Odporúčania

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

Odporúčania 01/2020 o opatreniach, ktoré dopĺňajú nástroje na prenos, aby sa zabezpečil súlad s úrovňou ochrany osobných údajov v EÚ

Verzia 2.0

Prijaté 18. júna 2021

Prijaté

História verzií

Verzia 2.0	18. jún 2021	Prijatie odporúčaní po verejnej konzultácii
Verzia 1.0	10. november 2020	Prijatie odporúčaní na verejnú konzultáciu

Zhrnutie

Všeobecné nariadenie EÚ o ochrane údajov bolo prijaté s dvojakým cieľom: uľahčenie voľného toku osobných údajov v rámci Európskej únie pri súčasnom zachovaní základných práv a slobôd fyzických osôb, najmä ich práva na ochranu osobných údajov.

Súdny dvor Európskej únie (SDEÚ) vo svojom nedávnom rozsudku vo veci C-311/18 (Schrems II) pripomína, že ochrana osobných údajov v Európskom hospodárskom priestore (EHP) musí byť zaručená všade tam, kam sa odovzdávajú údaje. Prenos osobných údajov do tretích krajín nemôže viesť k oslabeniu alebo narušeniu ochrany, ktorá im je poskytovaná v rámci EHP. Súdny dvor to tiež potvrdzuje tým, že objasňuje, že úroveň ochrany v tretích krajinách nemusí byť rovnaká ako úroveň zaručená v rámci EHP, ale musí byť v podstate rovnocenná [essentially equivalent]. Súdny dvor tiež potvrdzuje platnosť štandardných zmluvných doložiek ako nástroja na prenos, ktorý môže slúžiť na zmluvné zabezpečenie v podstate rovnocennej úrovne ochrany údajov prenášaných do tretích krajín.

Štandardné zmluvné doložky a iné nástroje na prenos uvedené v článku 46 všeobecného nariadenia o ochrane údajov nefungujú vo vákuu. Súdny dvor konštatuje, že prevádzkovatelia alebo sprostredkovatelia, ktorí konajú ako vývozcovia, sú v každom jednotlivom prípade, príp. aj v spolupráci s dovozcom v tretej krajine, zodpovední za overenie toho, či právne predpisy alebo postupy tretej krajiny ovplyvňujú účinnosť primeraných záruk uvedených v článku 46 všeobecného nariadenia o ochrane údajov. V týchto prípadoch Súdny dvor stále ponecháva vývozcom otvorenú možnosť zaviesť dodatočné opatrenia [supplementary measures], ktorými sa odstránia tieto medzery v ochrane a dosiahne sa úroveň vyžadovaná právnymi predpismi EÚ. Súdny dvor nešpecifikuje, aké opatrenia by to mohli byť. Súdny dvor však zdôrazňuje, že vývozcovia ich budú musieť v každom jednotlivom prípade identifikovať. Je to v súlade so zásadou zodpovednosti uvedenou v článku 5 ods. 2 všeobecného nariadenia o ochrane údajov, ktorá vyžaduje, aby prevádzkovatelia boli zodpovední za, a boli schopní preukázať, súlad so zásadami všeobecného nariadenia o ochrane údajov týkajúcimi sa spracúvania osobných údajov.

Európsky výbor pre ochranu údajov (EDPB) prijal tieto odporúčania s cieľom pomôcť vývozcom (či už prevádzkovateľom alebo sprostredkovateľom, súkromným subjektom alebo verejnoprávnym subjektom, ktoré spracúvajú osobné údaje v rozsahu pôsobnosti všeobecného nariadenia o ochrane údajov) s komplexnou úlohou posudzovania tretích krajín a v prípade potreby identifikácie vhodných dodatočných opatrení. Tieto odporúčania poskytujú vývozcom viacero krokov, ktoré treba podniknúť, možné zdroje informácií a niekoľko príkladov dodatočných opatrení, ktoré by sa mohli zaviesť.

EDPB vývozcom **v prvom kroku** odporúča, aby **poznali vlastné prenosy**. Mapovanie všetkých prenosov osobných údajov do tretích krajín môže byť náročné. Informácie o tom, kam osobné údaje odchádzajú, sú však potrebné na zabezpečenie toho, aby sa im poskytla v podstate rovnocenná úroveň ochrany bez ohľadu na to, kde sa spracúvajú. Musíte tiež overiť, či sú údaje, ktoré prenášate, primerané, relevantné a obmedzené vo vzťahu k tomu, čo je potrebné vzhľadom na účel, na ktorý sa spracúvajú.

Druhým krokom je **overiť, či nástroj na prenos, ktorý pri prenose využívate**, je uvedený v zozname v kapitole V všeobecného nariadenia o ochrane údajov. Ak už Európska komisia vyhlásila krajinu, región alebo sektor, do ktorých prenášate údaje, v jednom zo svojich rozhodnutí o primeranosti podľa článku 45 všeobecného nariadenia o ochrane údajov alebo na základe predchádzajúcej smernice 95/46 za primerané, pokiaľ je takéto rozhodnutie stále účinné, nebudete musieť podniknúť žiadne ďalšie kroky okrem monitorovania toho, či rozhodnutie o primeranosti zostáva v platnosti. Ak neexistuje rozhodnutie o primeranosti, musíte sa spoľahnúť na niektorý z nástrojov na prenos uvedených v článku 46 všeobecného nariadenia o ochrane údajov. Iba v niektorých prípadoch sa môžete spoľahnúť na niektorú z výnimiek uvedených v článku 49 všeobecného nariadenia o ochrane údajov, ak spĺňate podmienky. Výnimky sa v praxi nemôžu stať „pravidlom“, ale musia byť obmedzené na konkrétne situácie.

Prijaté

Tretím krokom je **posúdiť**, či platné právne predpisy a/alebo postupy tretej krajiny obsahujú niečo, čo v súvislosti s konkrétnym prenosom môže ovplyvniť účinnosť primeraných záruk nástrojov na prenos, ktoré využívate. Vaše hodnotenie by sa malo v prvom rade zamerať na právne predpisy tretej krajiny, ktoré sú relevantné pre váš prenos, a nástroj na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov, ktorý využívate. Taktiež na základe preskúmania postupov orgánov verejnej moci tretej krajiny môžete overiť, či záruky obsiahnuté v nástroji na prenos môžu v praxi zabezpečiť účinnú ochranu prenášaných osobných údajov. Preskúmanie týchto postupov bude pre vaše hodnotenie významné najmä vtedy, ak:

(i.) sa právne predpisy v tretej krajine, ktorá formálne spĺňa normy EÚ, v praxi zjavne neuplatňujú/nedodržiavajú;

(ii.) existujú postupy nezlučiteľné s požiadavkami nástroja na prenos, keď v tretej krajine chýbajú príslušné právne predpisy;

(iii.) vaše prenesené údaje a/alebo dovozca spadajú alebo by mohli spadať do pôsobnosti problematickej právnej úpravy (t. j. ovplyvňujúcej zmluvnú záruku nástroja na prenos, ktorá je v podstate na rovnocennej úrovni ochrany, a nespĺňajúcej normy EÚ týkajúce sa základných práv, nevyhnutnosti a proporcionality).

V prvých dvoch situáciách budete musieť pozastaviť prenos alebo prijať vhodné dodatočné opatrenia, ak v ňom chcete pokračovať.

V tretej situácii sa vzhľadom na neistoty týkajúce sa potenciálneho uplatnenia problematickej právnej úpravy na váš prenos môžete rozhodnúť: pozastaviť prenos, prijať dodatočné opatrenia na pokračovanie v prenose alebo sa môžete rozhodnúť pokračovať v prenose bez zavedenia dodatočných opatrení, ak usúdite a ste schopní preukázať a zdokumentovať, že nemáte dôvod domnievať sa, že relevantná a problematická právna úprava sa budú v praxi vykladať a/alebo uplatňovať tak, aby sa vzťahovali na vaše prenesené údaje a dovozcu.

Pokiaľ ide o hodnotenie prvkov, ktoré sa majú zohľadniť pri posudzovaní právnych predpisov tretej krajiny, ktoré sa zaoberajú prístupom orgánov verejnej moci k údajom na účely sledovania [surveillance], pozri odporúčania EDPB týkajúce sa európskych základných záruk.

Toto posúdenie by ste mali vykonať s náležitou starostlivosťou a dôkladne ho zdokumentovať. Vaše príslušné dozorné a/alebo súdne orgány to môžu vyžadovať a považovať vás za zodpovedných za akékoľvek rozhodnutie, ktoré na základe toho prijmete.

