete prenositi osobne podatke;
ili
- članak 702. FISA-e u praksi se ne primjenjuje na vaš određeni prijenos i stoga ne dovodi u pitanje učinkovitost vašeg alata za prijenos iz članka 46. OUZP-a. U tom slučaju možete nastaviti prijenos bez ikakvih dodatnih mjera.
-

-

[60] Npr. odredbe članka 702. FISA-e; Poslovnik Suda za nadzor stranih obavještajnih službi (FISC), mišljenja i odluke FISC-a s kojih je skinuta tajnost, sudska praksa američkih sudova; izvješća i transkripti saslušanja Odbora za nadzor privatnosti i građanskih sloboda (PCLOB); izvješća Ureda glavnog inspektora – Ministarstva pravosuđa SAD-a; izvješća ravnatelja Ureda za građanske slobode i privatnost NSA-a; izvješća koje priprema Kongresna istraživačka služba; izvješća Zaklade američkog udruženja za građanske slobode (ACLU).

2.4 4. korak: donesite dodatne mjere

50. Ako je procjenom iz 3. koraka otkriveno da alat za prijenos iz članka 46. OUZP-a 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 podatcima u trećoj zemlji pruži razina zaštite koja je u načelu istovjetna razini zajamčenoj unutar EU-a.[61] „Dodatne mjere" po definiciji dopunjuju zaštitne mjere koje već pruža alat za prijenos iz članka 46. OUZP-a i sve druge primjenjive sigurnosne zahtjeve (npr. tehničke sigurnosne mjere) utvrđene OUZP-om.[62]

51. 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. OUZP-a. Ne morate ponavljati procjenu svaki put kada izvršite isti prijenos određene vrste podataka u istu treću zemlju. Neki od podataka planiranih za prijenos mogu zahtijevati dodatne mjere, dok drugi podatci možda neće (s obzirom na formalnu i/ili praktičnu primjenu zakona treće zemlje). Moći ćete se nadovezati na prethodne procjene i zaključke 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.

52. 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.

53. Ugovorne i organizacijske mjere same po sebi neće spriječiti pristup osobnim podatcima od strane javnih tijela treće zemlje na temelju problematičnog zakonodavstva i/ili praksi[63]. Doista, pojavit će se situacije u kojima će samo primjereno provedene tehničke mjere moći spriječiti pristup osobnim podatcima od strane javnih tijela u trećim zemljama ili ga učiniti neučinkovitim, posebno kada se podatcima nastoji pristupiti u nadzorne svrhe.[64] U takvim situacijama ugovornim i organizacijskim mjerama mogu se dopuniti tehničke mjere i može se ojačati sveukupna razina zaštite podataka (npr. uvođenjem provjera i uklanjanjem automatizama za pokušaje javnih tijela da pristupe podatcima na način koji nije u skladu sa standardima EU-a).

54. 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

---

[61] C-311/18 (Schrems II), stavak 96.

[62] Uvodna izjava 109. OUZP-a i C-311/18 (Schrems II), stavak 133.

[63] Pod „problematičnim zakonodavstvom" podrazumijeva se zakonodavstvo: 1) kojim se primatelju osobnih podataka iz Europske unije nameću obveze i/ili utječe na podatke koji se prenose na način koji može dovesti u pitanje ugovorno jamstvo načelno istovjetne razine zaštite alata za prijenos i 2) kojim se ne poštuje suština temeljnih prava i sloboda priznatih Poveljom o temeljnim pravima EU-a ili premašuje ono što je potrebno i razmjerno u demokratskom društvu za zaštitu jednog od važnih ciljeva priznatih i u pravu Unije ili država članica EU-a, poput onih navedenih u čl. 23., st. 1. OUZP-a.

[64] 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. OUZP-a, i Preporuke Europskog odbora za zaštitu podataka 02/2020 o europskim temeljnim jamstvima za mjere nadzora, 10. studenoga 2020., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

podataka od zahtjeva javnih tijela za pristup podatcima na temelju problematičnog zakonodavstva koje se primjenjuje u praksi:

- format podataka koji će se prenijeti (tj. nešifrirani/pseudonimizirani ili šifrirani podatci),
- priroda podataka (npr. viša razina zaštite pruža se u EGP-u kategorijama podataka obuhvaćenih člancima 9. i 10. OUZP-a)[65]
- 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)[66]
- tehnika ili parametri praktične primjene zakona treće zemlje koji su zaključeni u 3. koraku
- 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 podataka[67]).

[65] Vidjeti bilješku 42.
[66] 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.
[67] Vidjeti bilješku 26.

Primjeri dodatnih mjera

55. Neke primjere tehničkih, ugovornih i organizacijskih mjera za razmatranje, koje već nisu uključene u korišteni alat za prijenos iz članka 46. OUZP-a, možete pronaći u oglednom popisu opisanom u Prilogu 2.

***

56. Ako ste uspostavili učinkovite dodatne mjere koje u kombinaciji s odabranim alatom za prijenos iz članka 46. OUZP-a dosežu razinu zaštite koja je sada u načelu istovjetna razini zaštite zajamčenoj unutar EGP-a, možete nastaviti s prijenosom.

57. Ako ne možete pronaći ili provesti učinkovite dodatne mjere kojima se može osigurati da preneseni osobni podatci imaju u načelu istovjetnu razinu zaštite,[68] ne smijete početi prenositi osobne podatke u predmetnu treću zemlju na temelju alata za prijenos iz članka 46. OUZP-a na koji se oslanjate. Ako već vršite prijenose, morate obustaviti ili potpuno prekinuti prijenos osobnih podataka.[69] U skladu sa zaštitnim mjerama sadržanima u alatu za prijenos iz članka 46. OUZP-a 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.[70]

Primjer:

Pravom treće zemlje zabranjuju se dodatne mjere koje ste utvrdili (npr. zabranjuje se uporaba šifriranja) ili se na drugi način sprječava njihova učinkovitost. Ne smijete početi prenositi osobne podatke u tu zemlju ili morate zaustaviti postojeće prijenose u tu zemlju koji su u tijeku.

58. 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

59. 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. OUZP-a koji upotrebljavate ili planirate upotrebljavati.

---

[68] 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. OUZP-a, i Preporuke Europskog odbora za zaštitu podataka 02/2020 o europskim temeljnim jamstvima za mjere nadzora, 10. studenoga 2020., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[69] C-311/18 (Schrems II), stavak 135.

[70] Vidjeti, na primjer, 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.

2.5.1 Standardne klauzule o zaštiti podataka (članak 46. stavak 2. točke (c) i (d) OUZP-a)

60. 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 OUZP-om nije narušena.[71] 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).

61. 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 klauzule[72] i morate zatražiti odobrenje nadležnog nadzornog tijela u skladu s člankom 46. stavkom 3. točkom (a) OUZP-a.

2.5.2 Obvezujuća korporativna pravila (članak 46. stavak 2. točka (b) OUZP-a o zaštiti podataka)

62. Obrazloženje izneseno u presudi Schrems II primjenjuje se i na druge instrumente za prijenos u skladu s člankom 46. stavkom 2. OUZP-a 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.[73]

63. 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.

---

[71] U uvodnoj izjavi 109. OUZP-a navodi se: „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.

[72] 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. OUZP-a) o članku 28. već donesenih standardnih ugovornih klauzula, 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_art28sccs_si_en.pdf.

[73] Sud EU-a, C-311/18 (Schrems II), stavak 132.

64. Sve obveze koje je potrebno uključiti bit će navedene u ažuriranim referentnim dokumentima WP256/257[74] prema kojima će sve skupine koje se oslanjaju na OKP-ove kao alate za prijenos morati uskladiti svoje postojeće i buduće OKP-ove.

65. 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) OUZP-a)

66. Obrazloženje izneseno u presudi Schrems II primjenjuje se i na druge instrumente za prijenos u skladu s člankom 46. stavkom 2. OUZP-a 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.[75] 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.

2.6 6. korak: ponovna procjena u odgovarajućim vremenskim razmacima

67. Morate nadzirati, 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 početnu procjenu razine zaštite i na odluke koje ste možda donijeli na temelju te procjene u vezi s prijenosima. Odgovornost je kontinuirana obveza (članak 5. stavak 2. OUZP-a).

68. 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. OUZP-a ili ih ne može ispuniti, ili
- dodatne mjere više nisu učinkovite u toj trećoj zemlji.

3 ZAKLJUČAK

69. Opća uredba o zaštiti podataka propisuje pravila o obradi osobnih podataka u EGP-u i na taj način omogućuje slobodu kretanja osobnih podataka unutar EGP-a. Poglavlje V. OUZP-a 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. OUZP-a). U presudi Suda EU-a C-311/18 (Schrems II) naglašava se potreba osiguranja

[74] 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.
[75] Sud EU-a, C-311/18 (Schrems II), stavak 132.

kontinuiteta u razini zaštite koju pruža OUZP o zaštiti podataka kad su u pitanju osobni podatci preneseni u treću zemlju.[76]

70. 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 obrađuju.

71. 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. OUZP-a u kontekstu vaših prijenosa. Ako sam alat za prijenos iz članka 46. OUZP-a ne uspije postići u načelu istovjetnu razinu zaštite za osobne podatke koje prenosite, možete ga dopuniti dodatnim mjerama.

72. 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.

73. 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. OUZP-a i Poveljom o temeljnim pravima.

Za Europski odbor za zaštitu podataka

Predsjednica

(Andrea Jelinek)

[76] C-311/18 (Schrems II), stavak 93.

PRILOG 1.: DEFINICIJE

- „Treća zemlja” je bilo koja zemlja koja nije država članica EGP-a.
- „EGP” je Europski gospodarski prostor i uključuje sve države članice Europske unije i Island, Norvešku i Lihtenštajn. OUZP o zaštiti podataka primjenjuje se na potonje na temelju Sporazuma o Europskom gospodarskom prostoru, posebno njegovih priloga XI. i protokola 37.
- „OUZP” je 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” je Povelja Europske unije o temeljnim pravima, SL C 326, 26. 10. 2012., str. 391. – 407.
- „Sud EU-a” ili „Sud” je Sud Europske unije. Predstavlja pravosudno tijelo Europske unije i u suradnji sa sudovima država članica osigurava jedinstvenu primjenu i tumačenje prava Unije.
- „Izvoznik podataka” je voditelj obrade ili izvršitelj obrade unutar EGP-a koji prenosi osobne podatke voditelju obrade ili izvršitelju obrade u trećoj zemlji.
- „Uvoznik podataka” je voditelj obrade ili izvršitelj obrade u trećoj zemlji koji prima ili ostvaruje pristup osobnim podatcima prenesenima iz EGP-a.
- „Alat za prijenos iz članka 46. OUZP-a” odnosi se na odgovarajuće zaštitne mjere iz članka 46. OUZP-a koje izvoznici podataka uspostavljaju prilikom prijenosa osobnih podataka u treću zemlju u izostanku odluke o primjerenosti u skladu s člankom 45. stavkom 3. OUZP-a. Članak 46. stavci 2. i 3. OUZP-a sadrže popis alata za prijenos iz članka 46. OUZP-a koje voditelji obrade i izvršitelji obrade mogu upotrebljavati.
- „Standardne ugovorne klauzule” su 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 OUZP-a, u skladu s člankom 46. stavkom 2. točkom (c) i člankom 46. stavkom 5. OUZP-a.