Štvrtým krokom je **identifikovať a prijať dodatočné opatrenia**, ktoré sú potrebné na to, aby úroveň ochrany prenášaných údajov dosiahla úroveň v podstate rovnocennú úrovni ochrany poskytovanej v EÚ. Tento krok je potrebný len vtedy, ak z posúdenia vyplynie, že právne predpisy tretej krajiny majú vplyv na účinnosť nástroja na prenos údajov podľa článku 46 všeobecného nariadenia o ochrane údajov, ktorý využívate, alebo chcete využívať v súvislosti s vaším prenosom. Tieto odporúčania obsahujú (v prílohe 2) aj orientačný zoznam príkladov dodatočných opatrení a niektoré podmienky na dosiahnutie ich účinnosti. Podobne ako v prípade primeraných záruk obsiahnutých v nástrojoch na prenos podľa článku 46, niektoré dodatočné opatrenia môžu byť účinné v niektorých krajinách, ale nie nevyhnutne v iných. Budete zodpovedný za posúdenie ich účinnosti v súvislosti s prenosom a vzhľadom na právne predpisy a postupy tretej krajiny a nástroje na prenos, ktoré využívate, a budete niesť zodpovednosť za akékoľvek rozhodnutie, ktoré na základe toho prijmete. Môže si to vyžadovať aj kombináciu niekoľkých dodatočných opatrení. V konečnom dôsledku môžete dospieť k záveru, že žiadne dodatočné opatrenie nemôže zabezpečiť v podstate rovnocennú úroveň ochrany konkrétneho prenosu. V prípadoch, keď nie je vhodné žiadne dodatočné opatrenie, musíte zabrániť prenosu, pozastaviť ho alebo ukončiť, aby nedošlo k ohrozeniu úrovne ochrany osobných údajov. Toto posúdenie dodatočných opatrení by ste mali vykonať s náležitou starostlivosťou a zdokumentovať ho.

Piatym krokom je **podniknúť** akékoľvek **formálne procesné kroky**, ktoré si prijatie vášho dodatočného opatrenia môže vyžadovať, v závislosti od nástroja na prenos údajov podľa článku 46 všeobecného nariadenia o ochrane údajov, ktorý využívate. V týchto odporúčaniach sú niektoré z týchto formalít konkretizované. O niektorých z nich sa možno budete musieť poradiť s vašimi príslušnými dozornými orgánmi.

Šiestym a posledným krokom je **prehodnocovať** v primeraných intervaloch úroveň ochrany údajov, ktoré prenášate do tretích krajín, a sledovať, či došlo alebo dôjde k akémukoľvek vývoju, ktorý by túto úroveň mohol ovplyvniť. Zásada zodpovednosti si vyžaduje nepretržitú obozretnosť, pokiaľ ide o úroveň ochrany osobných údajov.

Dozorné orgány budú naďalej vykonávať svoj mandát na monitorovanie uplatňovania všeobecného nariadenia o ochrane údajov a jeho presadzovanie. Dozorné orgány budú venovať náležitú pozornosť opatreniam, ktoré vývozcovia prijmú na zabezpečenie toho, aby údaje, ktoré prenášajú, mali v podstate rovnocennú úroveň ochrany. Ako pripomína Súdny dvor, dozorné orgány pozastavia alebo zakážu prenosy údajov v tých prípadoch, keď na základe vyšetrovania alebo sťažnosti zistia, že nie je možné zabezpečiť v podstate rovnocennú úroveň ochrany.

Dozorné orgány budú naďalej vypracúvať usmernenia pre vývozcov a koordinovať ich činnosť v rámci EDPB s cieľom zabezpečiť konzistentnosť pri uplatňovaní právnych predpisov EÚ o ochrane údajov.

OBSAH

Európsky výbor pre ochranu údajov

so zreteľom na článok 70 ods. 1 písm. e) nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „všeobecné nariadenie o ochrane údajov“),

so zreteľom na Dohodu o Európskom hospodárskom priestore (EHP), najmä na jej prílohu XI a protokol 37, ktoré boli zmenené rozhodnutím Spoločného výboru EHP č. 154/2018 zo 6. júla 2018[1],

so zreteľom na článok 12 a článok 22 svojho rokovacieho poriadku,

keďže:

(1) Súdny dvor Európskej únie (SDEÚ) vo svojom rozsudku zo 16. júla 2020 vo veci C-311/18, Data Protection Commissioner/Facebook Ireland LTD a Maximillian Schrems, dospel k záveru, že článok 46 ods. 1 a článok 46 ods. 2 písm. c) všeobecného nariadenia o ochrane údajov sa majú vykladať v tom zmysle, že primerané záruky, vymožiteľné práva a účinné právne prostriedky nápravy vyžadované týmito ustanoveniami musia zabezpečiť, aby práva osôb, ktorých osobné údaje sa prenášajú do tretej krajiny na základe štandardných doložiek o ochrane údajov, požívali úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v rámci Európskej únie týmto nariadením v spojení s Chartou základných práv Európskej únie.[2]

(2) Ako zdôraznil Súdny dvor, úroveň ochrany fyzických osôb, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v rámci Európskej únie všeobecným nariadením o ochrane údajov v spojení s Chartou, musí byť zaručená bez ohľadu na ustanovenie kapitoly V, na základe ktorého sa uskutočňuje prenos osobných údajov do tretej krajiny. Cieľom ustanovení kapitoly V je zabezpečiť kontinuitu vysokej úrovne tejto ochrany v prípade prenosu osobných údajov do tretej krajiny.[3]

(3) V odôvodnení 108 a článku 46 ods. 1 všeobecného nariadenia o ochrane údajov sa stanovuje, že ak neexistuje rozhodnutie EÚ o primeranosti, prevádzkovateľ alebo sprostredkovateľ by mali prijať opatrenia na kompenzáciu nedostatočnej ochrany údajov v tretej krajine prostredníctvom primeraných záruk pre dotknutú osobu. Prevádzkovateľ alebo sprostredkovateľ môžu ustanoviť primerané záruky bez toho, aby si to od dozorného orgánu vyžadovalo osobitné povolenie, a to prostredníctvom použitia jedného z nástrojov na prenos uvedených v článku 46 ods. 2 všeobecného nariadenia o ochrane údajov, ako sú napríklad štandardné doložky o ochrane údajov.

(4) Súdny dvor objasňuje, že cieľom štandardných doložiek o ochrane údajov prijatých Komisiou je len poskytnúť zmluvné záruky, ktoré sa jednotne uplatňujú vo všetkých tretích krajinách na

[1] Odkazy na „členské štáty“ uvedené v tomto dokumente by sa mali chápať ako odkazy na „členské štáty EHP“.
[2] Rozsudok SDEÚ zo 16. júla 2020, Data Protection Commissioner/Facebook Ireland Ltd a Maximillian Schrems [ďalej len „C-311/18 (Schrems II)“], druhý záver.
[3] C-311/18 (Schrems II), body 92 a 93.

prevádzkovateľov a sprostredkovateľov usadených v Európskej únii. Štandardné doložky o ochrane údajov nemôžu vzhľadom na svoju zmluvnú povahu zaväzovať orgány verejnej moci tretích krajín, keďže tieto nie sú zmluvnou stranou zmluvy. V dôsledku toho môžu vývozcovia údajov potrebovať doplniť záruky obsiahnuté v uvedených štandardných doložkách o ochrane údajov dodatočnými opatreniami na zabezpečenie súladu s úrovňou ochrany vyžadovanou podľa práva Únie v konkrétnej tretej krajine. Súdny dvor odkazuje na odôvodnenie 109 všeobecného nariadenia o ochrane údajov, v ktorom sa spomína táto možnosť a nabáda prevádzkovateľov a sprostredkovateľov, aby ju využívali.[4]

(5) Súdny dvor konštatoval, že prináleží predovšetkým vývozcovi údajov, aby v každom jednotlivom prípade a eventuálne v spolupráci s dovozcom údajov overil, či právo tretej krajiny určenia zaručuje primeranú ochranu osobných údajov prenášaných na základe štandardných doložiek o ochrane údajov z hľadiska práva Únie a v prípade potreby poskytol dodatočné záruky k zárukám poskytovaným týmito ustanoveniami.[5]

(6) Ak prevádzkovateľ alebo sprostredkovateľ usadený v Európskej únii nie je schopný prijať dostatočné doplňujúce opatrenia na zabezpečenie v podstate rovnocennej úrovne ochrany podľa práva Únie, prevádzkovateľ alebo sprostredkovateľ alebo subsidiárne príslušný dozorný orgán musí pozastaviť alebo ukončiť prenos osobných údajov do dotknutej tretej krajiny.[6]

(7) Vo všeobecnom nariadení o ochrane údajov ani v rozhodnutiach Súdneho dvora sa nevymedzujú ani nešpecifikujú „ďalšie záruky“ [additional safeguards], „ďalšie opatrenia“ [additional measures] alebo „dodatočné opatrenia“ [supplementary measures] k zárukám týkajúcim sa nástrojov na prenos uvedeným v článku 46 ods. 2 všeobecného nariadenia o ochrane údajov, ktoré môžu prevádzkovatelia a sprostredkovatelia prijať na zabezpečenie súladu s úrovňou ochrany požadovanej podľa práva EÚ v konkrétnej tretej krajine.

(8) EDPB sa z vlastnej iniciatívy rozhodol preskúmať túto otázku a poskytnúť prevádzkovateľom a sprostredkovateľom, ktorí konajú ako vývozcovia, odporúčania týkajúce sa postupu, ktorý môžu dodržiavať pri identifikácii a prijímaní dodatočných opatrení. Cieľom týchto odporúčaní je poskytnúť vývozcom metodiku na určenie toho, či a aké ďalšie opatrenia by bolo potrebné zaviesť v prípade ich prenosov. Hlavnou zodpovednosťou vývozcov je zabezpečiť, aby sa prenášaným údajom v tretej krajine poskytla úroveň ochrany, ktorá je v podstate rovnocenná úrovni zaručenej v rámci EHP. EDPB sa týmito odporúčaniami snaží podporovať konzistentné uplatňovanie všeobecného nariadenia o ochrane údajov a rozhodnutia Súdneho dvora v súlade s mandátom EDPB.[7]

PRIJAL TIETO ODPORÚČANIA:

[4] C-311/18 (Schrems II), body 132 a 133.
[5] C-311/18 (Schrems II), bod 134.
[6] C-311/18 (Schrems II), bod 135.
[7] Článok 70 ods. 1 písm. e) všeobecného nariadenia o ochrane údajov.

1 ZODPOVEDNOSŤ PRI PRENOSOCH ÚDAJOV

1. V primárnom práve EÚ sa právo na ochranu údajov považuje za základné právo.[8] Právu na ochranu údajov sa preto poskytuje vysoká úroveň ochrany a obmedzenia možno vykonať len vtedy, ak sú stanovené zákonom, rešpektujú podstatu práva, sú primerané, nevyhnutné a skutočne zodpovedajú cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných.[9] Právo na ochranu osobných údajov nie je absolútnym právom; musí sa posudzovať vo vzťahu k jeho funkcii v spoločnosti a musí byť vyvážené s ostatnými základnými právami, a to v súlade so zásadou proporcionality.[10]

2. Keď budú údaje zaslané do tretích krajín mimo EHP, musí im byť poskytnutá v podstate rovnocenná úroveň ochrany, akú majú zaručenú v rámci EÚ, aby sa zabezpečilo, že sa nenaruší úroveň ochrany zaručená všeobecným nariadením o ochrane údajov, a to počas prenosu, ani po ňom.

3. Právo na ochranu údajov má aktívnu povahu. Od vývozcov a dovozcov (či už sú prevádzkovateľmi a/alebo sprostredkovateľmi) vyžaduje viac ako len uznanie alebo pasívne dodržiavanie tohto práva.[11] Prevádzkovatelia a sprostredkovatelia sa musia snažiť aktívne a nepretržite dodržiavať právo na ochranu údajov prostredníctvom vykonávania právnych, technických a organizačných opatrení, ktorými sa zabezpečí jeho účinnosť. Prevádzkovatelia a sprostredkovatelia musia byť tiež schopní preukázať toto úsilie dotknutým osobám a dozorným orgánom pre ochranu údajov. Ide o tzv. zásadu zodpovednosti.[12]

4. Zásada zodpovednosti, ktorá je potrebná na zabezpečenie účinného uplatňovania úrovne ochrany stanovenej vo všeobecnom nariadení o ochrane údajov, sa uplatňuje aj na prenosy údajov do tretích krajín[13], keďže ako také predstavujú formu spracúvania údajov.[14] Ako Súdny dvor zdôraznil vo svojom rozsudku, úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v rámci Únie všeobecným nariadením o ochrane údajov v spojení s Chartou, musí byť zaručená bez ohľadu na ustanovenie tejto kapitoly, na základe ktorého sa uskutočňuje prenos osobných údajov do tretej krajiny.[15]

5. V rozsudku Schrems II Súdny dvor zdôrazňuje povinnosť vývozcov a dovozcov zabezpečiť, aby sa spracúvanie osobných údajov uskutočňovalo a naďalej bolo uskutočňované v súlade s úrovňou ochrany stanovenou v právnych predpisoch EÚ o ochrane údajov, a pozastaviť prenos a/alebo vypovedať zmluvu, ak dovozca údajov nie je alebo už nie je schopný dodržiavať štandardné

[8] Článok 8 ods. 1 Charty základných práv Európskej únie a článok 16 ods. 1 ZFEÚ, preambula 1, článok 1 ods. 2 všeobecného nariadenia o ochrane údajov.
[9] Článok 52 ods. 1 Charty základných práv Európskej únie.
[10] Odôvodnenie 4 všeobecného nariadenia o ochrane údajov a vec C-507/17 Google LLC/Commission nationale de l'informatique et des libertés (CNIL), bod 60.
[11] Spojené veci C-92/09 a C-93/02, Volker und Markus Schecke GbR/Land Hessen, návrhy, ktoré predniesla generálna advokátka Sharpston, 17. júna 2010, bod 71.
[12] Článok 5 ods. 2 a článok 28 ods. 3 písm. h) všeobecného nariadenia o ochrane údajov.
[13] Článok 44 a odôvodnenie 101 všeobecného nariadenia o ochrane údajov, ako aj článok 47 ods. 2 písm. d) všeobecného nariadenia o ochrane údajov.
[14] Rozsudok SDEÚ zo 6. októbra 2015, Maximillian Schrems/Data Protection Commissioner [ďalej len „C-362/14 (Schrems I)“], bod 45.
[15] C-311/18 (Schrems II), body 92 a 93.

doložky o ochrane údajov začlenené do príslušnej zmluvy medzi vývozcom a dovozcom.[16] Prevádzkovateľ alebo sprostredkovateľ konajúci ako vývozca musí zabezpečiť, aby dovozcovia v prípade potreby spolupracovali s vývozcom, pri plnení týchto povinností, a to tak, že ho budú informovať napríklad o akomkoľvek vývoji, ktorý má vplyv na úroveň ochrany osobných údajov prijatých v krajine dovozcu.[17] Tieto povinnosti predstavujú uplatňovanie zásady zodpovednosti na prenos údajov podľa všeobecného nariadenia o ochrane údajov.[18]

2 POSTUP: UPLATŇOVANIE ZÁSADY ZODPOVEDNOSTI NA PRENOSY ÚDAJOV V PRAXI

6. V ďalšom texte je uvedená postupnosť krokov, ktoré treba podniknúť s cieľom zistiť, či vy (ako vývozca údajov) potrebujete zaviesť dodatočné opatrenia, aby ste mohli legálne prenášať údaje mimo EHP. „Vy“ v tomto dokumente znamená prevádzkovateľ alebo sprostredkovateľ, ktorý koná ako vývozca údajov[19] a spracúva osobné údaje v rozsahu pôsobnosti všeobecného nariadenia o ochrane údajov – vrátane spracúvania súkromnými subjektmi a verejnoprávnymi subjektmi pri prenose údajov súkromným subjektom.[20] Pokiaľ ide o prenosy osobných údajov medzi verejnoprávnymi subjektmi, v *Usmerneniach 2/2020 k článku 46 ods. 2 písm. a) a článku 46 ods. 3 písm. b) nariadenia (EÚ) 2016/679 o prenose osobných údajov medzi orgánmi verejnej moci a verejnoprávnymi subjektmi v EHP a mimo EHP* sa poskytuje osobitné usmernenie.[21]

7. Toto posúdenie a dodatočné opatrenia, ktoré si zvolíte a budete vykonávať, budete musieť náležite zdokumentovať a takúto dokumentáciu na požiadanie sprístupniť príslušnému dozornému orgánu.[22]

2.1 Krok 1: Poznajte vlastné prenosy

8. Ak chcete vedieť, čo sa od vás (vývozcu údajov) môže vyžadovať, aby ste mohli pokračovať v prenose alebo vykonávať nové prenosy osobných údajov[23], prvým krokom je zabezpečiť, aby ste boli plne informovaní o vašich prenosoch (poznali vlastné prenosy). Zaznamenávanie a mapovanie všetkých prenosov môže byť zložitým úkonom pre subjekty zapojené do viacnásobných, rôznorodých a pravidelných prenosov do tretích krajín a využívajúce viacerých sprostredkovateľov

[16] C-311/18 (Schrems II), body 134, 135, 139, 140, 141, 142.
[17] C-311/18 (Schrems II), bod 134.
[18] Článok 5 ods. 2 a článok 28 ods. 3 písm. h) všeobecného nariadenia o ochrane údajov.
[19] Preto sa za vývozcu údajov nebudete považovať v prípade, ak ste dotknutou osobou, ktorá poskytuje svoje osobné údaje prevádzkovateľovi usadenému v tretej krajine prostredníctvom online dotazníka.
[20] Pozri Usmernenia EDPB 3/2018 o územnej pôsobnosti všeobecného nariadenia o ochrane údajov (článok 3) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en
[21] Usmernenia EDPB 2/2020 k článku 46 ods. 2 písm. a) a článku 46 ods. 3 písm. b) nariadenia (EÚ) 2016/679 o prenose osobných údajov medzi orgánmi verejnej moci a verejnoprávnymi subjektmi, v EHP a mimo EHP, pozri https://edpb.europa.eu/system/files/2021-05/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_sk.pdf
[22] Článok 5 ods. 2 všeobecného nariadenia o ochrane údajov a článok 24 ods. 1 všeobecného nariadenia o ochrane údajov.
[23] Upozorňujeme, že za prenos sa považuje aj vzdialený prístup subjektu z tretej krajiny k údajom nachádzajúcim sa v EHP.

a ďalších sprostredkovateľov [sub-processors]. Znalosť vlastných prenosov je nevyhnutným prvým krokom k splneniu vašich povinností v rámci zásady zodpovednosti.