PRILOG 2.: PRIMJERI DODATNIH MJERA

74. Sljedeće mjere predstavljaju primjere dodatnih mjera koje možete razmotriti kad dosegnete 4. korak „Donesite dodatne mjere". Taj popis nije potpun. Možete istražiti druge dodatne mjere. Budući tehnološki, pravni ili organizacijski razvoji mogu dovesti do pojave novih dodatnih mjera koje morate razmotriti. 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.

75. Bilo koja dodatna mjera može se smatrati učinkovitom u smislu presude Suda EU-a „Schrems II" ako otklanja određene nedostatke koje ste utvrdili u svojoj procjeni situacije u trećoj zemlji u pogledu zakona i praksi koji se primjenjuju na vaš prijenos i samo u mjeri u kojoj otklanja te nedostatke – sama po sebi ili u kombinaciji s drugima. Ako u konačnici ne možete osigurati u načelu istovjetnu razinu zaštite, ne smijete prenositi osobne podatke.

76. Kao voditelj obrade ili izvršitelj obrade možda već morate provesti neke mjere opisane u ovom prilogu kako biste bili u skladu s OUZP-om. To znači da bi slične mjere mogle biti potrebne za osobne podatke koji se obrađuju u EGP-u, prenose uvozniku podataka koji je obuhvaćen odlukom o primjerenosti ili u druge treće zemlje.[77]

2.1 Tehničke mjere

77. U ovom se odjeljku opisuju ogledni primjeri tehničkih mjera kojima se mogu dopuniti zaštitne mjere sadržane u alatima za prijenos iz članka 46. OUZP-a 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. OUZP-a i koje, posebice, mogu ugroziti ugovorno jamstvo o načelu istovjetne razine zaštite od pristupa javnih tijela treće zemlje tim podatcima.[78]

78. Kako bi se postigla veća jasnoća, u ovom se odjeljku prvo opisuju neki primjeri scenarija za neke tehničke mjere koje bi potencijalno mogle biti učinkovite u osiguranju načelno istovjetne razine zaštite. U nastavku odjeljka navode se neki scenariji za koje nisu utvrđene tehničke mjere za osiguranje ove razine zaštite.

[77] Članak 5. stavak 2. i članak 32. OUZP-a.
[78] C-311/18 (Schrems II), stavak 135.

Primjeri scenarija koji se odnose na slučajeve u kojima su utvrđene *učinkovite* mjere

79. Mjere navedene u nastavku namijenjene su osiguravanju da pristup prenesenim podatcima od strane javnih tijela u trećim zemljama ne ugrozi učinkovitost odgovarajućih zaštitnih mjera sadržanih u alatima za prijenos iz članka 46. OUZP-a. Te bi mjere bile potrebne kako bi se zajamčila načelno istovjetna razina zaštite onoj zajamčenoj u EGP-u, čak i ako je pristup javnih tijela u skladu sa zakonom zemlje uvoznika ako takav pristup u praksi nadilazi ono što je nužno i razmjerno u demokratskom društvu.[79] Cilj je ovih mjera onemogućiti pristup podatcima 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 koji mogu sadržavati, među ostalim podatcima, mrežne identifikatore koje pružaju uređaji, aplikacije, alati i protokoli koje ispitanici upotrebljavaju u drugim kontekstima.

80. Javna tijela u trećim zemljama mogu nastojati pristupiti prenesenim podatcima

    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.

81. 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 podatcima 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.

82. Scenariji opisuju posebne okolnosti i poduzete mjere kako bi poslužili kao primjeri. Sve promjene u scenariju mogu dovesti do drugačijih zaključaka. Scenariji se odnose na situacije u kojima je

[79] Vidjeti članke 47. i 52. Povelje Europske unije o temeljnim pravima, članak 23. stavak 1. OUZP-a, i Preporuke Europskog odbora za zaštitu podataka 02/2020 o europskim temeljnim jamstvima za mjere nadzora, 10. studenoga 2020.

zaključeno da su prije svega potrebne dodatne mjere, odnosno situacije u kojima se u praksi na predmetni prijenos primjenjuje problematično zakonodavstvo treće zemlje.

83. 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. OUZP-a 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 podatcima

84. 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, a identitet je uvoznika potvrđen
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 kriptoanalizu 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[80]
3. snaga šifriranja i duljina ključa uzima u obzir određeno vremensko razdoblje tijekom kojeg se mora očuvati povjerljivost šifriranih osobnih podataka[81]
4. algoritam šifriranja besprijekorno je primijenjen pravilno održavanim softverom bez poznatih ranjivosti čija je sukladnost sa specifikacijom odabranog algoritma provjerena, npr. certificiranjem

[80] Za procjenu snage algoritama za šifriranje, njihove sukladnosti s najnovijim dostignućima i njihove otpornosti na kriptoanalizu tijekom vremena, izvoznici podataka mogu se osloniti na tehničke smjernice koje su objavila službena tijela za računalnu sigurnost EU-a i njegovih država članica. Vidjeti, na primjer, Izvješće ENISA-e « What is 'state of the art' in IT security? », 2019., https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security; smjernice njemačkog Saveznog ureda za informacijsku sigurnost u njegovim Tehničkim smjernicama serije TR-02102 i "Algorithms, Key Size and Protocols Report (2018.), H2020-ICT-2014 – Projekt 645421, D5.4, ECRYPT-CSA, 02/2018" na https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

[81] Zaštitni kapacitet kriptografskih algoritama s vremenom je podložan opadanju zbog otkrivanja novih kriptoanalitičkih tehnika, pojave novih računalnih paradigmi poput kvantnog računalstva i općeg povećanja raspoložive računalne snage, osim ako se ne dokaže da su primijenjeni algoritmi teoretski sigurni. Ovo se pitanje posebno odnosi na algoritme javnog ključa koji su u vrijeme pisanja ovog dokumenta u općoj upotrebi. Zbog toga izvoznik podataka mora uzeti u obzir da se javna tijela mogu obvezati na to da pristupe šifriranim podatcima u okolnostima opisanima u stavku br. 80 i pohrane ih dok njihovi resursi ne budu dovoljni za dešifriranje. Dodatna mjera može se smatrati učinkovitom samo ako takvo dešifriranje i naknadna daljnja obrada u to vrijeme više ne bi predstavljali povredu prava ispitanika, npr. jer se podatci više ne mogu koristiti za njihovu izravnu ili neizravnu identifikaciju.

5. ključevima se pouzdano upravlja (stvaranje, upravljanje, pohranjivanje te, ako je potrebno, povezivanje s identitetom namjeravanog primatelja, opoziv) [82] i
6. ključevi se zadržavaju isključivo pod kontrolom izvoznika podataka ili subjekta kojemu izvoznik vjeruje u EGP-u ili pod područjem nadležnosti u kojem se nudi u načelu istovjetnu razinu zaštite onoj zajamčenoj unutar EGP-a,

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

2. slučaj uporabe: prijenos pseudonimiziranih podataka

85. 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 informacija [83]
2. dodatne informacije drži isključivo izvoznik podataka i čuva ih odvojeno u državi članici ili u trećoj zemlji, subjekt kojem vjeruje izvoznik u EGP-u ili u području nadležnosti u kojem se nudi razina zaštite koja je načelno istovjetna onoj zajamčenoj unutar EGP-a
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. temeljitom analizom predmetnih podataka voditelj obrade utvrdio je, uzimajući u obzir sve informacije za koje se može očekivati da ih javna tijela zemlje primateljice posjeduju i koriste, 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.

86. 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

---

[82] Posebna publikacija NIST-a 800-57, Preporuka za upravljanje ključevima https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

[83] U skladu s člankom 4. stavkom 5. OUZP-a: „„pseudonimizacija“ je obrada osobnih podataka na način da se osobni podatci više ne mogu pripisati određenom ispitaniku bez upotrebe 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“; dodatni podatci mogu se sastojati od tablica u kojima se pseudonimi postavljaju uz identifikacijske atribute koje zamjenjuju, kriptografskih ključeva ili drugih parametara za transformaciju atributa ili drugih podataka koji dopuštaju pripisivanje pseudonimiziranih podataka identificiranim fizičkim osobama ili fizičkim osobama koje se mogu identificirati.

interakcija s internetskom uslugom u određenim trenutcima[84] mogu omogućiti utvrđivanje identiteta te osobe čak i ako se ime, adresa ili drugi jednostavni identifikatori osobe izostave.

87. 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.

88. 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.

89. Ako se tijekom izvođenja pseudonimizacije atributi sadržani u osobnim podatcima transformiraju pomoću kriptografskog algoritma, tada se primjenjuju smjernice navedene u bilješkama 80 i 81. Od sada se preporučuje napustiti isključivu upotrebu kriptografije i primijeniti transformacije koje se temelje na mehanizmima pretraživanja tablica.

3. slučaj uporabe: šifriranje podataka radi zaštite od pristupa javnih tijela treće zemlje uvoznika kada se podatci prenose između izvoznika i njegova uvoznika

90. Izvoznik podataka želi prenijeti podatke na odredište gdje zakon i/ili praksa dopuštaju javnim tijelima pristup podatcima dok oni prolaze između zemlje izvoznika i zemlje odredišta.