9. Ak sa chcete mať úplnú znalosť o vlastných prenosoch, môžete vychádzať zo záznamov o spracovateľských činnostiach, ktoré ste možno povinní uchovávať ako prevádzkovateľ alebo sprostredkovateľ podľa článku 30 všeobecného nariadenia o ochrane údajov.[24] Pomôcť vám môžu aj predchádzajúce opatrenia na splnenie povinností informovať dotknuté osoby podľa článku 13 ods. 1 písm. f) a článku 14 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov o vašich prenosoch ich osobných údajov do tretích krajín.[25]

10. Pri mapovaní prenosov nezabudnite zohľadniť aj následné prenosy, napríklad či sprostredkovatelia mimo EHP prenášajú osobné údaje, ktoré ste im zverili, ďalšiemu sprostredkovateľovi v inej tretej krajine alebo v tej istej tretej krajine[26].

11. V súlade so zásadou „minimalizácie údajov“ podľa všeobecného nariadenia o ochrane údajov[27] musíte overiť, či sú údaje, ktoré prenášate, primerané, relevantné a obmedzené vo vzťahu k tomu, čo je nevyhnutné vzhľadom na účely, na ktoré sa tieto údaje spracúvajú.

12. Tieto činnosti sa musia vykonať pred realizáciou akéhokoľvek prenosu a aktualizovať pred obnovením prenosov po pozastavení operácií prenosu údajov: musíte vedieť, kde sa môžu nachádzať osobné údaje, ktoré ste vyviezli alebo kde ich vývozcovia môžu spracúvať (mapa miest určenia).

13. Pamätajte si, že za prenos sa považuje aj vzdialený prístup z tretej krajiny (napríklad v prípadoch poskytovania podpory) a/alebo ukladanie v cloude nachádzajúcom sa mimo EHP, ktoré ponúka poskytovateľ služby.[28] Pokiaľ používate konkrétne medzinárodnú cloudovú infraštruktúru, musíte posúdiť, či sa vaše údaje budú prenášať do tretích krajín a do ktorých, pokiaľ poskytovateľ cloudu

---

[24] Pozri článok 30 všeobecného nariadenia o ochrane údajov, a najmä odseky 1 písm. e) a 2 písm. c). Okrem toho by záznamy o spracúvaní mali obsahovať opis vašich spracovateľských činností (okrem iného vrátane kategórií dotknutých osôb, kategórií osobných údajov a účelov spracúvania a osobitných informácií o prenose údajov). Niektorí prevádzkovatelia a sprostredkovatelia sú oslobodení od povinnosti viesť záznamy o spracúvaní (článok 30 ods. 5 všeobecného nariadenia o ochrane údajov). Pokiaľ ide o usmernenie k tejto výnimke, pozri pozičný dokument pracovnej skupiny zriadenej podľa článku 29 o výnimkách z povinnosti viesť záznamy o spracovateľských činnostiach podľa článku 30 ods. 5 všeobecného nariadenia o ochrane údajov (schválený EDPB 25. mája 2018).

[25] Podľa pravidiel transparentnosti na základe všeobecného nariadenia o ochrane údajov musíte dotknuté osoby informovať o prenose osobných údajov do tretích krajín [článok 13 ods. 1 písm. f) a článok 14 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov]. Konkrétne ich musíte informovať o existencii alebo neexistencii rozhodnutia Európskej komisie o primeranosti, alebo v prípade prenosov uvedených v článkoch 46 alebo 47 všeobecného nariadenia o ochrane údajov alebo v článku 49 ods. 1 druhom pododseku všeobecného nariadenia o ochrane údajov musíte uviesť odkaz na primerané alebo vhodné záruky a prostriedky na získanie ich kópie alebo informácie o tom, kde boli poskytnuté. Informácie poskytované dotknutej osobe musia byť správne a aktuálne, najmä vzhľadom na judikatúru Súdneho dvora týkajúcu sa prenosov.

[26] Ak prevádzkovateľ udelil svoje predchádzajúce osobitné alebo všeobecné písomné povolenie v súlade s článkom 28 ods. 2 všeobecného nariadenia o ochrane údajov.

[27] Článok 5 ods. 1 písm. c) všeobecného nariadenia o ochrane údajov.

[28] Pozri otázku č. 11 „je potrebné mať na pamäti, že aj poskytnutie prístupu k údajom z tretej krajiny, napríklad na administratívne účely, predstavuje prenos“, v dokumente EDPB Často kladené otázky k rozsudku Súdneho dvora Európskej únie vo veci C-311/18 – Data Protection Commissioner/Facebook Ireland Ltd a Maximillian Schrems, 23. júla 2020.

so sídlom v EHP vo svojej zmluve jasne neuvádza, že údaje sa v tretích krajinách vôbec nespracúvajú.

2.2 Krok 2: Identifikácia nástrojov na prenos, ktoré využívate

14. Druhým krokom, ktorý musíte podniknúť, je identifikovať nástroje na prenos, ktoré využívate spomedzi nástrojov, ktoré sa uvádzajú a o ktorých sa uvažuje v kapitole V všeobecného nariadenia o ochrane údajov.

Rozhodnutia o primeranosti

15. Európska komisia môže prostredníctvom svojich **rozhodnutí o primeranosti** týkajúcich sa niektorých alebo všetkých tretích krajín, do ktorých prenášate osobné údaje, uznať, že poskytujú primeranú úroveň ochrany osobných údajov.[29]

16. Dôsledkom takéhoto rozhodnutia o primeranosti je, že osobné údaje môžu byť prenášané z EHP do danej tretej krajiny bez toho, aby bol potrebný akýkoľvek nástroj na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov.

17. Rozhodnutia o primeranosti sa môžu vzťahovať na krajinu ako celok alebo sa môžu obmedziť na jej časť. Rozhodnutia o primeranosti sa môžu vzťahovať na všetky prenosy údajov do krajiny alebo sa môžu obmedziť na niektoré typy prenosov (napr. do jedného sektoru).[30]

18. Európska komisia uverejňuje zoznam svojich rozhodnutí o primeranosti na svojej webovej stránke.[31]

19. Ak prenášate osobné údaje do tretích krajín, regiónov alebo sektorov, na ktoré sa vzťahuje rozhodnutie Komisie o primeranosti (v príslušnom rozsahu), nemusíte podniknúť žiadne **ďalšie kroky opísané v týchto odporúčaniach.**[32] Stále však musíte monitorovať, či rozhodnutia o primeranosti týkajúce sa prenosov neboli zrušené alebo vyhlásené za neplatné.[33]

20. Rozhodnutia o primeranosti však nebránia dotknutým osobám podať sťažnosť. Nebránia ani dozorným orgánom, aby sa obrátili na vnútroštátny súd, ak majú pochybnosti o platnosti

[29] Európska komisia má právomoc na základe článku 45 všeobecného nariadenia o ochrane údajov určiť, či krajina mimo EÚ ponúka primeranú úroveň ochrany údajov. Podobne má Európska komisia právomoc určiť, či primeranú úroveň ochrany poskytuje medzinárodná organizácia.
[30] Článok 45 ods. 1 všeobecného nariadenia o ochrane údajov.
[31] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[32] Za predpokladu, že vy a dovozca údajov ste vykonali opatrenia na splnenie ostatných povinností podľa všeobecného nariadenia o ochrane údajov; v opačnom prípade tieto opatrenia vykonajte.
[33] Európska komisia musí pravidelne preskúmavať všetky rozhodnutia o primeranosti a monitorovať, či tretie krajiny, ktoré využívajú rozhodnutia o primeranosti, naďalej zabezpečujú primeranú úroveň ochrany (pozri článok 45 ods. 3 a článok 45 ods. 4 všeobecného nariadenia o ochrane údajov). Súdny dvor môže tiež zrušiť platnosť rozhodnutí o primeranosti [pozri jeho rozsudky vo veciach C-362/14 (Schrems I) a C-311/18 (Schrems II)].

rozhodnutia, takže vnútroštátny súd môže podať návrh na začatie prejudiciálneho konania na SDEÚ na účely preskúmania tejto platnosti.[34]

Príklad:

Občan EÚ, pán Schrems, podal v júni 2013 sťažnosť írskemu dozornému orgánu (Irish Data Protection Commission, ďalej aj „DPC“) a požiadal tento dozorný orgán, aby zakázal alebo pozastavil prenos jeho osobných údajov zo spoločnosti Facebook Ireland do Spojených štátov amerických, keďže sa domnieval, že právne predpisy a postupy Spojených štátov nezabezpečujú primeranú ochranu osobných údajov uchovávaných na ich území pred činnosťami sledovania, ktoré tam vykonávajú orgány verejnej moci. DPC sťažnosť zamietla najmä z dôvodu, že Európska komisia vo svojom rozhodnutí 2000/520 usúdila, že v rámci systému „Safe Harbour“ Spojené štáty zabezpečujú primeranú úroveň ochrany prenášaných osobných údajov (rozhodnutie o Safe Harbour). Pán Schrems napadol rozhodnutie DPC a írsky High Court položil Súdnemu dvoru Európskej únie (SDEÚ) otázku týkajúcu sa platnosti rozhodnutia 2000/520. SDEÚ následne rozhodol o zrušení rozhodnutia Komisie 2000/520 o primeranosti ochrany poskytovanej zásadami Safe Harbour.[35]

Nástroje na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov

21. V článku 46 všeobecného nariadenia o ochrane údajov sa uvádza súbor nástrojov na prenos údajov, ktoré poskytujú *„primerané záruky“* a ktoré vývozcovia môžu použiť na prenos osobných údajov do tretích krajín, ak neexistujú rozhodnutia o primeranosti. Hlavnými typmi nástrojov na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov sú:

- štandardné doložky o ochrane údajov,
- záväzné vnútropodnikové pravidlá,
- kódexy správania,
- certifikačné mechanizmy,
- zmluvné doložky ad hoc.

22. Bez ohľadu na to, aký nástroj si na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov zvolíte, musíte zabezpečiť, aby prenášané osobné údaje vo všeobecnosti požívali v podstate rovnocennú úroveň ochrany.

23. Nástroje na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov obsahujú najmä primerané záruky zmluvnej povahy, ktoré sa môžu uplatňovať na prenosy do všetkých tretích

[34] C-311/18 (Schrems II), body 118 – 120. Dozorné orgány nesmú ignorovať rozhodnutie o primeranosti a pozastaviť alebo zakázať prenosy osobných údajov do takýchto krajín len na základe neprimeranosti úrovne ochrany. Svoju právomoc pozastaviť alebo zakázať prenos osobných údajov do tejto tretej krajiny môžu uplatniť len z iných dôvodov (napr. nedostatočné bezpečnostné opatrenia v rozpore s článkom 32 všeobecného nariadenia o ochrane údajov, spracúvanie údajov nie je založené na žiadnom platnom právnom základe a ako také je v rozpore s článkom 6 všeobecného nariadenia o ochrane údajov). Dozorné orgány môžu úplne nezávisle preskúmať, či je prenos týchto údajov v súlade s požiadavkami stanovenými vo všeobecnom nariadení o ochrane údajov, a v prípade potreby podať na vnútroštátne súdy žalobu, aby tieto v prípade, že majú pochybnosti o platnosti rozhodnutia Komisie o primeranosti, podali návrh na začatie prejudiciálneho konania na Súdny dvor Európskej únie na účely preskúmania jeho platnosti.

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

krajín. Situácia v tretej krajine, do ktorej prenášate údaje, si môže stále vyžadovať, aby ste doplnili tieto nástroje na prenos a záruky, ktoré obsahujú, ďalšími opatreniami („dodatočné opatrenia“) s cieľom zabezpečiť v podstate rovnocennú úroveň ochrany.[36]

Výnimky

24. Okrem rozhodnutí o primeranosti a nástrojov na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov obsahuje všeobecné nariadenie o ochrane údajov tretiu možnosť, ktorá umožňuje prenos osobných údajov v určitých situáciách. Za osobitných podmienok môžete preniesť osobné údaje na základe výnimky uvedenej v článku 49 všeobecného nariadenia o ochrane údajov.

25. Článok 49 všeobecného nariadenia o ochrane údajov má výnimočnú povahu. Výnimky, ktoré obsahuje, sa musia vykladať spôsobom, ktorý nie je v rozpore so samotnou povahou výnimiek, ktoré sú odchýlkami z pravidla, že osobné údaje nemožno prenášať do tretej krajiny, pokiaľ táto krajina nezabezpečuje primeranú úroveň ochrany údajov alebo sa alternatívne nezavedú primerané záruky. Výnimky sa v praxi nemôžu stať „pravidlom“, ale musia byť obmedzené na konkrétne situácie. EDPB vydal Usmernenia č. 2/2018 o výnimkách podľa článku 49 nariadenia (EÚ) 2016/679.[37]

26. Pred odvolaním sa na výnimku podľa článku 49 všeobecného nariadenia o ochrane údajov musíte skontrolovať, či prenos spĺňa prísne podmienky stanovené v tomto ustanovení pre každú z nich.

***

27. Ak váš prenos nemôže byť právne založený na rozhodnutí o primeranosti, ani na výnimke podľa článku 49, musíte pokračovať v kroku 3.

2.3 3. krok: Posúdenie účinnosti využívaného nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov vzhľadom na všetky okolnosti prenosu

28. Vybraný nástroj na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov musí účinne zabezpečiť, aby prenos v praxi nenarušil úroveň ochrany zaručenú všeobecným nariadením o ochrane údajov.[38]

29. Predovšetkým ochrana poskytovaná preneseným osobným údajom v tretej krajine musí byť v podstate rovnocenná s ochranou, ktorú v EHP zaručuje všeobecné nariadenie o ochrane údajov v zmysle Charty základných práv EÚ.[39] To neplatí v prípade, ak si dovozca údajov nemôže splniť svoje povinnosti vyplývajúce z vybraného nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov z dôvodu, že mu v tom bránia právne predpisy a postupy tretej krajiny, ktoré sa vzťahujú na prenos, a to aj počas prenosu údajov od vývozcu do krajiny dovozcu[40].

---

[36] C-311/18 (Schrems II), body 130 a 133. Pozri tiež časť 2.3 ďalej.
[37] Viac informácií k tejto téme nájdete na adrese https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_sk_0.pdf.
[38] Článok 44 všeobecného nariadenia o ochrane údajov a body 126, 137 a 148 rozsudku C-311/18 (Schrems II).
[39] C-311/18 (Schrems II), bod 105 a druhý bod výroku.
[40] Pozri bod 183 rozsudku C-311/18 (Schrems II) v spojení v bodom 184.

30. V prvom rade musíte posúdiť, v prípade potreby aj v spolupráci s dovozcom, či platné právne predpisy a/alebo postupy[41] tretej krajiny môžu obsahovať niečo, čo by v súvislosti s konkrétnym prenosom mohlo ovplyvniť účinnosť primeraných záruk nástrojov na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov, ktoré využívate. To znamená určiť, či váš prenos patrí do pôsobnosti právnych predpisov a/alebo postupov, ktoré môžu mať vplyv na účinnosť vášho nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov. Vyžadované posúdenie musí vychádzať predovšetkým z právnych predpisov, ktoré sú verejne dostupné.

31. Toto posúdenie musí obsahovať skutočnosti týkajúce sa prístupu orgánov verejnej moci tretej krajiny vášho dovozcu k údajom, ako napríklad:

    - Skutočnosti o tom, či orgány verejnej moci tretej krajiny vášho dovozcu môžu požadovať prístup k údajom s vedomím alebo bez vedomia dovozcu údajov vzhľadom na právne predpisy, prax a zaznamenané prípady;
    - Skutočnosti o tom, či orgány verejnej moci tretej krajiny vášho dovozcu môžu mať prístup k údajom prostredníctvom dovozcu údajov alebo prostredníctvom telekomunikačných poskytovateľov alebo komunikačných kanálov vzhľadom na právne predpisy, zákonné právomoci, technické, finančné a ľudské zdroje, ktoré majú k dispozícii, a zaznamenané prípady.

Identifikácia relevantných právnych predpisov a postupov vzhľadom na všetky okolnosti prenosu

32. Budete musieť preskúmať charakteristické znaky každého z vašich prenosov a určiť, či vaše prenosy ovplyvňuje vnútroštátny právny poriadok a/alebo postupy krajiny, do ktorej sa údaje prenášajú (alebo sa následne prenášajú). Rozsah vášho posúdenia je teda obmedzený na právne predpisy a postupy týkajúce sa ochrany konkrétnych údajov, ktoré prenášate, na rozdiel od všeobecných a rozsiahlych hodnotení primeranosti, ktoré vykonáva Európska komisia v súlade s článkom 45 všeobecného nariadenia o ochrane údajov.

33. Uplatniteľný právny rámec a/alebo postupy budú závisieť od konkrétnych okolností vášho prenosu, najmä od:

    - účelu, na ktoré sa údaje prenášajú a spracúvajú (napr. marketing, ľudské zdroje, uchovávanie, podpora IT, klinické skúšanie),
    - typu subjektov zapojených do spracúvania údajov (verejné/súkromné; prevádzkovatelia/sprostredkovatelia),
    - sektoru, v ktorom dochádza k prenosu (napr. reklamné technológie, telekomunikácie, finančníctvo atď.),
    - kategórie prenášaných osobných údajov (napr. osobné údaje týkajúce sa detí môžu patriť do rozsahu pôsobnosti osobitných právnych predpisov v tretej krajine),[42]

[41] Pozri bod 126 rozsudku C-311/18 (Schrems II), v ktorom sa Súdny dvor výslovne odvoláva na „právny stav a prax uplatňovanú v dotknutej tretej krajine“ a požaduje „(...) v praxi zabezpečiť účinnú ochranu osobných údajov prenášaných do dotknutej tretej krajiny.“ (doplnené zvýraznenie) a bod 158.

[42] Prenos osobných údajov je spracovateľskou operáciou (článok 4 bod 2 všeobecného nariadenia o ochrane údajov). Ak máte v úmysle prenášať citlivé údaje spadajúce do článkov 9 a 10 všeobecného nariadenia o ochrane údajov, môžete prenos uskutočniť iba ak spadá pod niektorú z výnimiek a podmienok ustanovených v článkoch

- či sa údaje budú uchovávať v tretej krajine alebo či dochádza k vzdialenému prístupu k údajom uchovávaným v rámci EÚ/EHP,
- formát údajov, ktoré sa majú preniesť (t. j. obyčajný text/pseudonymizované alebo zašifrované[43]),
- možnosť, že údaje môžu byť predmetom následného prenosu z tretej krajiny do ďalšej tretej krajiny.[44]

34. V posúdení by sa mali zohľadniť všetky subjekty zapojené do prenosu (napr. prevádzkovatelia, sprostredkovatelia a ďalší sprostredkovatelia spracúvajúci údaje v tretej krajine), ktoré boli identifikované pri mapovaní prenosov. Čím viac prevádzkovateľov, sprostredkovateľov alebo dovozcov je zapojených, tým zložitejšie bude vaše posúdenie. Pri tomto posúdení budete musieť zohľadniť aj každý predpokladaný následný prenos.