Ako vrijedi sljedeće:

1. izvoznik podataka prenosi osobne podatke uvozniku podataka u području nadležnosti u kojem zakon i/ili praksa dopuštaju javnim tijelima pristup podatcima dok se oni prenose putem interneta u ovu treću zemlju bez europskih temeljnih jamstava u vezi s tim pristupom, 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
2. subjekti uključeni u komunikaciju suglasni su oko pouzdanog certifikacijskog tijela koje izdaje certifikat javnog ključa ili oko infrastrukture javnog ključa
3. protiv aktivnih i pasivnih napada na sustave slanja i primanja koji osiguravaju šifriranje prijenosa koriste se posebne zaštitne i najmodernije mjere, uključujući testove ranjivosti softvera i mogućih stražnjih ulaza
4. 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

[84] Članak 4. stavak 1. OUZP-a: „‚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;”.

5. 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 kriptoanalizu koju provode javna tijela kada se podatci prenose u tu treću zemlju, uzimajući u obzir resurse i tehničke mogućnosti (npr. računalna snaga potrebna za napade grubom silom) koji su im na raspolaganju (vidjeti naprijed navedenu bilješku 80) [85]
6. snaga šifriranja uzima u obzir određeno vremensko razdoblje tijekom kojeg se mora očuvati povjerljivost šifriranih osobnih podataka
7. algoritam šifriranja besprijekorno je primijenjen pravilno održavanim softverom bez poznatih ranjivosti čija je sukladnost sa specifikacijom odabranog algoritma provjerena, npr. certificiranjem
8. 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

91. 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 podatcima 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 podatcima 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. OUZP-a
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, eventualno, sami izvoznik ili drugi subjekt kojemu izvoznik vjeruje, a koji se nalazi u EGP-u ili području nadležnosti u kojem se nudi razina zaštite koja je u načelu istovjetna onoj zajamčenoj unutar EGP-a i ključ je odgovarajuće zaštićen od neovlaštene upotrebe 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,

[85] Vidjeti bilješku 80 za neka upućivanja na tehničke smjernice koje su objavila službena tijela za računalnu sigurnost EU-a i njegovih država članica.

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

92. 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, a da im se pritom ne 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 dijela ili više dijelova od kojih se nijedan 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. temeljitom analizom predmetnih podataka voditelj obrade utvrdio je, uzimajući u obzir sve informacije koje nedostaju, a za koje se može pretpostaviti da ih javna tijela zemalja primateljica posjeduju i koriste, 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
6. 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 podatcima u posjedu izvršitelja obrade u svim predmetnim jurisdikcijama,

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

Primjeri scenarija koji se odnose na slučajeve u kojima *učinkovite* mjere nisu utvrđene

93. 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 primjerene dodatne mjere.

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

94. Izvoznik podataka prenosi osobne podatke elektroničkim putem ili stavljajući ih na raspolaganje pružatelju usluga u oblaku ili drugom izvršitelju obrade radi obrade osobnih podataka u skladu s njegovim uputama u trećoj zemlji (npr. za pružanje tehničke podrške ili bilo koje vrste obrade u oblaku), a ti podatci nisu pseudonimizirani – ili se ne mogu pseudonimizirati – kako je opisano u 2. slučaju upotrebe ili šifrirati kako je opisano u 1. slučaju upotrebe jer obrada zahtijeva pristup nešifriranim podatcima.

Ako vrijedi sljedeće:

1. voditelj obrade prenosi osobne podatke pružatelju usluga u oblaku ili drugom izvršitelju obrade
2. pružatelj usluga u oblaku ili drugi izvršitelj obrade treba pristup nešifriranim podatcima kako bi izvršio dodijeljeni zadatak i
3. ovlasti dane javnim tijelima u zemlji primateljici za pristup prenesenim podatcima nadilaze ono što je nužno i razmjerno u demokratskom društvu kada se u praksi problematično zakonodavstvo treće zemlje primjenjuje na predmetne prijenose (vidi 3. korak).[86]

Europski odbor za zaštitu podataka, s obzirom na trenutačna najmodernija dostignuća, ne može predvidjeti učinkovitu tehničku mjeru kojom bi se spriječila povreda temeljnih 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 podatcima.

95. 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: prijenos osobnih podataka u poslovne svrhe, uključujući putem daljinskog pristupa

96. Izvoznik podataka prenosi osobne podatke subjektima – u trećoj zemlji kako bi se koristili u zajedničke poslovne svrhe – elektronički putem ili stavljanjem na raspolaganje za daljinski pristup od strane uvoznika podataka, a ti podatci nisu pseudonimizirani – ili se ne mogu pseudonimizirati – kako je opisano u 2. slučaju upotrebe ili šifrirati kako je opisano u 1. slučaju upotrebe jer obrada zahtijeva pristup nešifriranim podatcima. Jedna 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 grupe poduzeća, ili skupine 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.

[86] Vidjeti članke 47. i 52. Povelje Europske unije o temeljnim pravima, članak 23. stavak 1. OUZP-a, i Preporuke Europskog odbora za zaštitu podataka 02/2020 o europskim temeljnim jamstvima za mjere nadzora, 10. studenoga 2020.,

Ako vrijedi sljedeće:

1. izvoznik podataka prenosi osobne podatke uvozniku podataka u trećoj zemlji tako što podatke čini dostupnima u informacijskom sustavu, na način kojim se uvozniku omogućuje izravan pristup podatcima po njegovom izboru, ili tako što izravno prenosi podatke, pojedinačno ili skupno, uporabom komunikacijske usluge;
2. uvoznik[87] obrađuje nešifrirane podatke u trećoj zemlji (uključujući za vlastite potrebe kada je uvoznik voditelj obrade);
3. ovlasti dane javnim tijelima u zemlji primateljici za pristup predmetnim prenesenim podatcima nadilaze ono što je nužno i razmjerno u demokratskom društvu kada se u praksi problematično zakonodavstvo treće zemlje primjenjuju na predmetne prijenose (vidjeti 3. korak),

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

97. 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.