35. V každom prípade by ste mali venovať osobitnú pozornosť všetkým príslušným právnym predpisom, najmä právnym predpisom, ktorými sa stanovujú požiadavky na poskytnutie osobných údajov orgánom verejnej moci alebo ktorými sa týmto orgánom verejnej moci udeľujú právomoci na prístup k osobným údajom (napríklad na účely presadzovania práva v trestných veciach, regulačného dohľadu a národnej bezpečnosti). Pokiaľ tieto požiadavky alebo právomoci obmedzujú základné práva dotknutých osôb, pričom rešpektujú ich podstatu a sú nevyhnutnými a primeranými opatreniami v demokratickej spoločnosti na ochranu významných cieľov, ktoré sú uznané aj v práve Únie alebo členských štátov EÚ,[45] nesmú zasahovať do povinností obsiahnutých v nástroji na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov, ktorý využívate.

36. Budete musieť posúdiť príslušné pravidlá a postupy všeobecnej povahy, pokiaľ majú vplyv na účinné uplatňovanie záruk obsiahnutých v nástroji na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov.

37. Pri vykonávaní tohto posúdenia sú relevantné aj rôzne aspekty právneho systému danej tretej krajiny, napr. prvky uvedené v článku 45 ods. 2 všeobecného nariadenia o ochrane údajov. Napríklad situácia v oblasti právneho štátu v tretej krajine môže byť relevantná pri posudzovaní účinnosti dostupných mechanizmov, ktoré majú jednotlivci k dispozícii na dosiahnutie (súdneho) prostriedku nápravy v prípade nezákonného prístupu vlády k osobným údajom. Existencia komplexného zákona o ochrane údajov alebo nezávislého orgánu pre ochranu údajov, ako aj

---

9 a 10 všeobecného nariadenia o ochrane údajov a v práve členského štátu EÚ. V súlade s článkom 32 všeobecného nariadenia o ochrane údajov budete musieť tiež zaviesť, pričom dovozca vystupuje ako prevádzkovateľ alebo sprostredkovateľ, primerané technické a organizačné opatrenia na zabezpečenie úrovne bezpečnosti primeranej rizikám pre práva a slobody dotknutých osôb, ktoré predstavujú potenciálne porušenie ochrany prenášaných údajov (článok 4 bod 12 všeobecného nariadenia o ochrane údajov). Kategórie prenášaných údajov a ich citlivosť budú relevantné pre posúdenie rizika a primeranosti opatrení.

[43] Niektoré tretie krajiny nepovoľujú dovoz šifrovaných údajov.

[44] Ak prevádzkovateľ udelil svoje predchádzajúce osobitné alebo všeobecné písomné povolenie v súlade s článkom 28 ods. 2 všeobecného nariadenia o ochrane údajov.

[45] Pozri články 47 a 52 Charty základných práv EÚ, článok 23 ods. 1 všeobecného nariadenia o ochrane údajov a odporúčania EDPB 02/2020 o európskych základných zárukách pre opatrenia týkajúce sa sledovania z 10. novembra 2020, https://edpb.europa.eu/system/files/2021-04/edpb_recommendations_202002_europeanessentialguaranteessurveillance_sk.pdf.

dodržiavanie medzinárodných nástrojov zabezpečujúcich záruky ochrany údajov môžu prispieť k zabezpečeniu proporcionality zasahovania zo strany vlády.

38. Povinnosti alebo právomoci vyplývajúce z takýchto právnych predpisov a postupov sa považujú za zasahujúce do požiadaviek alebo za nezlučiteľné s požiadavkami nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov,[46] pokiaľ:

- sú v rozpore s podstatou základných práv a slobôd Charty základných práv EÚ, alebo
- prekračujú rámec toho, čo je v demokratickej spoločnosti nevyhnutné a primerané na ochranu niektorého z významných cieľov, ktoré sú uznané aj v práve Únie alebo členského štátu, ako sú ciele, ktoré sú uvedené v článku 23 ods. 1 všeobecného nariadenia o ochrane údajov.

39. Mali by ste overiť, či sa povinnosti dovozcu údajov, ktoré umožňujú dotknutým osobám uplatňovať ich práva uvedené v nástroji na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov [ako sú žiadosti o prístup, opravu a vymazanie prenesených údajov, ako aj (súdny) prostriedok nápravy], môžu účinne uplatňovať v praxi a či tomu nebránia právne predpisy a/alebo postupy v tretej krajine určenia.

40. Normy EÚ, akými sú články 47 a 52 Charty základných práv EÚ, sa musia použiť ako východisko predovšetkým na posúdenie toho, či sa prístup orgánov verejnej moci obmedzuje na to, čo je v demokratickej spoločnosti nevyhnutné a primerané a či sa dotknutým osobám poskytujú účinné prostriedky nápravy.

41. Odporúčania EDPB o európskych základných zárukách[47] poskytujú vysvetlenia ku skutočnostiam, ktoré treba posúdiť pri určovaní toho, či právny rámec upravujúci prístup orgánov verejnej moci k osobným údajom v tretej krajine, či už ide o národné bezpečnostné agentúry alebo orgány presadzovania práva, možno alebo nemožno považovať za odôvodnený zásah.[48] Mali by sa starostlivo zvážiť najmä vtedy, keď sú právne predpisy upravujúce prístup orgánov verejnej moci k údajom nejednoznačné alebo nie sú verejne dostupné. Prvou požiadavkou európskych základných záruk je, že pokiaľ sa tento prístup predpokladá, mal by existovať právny rámec stanovujúci taký prístup, ktorý je verejne dostupný a dostatočne jasný.

42. V prípade situácie prenosu údajov na základe nástrojov na prenos podľa článku 46 môžu odporúčania EDPB o európskych základných zárukách usmerniť vývozcu údajov pri posudzovaní toho, či také právomoci neoprávnene zasahujú do povinností dovozcu a vývozcu údajov zaručiť v podstate rovnocennosť podľa všeobecného nariadenia o ochrane údajov alebo povinnosti obsiahnuté v nástroji na prenos. Neexistencia v podstate rovnocennej úrovne ochrany bude zrejmá najmä vtedy, keď právne predpisy alebo postupy tretej krajiny týkajúce sa vášho prenosu nespĺňajú požiadavky európskych základných záruk. EDPB opätovne uvádza, že európske základné záruky sú referenčným štandardom pri posudzovaní zásahov spôsobených opatreniami týkajúcimi

---

[46] Pozri články 47 a 52 Charty základných práv Európskej únie, článok 23 ods. 1 všeobecného nariadenia o ochrane údajov, rozsudok C-311/18 (Schrems II), body 174 a 187, a odporúčania EDPB 02/2020 o európskych základných zárukách pre opatrenia týkajúce sa sledovania z 10. novembra 2020.

[47] Odporúčania EDPB 02/2020 o európskych základných zárukách pre opatrenia týkajúce sa sledovania z 10. novembra 2020.

[48] A teda za nezasahujúci do povinností prijatých v rámci nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov.

sa sledovania tretích krajín v kontexte medzinárodných prenosov údajov. Tieto štandardy vyplývajú z práva EÚ a judikatúry SD EÚ a Európskeho súdu pre ľudské práva, ktorá je pre členské štáty EÚ záväzná.

43. Posúdenie musí vychádzať predovšetkým z právnych predpisov, ktoré sú verejne dostupné. Preskúmanie postupov orgánov verejnej moci tretích krajín vám umožní overiť, či môžu byť záruky obsiahnuté v nástroji na prenos údajov podľa článku 46 všeobecného nariadenia o ochrane údajov dostatočným prostriedkom na zabezpečenie účinnej ochrany prenášaných osobných údajov v praxi.[49] Preskúmanie postupov platných v tretej krajine je významné najmä pre vaše posúdenie v situáciách opísaných nižšie.

43.1 **Príslušné právne predpisy v tretej krajine môžu formálne spĺňať normy EÚ týkajúce sa základných práv a slobôd a nevyhnutnosť a primeranosť ich obmedzení.** Prax orgánov verejnej moci tretej krajiny (napr. prístup k osobným údajom, ktorými disponuje súkromný sektor, alebo pri uplatňovaní - či neuplatňovaní - právnych predpisov dozornými alebo súdnymi orgánmi) však môže jasne naznačovať, že bežne neuplatňujú/nedodržiavajú právne predpisy, ktorými sa v zásade riadia ich činnosti. V takom prípade musíte pri svojom posúdení vziať do úvahy tieto postupy a zohľadniť, že nástroj podľa článku 46 všeobecného nariadenia o ochrane údajov nebude schopný sám o sebe (t. j. bez dodatočných opatrení) účinne zaručiť v podstate rovnocennú úroveň ochrany. Ak chcete v takom prípade pokračovať v prenose, budete musieť prijať vhodné dodatočné opatrenia.