[87] Bilo da se radi o voditelju obrade ili izvršitelju obrade u trećoj zemlji koji prima osobne podatke ili dobiva pristup osobnim podatcima prenesenim iz EGP-a.

2.2 Dodatne ugovorne mjere

98. Te će se mjere općenito sastojati od jednostranih, dvostranih ili višestranih[88] ugovornih obveza.[89] Ako se upotrebljava alat za prijenos iz članka 46. OUZP-a, u većini će slučajeva već sadržavati određen broj (uglavnom ugovornih) obveza izvoznika podataka i uvoznika podataka koje služe kao zaštitne mjere za osobne podatke.[90]

99. U nekim situacijama tim se mjerama 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 EGP-a. S obzirom na narav ugovornih mjera koje općenito ne mogu obvezivati tijela te treće zemlje ako ta tijela nisu ugovorna strana,[91] te će se mjere vjerojatno često morati 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.

100. Ovisno o tome koje su ugovorne mjere već sadržane u alatu za prijenos iz članka 46. OUZP-a 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.

101. Kao što je već rečeno, ugovorne mjere neće moći spriječiti primjenu propisa treće zemlje koji ne zadovoljavaju standarde europskih temeljnih jamstava Europskog odbora za zaštitu podataka u onim slučajevima u kojima propisi obvezuju uvoznike da postupe po nalozima za otkrivanje podataka koje prime od javnim tijela.[92]

102. Neki primjeri tih mogućih ugovornih mjera navedeni su u nastavku i razvrstani prema njihovoj naravi.

Predviđanje ugovorne obveze uporabe određenih tehničkih mjera

103. Ovisno o posebnim okolnostima prijenosa (uključujući praktičnu primjenu zakonodavstva treće zemlje), ugovorom će se možda morati predvidjeti primjena posebnih tehničkih mjera da bi se prijenos mogao obaviti (vidjeti tehničke mjere predložene ranije u ovom dokumentu).

104. Uvjeti za učinkovitost:

---

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

[89] 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.

[90] 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.).

[91] C-311/18 (Schrems II), stavak 125.

[92] Presuda Suda EU-a C-311/18 (Schrems II), stavak 132.

- 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.

Obveze transparentnosti:

105. Izvoznik može ugovoru dodati priloge s informacijama koje bi uvoznik trebao pružiti prije sklapanja ugovora, koliko god mu je to moguće, o pristupu podatcima od strane javnih tijela, uključujući u obavještajnom području, pod uvjetom da je zakonodavstvo u skladu s europskim temeljnim jamstvima Europskog odbora za zaštitu podataka, u zemlji odredišta. To izvozniku podataka može pomoći da ispuni obvezu dokumentiranja svoje procjene razine zaštite u trećoj zemlji. Također može naglasiti obvezu uvoznika da pomogne izvozniku u njegovoj procjeni i uključiti njegovu odgovornost u pružanju informacija koje su objektivne, pouzdane, relevantne, provjerljive i javno dostupne ili na drugi način dostupne.

106. 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 podatcima koji se prenose, posebno u obavještajnom području, području kaznenog progona i području administrativnog i regulatornog nadzora, koji su primjenjivi na prenesene podatke

(2) u izostanku zakona kojima se uređuje pristup javnih tijela podatcima, da navede informacije i statističke podatke 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 podatcima u situacijama sličnima situaciji predmetnog prijenosa podataka (odnosno u određenom regulatornom području, s obzirom na vrstu subjekta kakav je uvoznik podataka i sl.)

(3) da navede koje se mjere provode da bi se spriječio pristup prenesenim podatcima (ako takve postoje)

(4) da pruži dovoljno detaljne informacije o svim zahtjevima za pristup osobnim podatcima od strane javnih tijela koje je uvoznik primio tijekom određenom razdoblja,[93] posebno u područjima navedenima u točki (1) i to informacije o zahtjevima koje je primio, podatcima 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[94]

(5) da navede je li i u kojoj mjeri uvozniku zakonski zabranjeno pružiti informacije navedene u točkama (1) – (5).

107. 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.

[93] Duljina razdoblja trebala bi ovisiti o riziku za prava i slobode ispitanika čiji se podatci predmet prijenosa, npr. zadnja godina prije sklapanja instrumenta za izvoz podataka s izvoznikom podataka.
[94] 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.

108. 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.
- 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 ispuni svoju obvezu obustave prijenosa i/ili raskida ugovora ako pravo treće zemlje, zaštitne mjere sadržane u upotrijebljenom alatu za prijenos iz članka 46. OUZP-a i sve dodatne zaštitne mjere koje je možda usvojio više ne mogu osigurati razinu zaštite koja je u načelu istovjetna razini zaštite u EGP-u. Međutim, ta obaveza ne može opravdati otkrivanje osobnih podataka od strane uvoznika ni stvoriti očekivanje da neće biti daljnjih zahtjeva za pristup.

***

109. 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 podatcima, (2) nije namjerno stvorio ili izmijenio svoje poslovne procese na način koji olakšava pristup osobnim podatcima ili sustavima i (3) nacionalno pravo ili vladine politike od uvoznika ne zahtijevaju da stvori ili održava stražnje ulaze ili da olakša pristup osobnim podatcima ili sustavima ili da posjeduje ili tijelima vlasti preda ključ za šifriranje.[95]

110. 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.
- 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.
- U okolnostima u kojima je uvoznik podataka otkrio prenesene osobne podatke povredom obveza sadržanih u odabranom alatu za prijenos, ugovor može uključivati i naknadu štete koju uvoznik podataka treba platiti ispitaniku za sve pretrpljene materijalne i nematerijalne štete.

***

111. Izvoznik bi mogao ojačati svoje ovlasti da provodi revizije[96] 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.

---

[95] Ova je klauzula važna kako bi se zajamčila primjerena razina zaštite prenesenih osobnih podataka i obično bi trebala biti obvezna.

[96] 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.

112. 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 (npr. treba ih učiniti nepromjenjivima upotrebom najmodernijih tehnika šifriranja, kao što je raspršivanje, i sustavno povremeno prenositi izvozniku) 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.

***

113. Ako su pravo i praksa treće zemlje uvoznika početno procijenjeni 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, u slučaju promjene situacije, odmah obavijesti ako nije u mogućnosti ispuniti ugovorne obveze i stoga ni propisani standard „u načelu istovjetne razine zaštite podataka“[97].

114. Ta nemogućnost ispunjavanja obveza može biti rezultat izmjena u zakonodavstvu ili praksi treće zemlje.[98] 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.

115. Uvjeti za učinkovitost:

- Izvoznika podataka treba obavijestiti prije nego što se odobri pristup podatcima. 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

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

[98] 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.”

obavijestiti izvoznika podataka, po mogućnosti prije nego što se one provedu kako bi izvoznik podataka mogao uzeti podatke od uvoznika.

- Klauzulama bi trebalo 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 potrebe da čeka upute izvoznika, ako se zadovolji određeni prag[99] koji će izvoznik podataka i uvoznik podataka dogovoriti. Uvoznik treba primjenjivati 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.

***

116. 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.

117. 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

118. 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.

[99] Ovaj prag treba osigurati da se ispitanicima i dalje pruža razina zaštite koja je u načelu istovjetna onoj zajamčenoj unutar EGP-a.

119. 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 podatcima 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.

***

120. 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. OUZP-a[100] 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.

121. 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.

[100] 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”.* Sud EU-a potvrđuje da su odredbe OUZP-a, tumačene u vezi s Poveljom Europske unije o temeljnim pravima, dio tog zakonodavstva, vidjeti Sud EU-a C-311/18 (Schrems II), stavak 138.

Osnaživanje ispitanika da ostvaruju svoja prava

122. Ugovorom se može predvidjeti da se osobnim podatcima koji se prenose nešifrirani tijekom redovitog poslovanja (uključujući u slučajevima pružanja podrške) može pristupiti samo uz izričiti ili implicitni pristanak izvoznika i/ili ispitanika za određeni pristup podatcima.

123. 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 podatcima 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).[101]
- 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.

***

124. 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 ispuni 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), uključujući naknadu koju uvoznik podataka treba platiti za bilo kakvu materijalnu i nematerijalnu štetu pretrpljenu zbog otkrivanja osobnih podataka ispitanika prenesenih u okviru odabranog alata za prijenos kojim se krše obveze koje sadrži.

125. Uvjeti za učinkovitost:

- Tom bi se obavijesti moglo upozoriti ispitanika o potencijalnim pristupima javnih tijela trećih zemalja njegovim podatcima. 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 i nadoknaditi 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 podatcima.
- 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

[101] Članak 4. stavak 11. OUZP-a.

ili prekidu prijenosa njegovih osobnih podataka zbog nemogućnosti uvoznika da ispuni svoje ugovorne obveze jer je primio zahtjev za pristup.

***

126. 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.

127. Uvjeti za učinkovitost:

- Neki nacionalni propisi možda neće dopustiti uvozniku podataka pružanje ove vrste pomoći izravno ispitanicima iako mogu dopustiti uvozniku podataka da tu pomoć za ispitanike osigura.
- 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 EGP-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, uključujući mehanizam zaštite protiv mjera nadzora.

2.3 Organizacijske mjere

128. 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 podatcima 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 EGP-u.

129. 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

130. Donošenje odgovarajućih unutarnjih politika s jasnom raspodjelom odgovornosti za prijenose podataka, kanalima prijavljivanja i standardnim operativnim postupcima za slučajeve formalnih ili neformalnih zahtjeva za pristup podatcima od strane javnih tijela. Posebno u slučaju prijenosa među grupama poduzeća, te politike mogu među ostalim uključivati imenovanje posebnog tima koji bi se trebao sastojati se od stručnjaka u području informacijskih tehnologija, zakona o zaštiti podataka i privatnosti, koji bi se bavili zahtjevima koji uključuju osobne podatke prenesene iz EGP-a; obavještavanje višeg pravnog i korporacijskog rukovodstva i izvoznika podataka po primitku takvih zahtjeva; postupovne korake za osporavanje nerazmjernih ili nezakonitih zahtjeva i pružanje transparentnih informacija ispitanicima.