43.2 **Príslušné právne predpisy (napr. o prístupe k osobným údajom, ktorými disponuje súkromný sektor) môžu v tretej krajine chýbať.** V tomto prípade nemôžete z tejto neexistencie príslušných právnych predpisov automaticky vyvodiť, že váš nástroj na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov možno efektívne uplatniť. Budete musieť skontrolovať, či existujú indície o platných postupoch v krajine, ktoré nie sú v súlade s právom EÚ a požiadavkami nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov. Ak v krajine existujú nezlučiteľné postupy, nástroj na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov nebude schopný sám o sebe (t. j. bez vhodných dodatočných opatrení) účinne zaručiť v podstate rovnocennú úroveň ochrany. Ak chcete v takom prípade pokračovať v prenose, budete musieť prijať vhodné dodatočné opatrenia.

43.3 **Posúdenie môže preukázať, že príslušné právne predpisy v tretej krajine môžu byť problematické[50]a že prenášané údaje a/alebo dotknutý dovozca patria alebo by mohli patriť do pôsobnosti týchto problematických právnych predpisov[51].**

---

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

[50] „Problematickými právnymi predpismi“ sa rozumejú právne predpisy, ktoré 1) príjemcovi osobných údajov z Európskej únie ukladajú povinnosti a/alebo môžu ovplyvniť prenášané údaje spôsobom, ktorý môže zasahovať do zmluvnej záruky nástrojov na prenos, ktorou je v podstate rovnocenná úroveň ochrany a 2) sú v rozpore s podstatou základných práv a slobôd uznaných Chartou základných práv EÚ alebo prekračujú rámec toho, čo je v demokratickej spoločnosti nevyhnutné a primerané na ochranu niektorého z významných cieľov, ktoré uznáva aj právo Únie alebo členských štátov EÚ, akými sú ciele, ktoré sú uvedené v článku 23 ods. 1 všeobecného nariadenia o ochrane údajov.

[51] Môže byť nejasné, či dovozca a/alebo prenášané údaje patria do rozsahu všeobecných pojmov, ktoré sa často používajú v právnych predpisoch o národnej bezpečnosti na obmedzenie rozsahu ich pôsobnosti, ako napríklad „poskytovateľ elektronických komunikačných služieb“ a „zahraničné spravodajské informácie“.

Vzhľadom na neistoty týkajúce sa potenciálneho uplatnenia problematických právnych predpisov na váš prenos sa môžete rozhodnúť:

- pozastaviť prenos;
- prijať dodatočné opatrenia[52], aby ste predišli riziku, že sa na vášho dovozcu a/alebo na vaše prenesené údaje potenciálne uplatnia právne predpisy a/alebo prax tretej krajiny dovozcu údajov, ktoré môžu zasahovať do zmluvných záruk nástroja na prenos, ktorými je v podstate rovnocenná úroveň ochrany, aká je zaručená v EHP; alebo
- sa môžete alternatívne rozhodnúť pokračovať v prenose bez toho, aby ste museli prijať dodatočné opatrenia, ak usúdite, že nemáte dôvod domnievať sa, že na vaše prenášané údaje a/alebo dovozcu sa v praxi budú uplatňovať príslušné a problematické právne predpisy. Na základe svojho posúdenia a v prípade potreby v spolupráci s dovozcom budete musieť preukázať a zdokumentovať, že právne predpisy sa v praxi nevykladajú a/alebo neuplatňujú tak, že by sa vzťahovali na vaše prenášané údaje a dovozcu, a to aj s prihliadnutím na skúsenosti ďalších subjektov pôsobiacich v rovnakom odvetví a/alebo týkajúce sa podobných prenesených osobných údajov a ďalšie zdroje informácií opísané ďalej.[53]

  Budete preto musieť preukázať a zdokumentovať v podrobnej správe,[54] že problematické právne predpisy sa v praxi na vaše prenášané údaje a/alebo dovozcu neuplatnia, a v dôsledku toho nebudú brániť dovozcovi v plnení jeho povinností podľa nástroja na prenos v článku 46 všeobecného nariadenia o ochrane údajov.[55]

Možné zdroje informácií

44. Váš dovozca údajov by vám mal poskytnúť relevantné zdroje a informácie týkajúce sa tretej krajiny, v ktorej má sídlo, ako aj právne predpisy a postupy, ktoré sa na prenos vzťahujú.

45. Vy a váš dovozca môžete doplniť svoje posúdenie informáciami získanými zo zdrojov, akými sú zdroje uvedené ako príklady v prílohe 3.

46. Okrem právneho rámca tretej krajiny, ktorý sa vzťahuje na prenos, by zdroje a informácie mali byť relevantné, objektívne, spoľahlivé, overiteľné a verejne dostupné alebo inak prístupné, aby bolo

[52] Pozri odôvodnenie 109 všeobecného nariadenia o ochrane údajov a rozsudok C-311/18 (Schrems II), bod 132.
[53] Pozri body 45 až 47.
[54] Správy, ktoré vypracujete, budú musieť obsahovať komplexné informácie o právnom posúdení právnych predpisov a postupov a ich uplatňovaní na konkrétne prenosy, interný postup vypracovania posúdenia (vrátane informácií o subjektoch zapojených do posudzovania – napr. právnické firmy, poradcovia alebo interné oddelenia) a dátumy kontrol. Správy by mal schváliť právny zástupca vývozcu.
[55] Preukázanie, že problematické právne predpisy sa v praxi na vaše prenášané údaje a dovozcu neuplatnia, a to aj s prihliadnutím na skúsenosti ďalších subjektov pôsobiacich v rovnakom odvetví a/alebo týkajúce sa podobných prenášaných osobných údajov, vás neoslobodzuje od povinnosti stanoviť nevyhnuté dodatočné opatrenia na ochranu osobných údajov počas ich poskytnutia a spracúvania v tretej krajine určenia (napr. end-to-end šifrovanie údajov – pozri príklady technických dodatočných opatrení v prílohe 2), pokiaľ vaša analýza platných právnych predpisov tretej krajiny určenia naznačuje, že k prístupu k údajom môže dôjsť aj v tomto okamihu prenosu, a to aj bez zásahu dovozcu. Také opatrenia ste už mohli predvídať, keď dovozca konal ako prevádzkovateľ alebo sprostredkovateľ v súlade s článkom 32 všeobecného nariadenia o ochrane údajov.

možné určiť, či váš nástroj na prenos podľa článku 46 možno účinne uplatniť[56] a vy budete musieť posúdiť a zdokumentovať, že sú.

Relevantné: informácie musia byť relevantné, pokiaľ ide o konkrétny prenos a/alebo dovozcu a ich súlad s požiadavkami stanovenými v práve EÚ a nástroji na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov, a nie príliš všeobecné alebo abstraktné.

Objektívne informácie: sú informácie, ktoré sú podložené empirickými dôkazmi na základe poznatkov získaných z minulosti, nie predpokladmi o potenciálnych udalostiach a rizikách.

Spoľahlivé: vývozca a dovozca musia objektívne posúdiť spoľahlivosť zdroja informácií a samotných informácií a vyhodnotiť ich oddelene.

Overiteľné: informácie a závery by mali byť overiteľné alebo porovnateľné s inými typmi informácií alebo zdrojov, ako súčasť celkového hodnotenia, aby aj príslušný dozorný orgán alebo súdny orgán mohol v prípade potreby skontrolovať objektivitu a spoľahlivosť týchto informácií.

Verejne dostupné alebo inak dostupné informácie: informácie by mali byť pokiaľ možno verejné alebo aspoň dostupné, aby sa uľahčilo overenie vyššie uvedených kritérií a aby sa zabezpečilo ich možné spoločné využívanie dozornými orgánmi, súdnymi orgánmi a v konečnom dôsledku dotknutými osobami.

47. Môžete tiež vziať do úvahy zdokumentované praktické skúsenosti dovozcu s príslušnými predchádzajúcimi prípadmi žiadostí o prístup [requests for access], ktoré dostali od orgánov verejnej moci v tretej krajine. Skúsenosti dovozcu ako dodatočný zdroj informácií budete môcť využiť len vtedy, pokiaľ právny rámec tretej krajiny nezakazuje dovozcovi poskytovať informácie o žiadostiach orgánov verejnej moci o poskytnutie údajov [request for disclosure] alebo o neexistencii takých žiadostí (a také posúdenie by ste mali aj zdokumentovať). Musíte si však uvedomiť, že neexistujúce predchádzajúce prípady žiadostí, ktoré by boli doručené dovozcovi, nemožno nikdy považovať samé osebe za rozhodujúci faktor účinnosti nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov, ktorý umožňuje, aby prenos pokračoval bez dodatočných opatrení. Tieto informácie budete môcť spolu s ďalšími typmi informácií získanými z iných zdrojov považovať za súčasť vášho celkového posúdenia právnych predpisov a postupov tretej krajiny vo vzťahu k vášmu prenosu. Relevantné a zdokumentované skúsenosti dovozcu by mali byť potvrdené a nemali by byť v rozpore s relevantnými, objektívnymi, spoľahlivými, overiteľnými a verejne dostupnými alebo inak prístupnými informáciami o praktickom uplatňovaní príslušných právnych predpisov (napr. existujúce alebo neexistujúce žiadosti o prístup doručené iným subjektom pôsobiacim v rovnakom odvetví a/alebo týkajúce sa podobných prenášaných osobných údajov[57] a/alebo uplatňovanie právnych predpisov v praxi, ako je judikatúra a správy nezávislých orgánov dohľadu).