131. Razvijanje posebnih postupaka osposobljavanja za osoblje odgovorno za upravljanje zahtjevima za pristup osobnim podatcima 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 podatcima, 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.

132. 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.[102] 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 podatcima.

Mjere transparentnosti i odgovornosti

133. 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 trebalo bi staviti na raspolaganje izvozniku podataka koji bi ju trebao prenijeti predmetnim ispitanicima.

134. 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 dostaviti evidenciju uzrokovala nemogućnost pružanja odgovarajuće razine zaštite.

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

***

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

136. 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

137. 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 podatcima 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 podatcima u EGP-u na daljinu, kao u slučajevima pružanja podrške kad se odobrava ograničen pristup umjesto potpunog pristupa podatcima; ili kad je za pružanje usluge potreban prijenos samo ograničenog skupa podataka, a ne cijele baze podataka).

138. 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 podatcima uzrokovao otkrivanje podataka koji se mogu identificirati.

***

139. 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 povezanima s međunarodnim prijenosima osobnih podataka.

140. 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.

Donošenje standarda i najboljih praksi

141. Donošenje 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.

Ostalo

142. Donošenje 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 načelno istovjetna razini zaštite zajamčenoj u EGP-u.

***

143. 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 koja je načelno istovjetna razini zaštite u EGP-u.[103]

[103] C-311/18 (Schrems II), stavci 135. i 137.

PRILOG 3.: MOGUĆI IZVORI INFORMACIJA ZA PROCJENU TREĆE ZEMLJE

144. 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 i prakse koji se primjenjuju na uvoznika i podatke koji se prenose. Vi i uvoznik možete provjeriti nekoliko izvora informacija, kao što su oni koji su ogledno navedeni u nastavku i prikazani prema redoslijedu poželjnosti:

- sudska praksa Suda Europske unije (Suda EU-a) i Europskog suda za ljudska prava (ESLJP)[104] na koju se upućuje u preporukama o europskim temeljnim jamstvima[105]
- odluke o primjerenosti u zemlji odredišta ako se prijenos oslanja na drugačiju pravnu osnovu[106]
- rezolucije i izvješća međuvladinih organizacija poput Vijeća Europe,[107] drugih regionalnih tijela[108] i tijela i agencija UN-a (npr. Vijeće Ujedinjenih naroda za ljudska prava,[109] Odbor za ljudska prava[110])
- izvješća i analize nadležnih regulatornih mreža, kao što je Svjetska konferencija povjerenika za zaštitu osobnih podataka i privatnosti (GPA)[111]
- nacionalna sudska praksa ili odluke neovisnih pravosudnih ili administrativnih tijela vlasti nadležnih u području privatnosti i zaštite podataka u trećim zemljama
- izvješća neovisnih nadzornih ili parlamentarnih tijela
- izvješća koja se temelje na praktičnom iskustvu s prethodnim slučajevima zahtjeva za otkrivanje podataka od strane tijela javne vlasti, ili nepostojanjem takvih zahtjeva, a koja su izdali subjekti aktivni u istom sektoru kao i uvoznik
- lažne obavijesti o nepostojanju naloga drugih subjekata koji obrađuju podatke u istom polju kao i uvoznik
- izvješća koja su izradile ili naručile gospodarske komore, poslovna, profesionalna i trgovačka udruženja, državne diplomatske, trgovinske i investicijske agencije izvoznika ili drugih trećih zemalja koje izvoze u treću zemlju u koju se podatci prenose
- izvješća akademskih institucija i organizacija civilnog društva (npr. nevladine organizacije)

---

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

[105] Preporuke EDPB-a 02/2020 o europskim temeljnim jamstvima za mjere nadzora, 10. studenog 2020., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en

[106] 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

[107] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

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

[109] Vidjeti https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx

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

[111] Vidjeti, na primjer: https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf

- izvješća privatnih pružatelja poslovnih informacija o financijskim, regulatornim i reputacijskim rizicima za tvrtke
- lažne obavijesti o nepostojanju naloga samog uvoznika[112]
- izvješća o transparentnosti, uz uvjet da se u njima izričito navodi činjenica da zahtjevi za pristup nisu zaprimljeni. Izvješća o transparentnosti koja ne navode ništa o ovome ne bi se kvalificirala kao dovoljan dokaz jer se ova izvješća najčešće fokusiraju na zahtjeve za pristup zaprimljene od tijela za provedbu zakona i navode brojke samo o ovom aspektu, dok ne navode ništa o zahtjevima za pristup primljenima u svrhe nacionalne sigurnosti. To ne znači da nisu primljeni zahtjevi za pristup, nego da se te informacije ne mogu dijeliti[113]
- interne izjave ili zapisi uvoznika koji izričito pokazuju da zahtjevi za pristup nisu primljeni dovoljno dugo; pri čemu prednost imaju izjave i zapisi koji uključuju odgovornost uvoznika i/ili koje su izdali interni službenici s određenom autonomijom kao što su unutarnji revizori, službenici za zaštitu podataka itd.[114]

[112] Vidjeti uvjete za razmatranje dokumentiranog praktičnog iskustva uvoznika s relevantnim prethodnim slučajevima zahtjeva za pristup zaprimljenih od tijela javne vlasti u trećoj zemlji u stavku 47.
[113] *Ibid.*
[114] *Ibid.*