[56] Pozri prílohu 3, pokiaľ ide o orientačný zoznam zdrojov informácií, ktoré môžete vy a dovozca použiť.

[57] Skúsenosti môžu byť skúsenosťami iných subjektov, ktoré priamo poznáte z dôvodu predchádzajúcich prenosov rovnakého druhu, ktoré ste uskutočnili, alebo ktoré sú uvedené v relevantnej judikatúre, správach mimovládnych organizácií atď. (pozri prílohu 3).

Výsledok vášho posúdenia

48. Toto celkové posúdenie právnych predpisov a postupov tretej krajiny vášho dovozcu, ktoré sa vzťahujú na váš prenos, by ste mali vykonať s náležitou starostlivosťou a dôkladne ho zdokumentovať. Vaše príslušné dozorné a/alebo súdne orgány to môžu vyžadovať a brať vás na zodpovednosť za akékoľvek rozhodnutie, ktoré na základe toho prijmete.[58]

49. Z posúdenia môže napokon vyplynúť, že nástroj na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov, ktorý využívate:

    - účinne zabezpečuje, že sa prenášaným osobným údajom v tretej krajine poskytuje úroveň ochrany, ktorá je v podstate rovnocenná úrovni zaručenej v EHP. Právne predpisy a postupy tretej krajiny, ktoré sa vzťahujú na prenos, umožňujú dovozcovi údajov splniť si svoje povinnosti podľa vybraného nástroja na prenos. V primeraných intervaloch alebo v prípade, že sa objavia významné zmeny, je potrebné prehodnotenie (pozri krok 6).

    - účinne nezabezpečuje v podstate rovnocennú úroveň ochrany. Dovozca údajov nemôže splniť svoje povinnosti v dôsledku právnych predpisov a/alebo postupov tretej krajiny, ktoré sa vzťahujú na prenos a ktoré nespĺňajú normy EÚ týkajúce sa základných práv a slobôd a nevyhnutnosť a primeranosť ich obmedzení na ochranu legitímnych cieľov verejného záujmu. SDEÚ zdôraznil, že ak nástroje na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov nie sú dostatočné, vývozca údajov je zodpovedný buď za zavedenie účinných dodatočných opatrení alebo za neuskutočnenie prenosu osobných údajov.[59]

Príklad:

Okolnosti:
SDEÚ rozhodol, že článok 702 amerického zákona FISA nerešpektuje minimálne záruky vyplývajúce zo zásady proporcionality podľa práva EÚ a nemožno ho považovať za obmedzený na to, čo je nevyhnutne potrebné. To znamená, že úroveň ochrany v rámci programov povolených na základe článku 702 FISA nie je v podstate rovnocenná zárukám požadovaným podľa práva EÚ.

Posúdenie:
Ak sa na základe posúdenia príslušnej legislatívy USA domnievate, že váš prenos by mohol spadať do pôsobnosti článku 702 FISA, ale nie ste si istý, či spadá do jeho praktického rozsahu pôsobnosti, môžete sa rozhodnúť:

1. zastaviť prenos;
2. prijať vhodné dodatočné opatrenia, ktoré účinne zabezpečia, že úroveň ochrany prenášaných údajov bude v podstate rovnocenná s úrovňou zaručenou v EHP; alebo
3. vyhľadať ďalšie objektívne, spoľahlivé, relevantné, overiteľné a pokiaľ možno verejne dostupné informácie (ktoré môžu zahŕňať informácie, ktoré vám poskytne váš dovozca údajov), aby ste si ozrejmili rozsah pôsobnosti článku 702 FISA v praxi na váš konkrétny prenos. Tieto informácie by mali poskytnúť odpovede na niektoré relevantné otázky, ako napríklad:

[58] Článok 5 ods. 2 všeobecného nariadenia o ochrane údajov.
[59] SDEÚ, C-311/18 (Schrems II), body 134 a 135.

- Poukazujú verejne dostupné informácie na to, že existuje zákonný zákaz informovať o konkrétnej žiadosti o prístup k prijatým údajom a rozsiahle obmedzenia týkajúce sa poskytovania všeobecných informácií o žiadostiach o prístup k prijatým údajom alebo o neexistencii doručených žiadostí?

- Potvrdil váš dovozca údajov, že v minulosti dostal žiadosti o prístup k údajom od orgánov verejnej moci USA? Alebo váš dovozca údajov potvrdil, že v minulosti nedostal žiadosti o prístup k údajom od orgánov verejnej moci USA a nemá zakázané poskytovať informácie o takých žiadostiach alebo ich neexistencii?

- Preukazujú verejne dostupné informácie, ktoré ste získali o judikatúre USA a správy od orgánov dohľadu, organizácií občianskej spoločnosti a akademických inštitúcií,[60] že dovozcovia údajov z rovnakého odvetvia ako váš dovozca dostali v minulosti žiadosti o prístup k údajom v prípade podobných prenesených údajov?

Odpovede na tieto otázky, ktoré získate na základe celkového posúdenia, vás vedú k záveru, že:

- Ustanovenie článku 702 FISA sa v praxi vzťahuje na váš konkrétny prenos, a preto má vplyv na účinnosť vášho nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov. Ak teda chcete pokračovať v prenose, musíte v prípade potreby v spolupráci s dovozcom zvážiť, či môžete prijať dodatočné opatrenia, ktoré účinne zabezpečia, že úroveň ochrany prenesených údajov bude v podstate rovnocenná s úrovňou zaručenou v EHP. Ak nemôžete nájsť účinné dodatočné opatrenia, nesmiete osobné údaje prenášať.

Alebo

- Ustanovenie článku 702 FISA sa v praxi nevzťahuje na váš konkrétny prenos, a preto nemá vplyv na účinnosť vášho nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov. Potom môžete pokračovať v prenose bez akýchkoľvek dodatočných opatrení.

2.4 4. krok: Prijatie dodatočných opatrení

50. Ak z posúdenia v kroku 3 vyplynie, že váš nástroj na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov nie je účinný, budete musieť zvážiť, v prípade potreby v spolupráci s dovozcom, či existujú dodatočné opatrenia, ktoré by po doplnení k zárukám obsiahnutým v nástrojoch na prenos mohli zabezpečiť, aby sa prenášaným údajom v tretej krajine poskytla úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v rámci EÚ.[61] „Dodatočné opatrenia“ podľa definície dopĺňajú záruky, ktoré už poskytuje nástroj na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov, a akékoľvek ďalšie platné bezpečnostné požiadavky (napr. technické bezpečnostné opatrenia) stanovené vo všeobecnom nariadení o ochrane údajov.[62]

[60] napr. článok 702 FISA, rokovací poriadok Dozorného súdu pre zahraničné spravodajské služby (FISC), odtajnené stanoviská a rozhodnutia FISC, judikatúra súdov USA, správy a prepisy vypočutí Výboru pre dohľad nad súkromím a občianskymi slobodami (PCLOB); správy Úradu generálneho inšpektora - Ministerstvo spravodlivosti USA, správy riaditeľa NSA Úradu pre občianske slobody a súkromie; správy vypracované Kongresovou výskumnou službou; správy Amerického zväzu pre občianske slobody (ACLU).
[61] C-311/18 (Schrems II), bod 96.
[62] Odôvodnenie 109 všeobecného nariadenia o ochrane údajov a vec C-311/18 (Schrems II), bod 133.

51. Pri použití osobitného nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov musíte v každom jednotlivom prípade určiť, ktoré dodatočné opatrenia by mohli byť účinné v prípade súboru prenosov do konkrétnej tretej krajiny. Posúdenie nemusíte vykonávať opakovane zakaždým, keď uskutočňujete rovnaký prenos určitého typu údajov do tej istej tretej krajiny. Niektoré údaje, ktoré plánujete prenášať, si môžu vyžadovať dodatočné opatrenia, kým iné údaje ich nevyžadujú (vzhľadom na formálne a/alebo praktické uplatňovanie právnych predpisov tretej krajiny). Budete môcť vychádzať z predchádzajúcich hodnotení v rámci krokov (1, 2 a 3 vyššie) a na základe ich zistení skontrolovať potenciálnu účinnosť dodatočných opatrení pri zabezpečovaní požadovanej úrovne ochrany.

52. V zásade môžu mať dodatočné opatrenia zmluvnú, technickú alebo organizačnú povahu. Kombináciou rôznych opatrení tak, aby sa vzájomne podporovali a rozvíjali, sa môže zvýšiť úroveň ochrany, a to môže prispieť k dosiahnutiu noriem EÚ.

53. Samotné zmluvné a organizačné opatrenia vo všeobecnosti nezabránia prístupu orgánov verejnej moci tretej krajiny k osobným údajom na základe problematických právnych predpisov a/alebo praxe.[63] Môžu nastať situácie, keď len vhodne zavedené technické opatrenia môžu zabrániť prístupu orgánov verejnej moci v tretích krajinách k osobným údajom, najmä na účely sledovania, alebo takýto prístup znemožniť.[64] V takých situáciách môžu zmluvné alebo organizačné opatrenia dopĺňať technické opatrenia a posilniť celkovú úroveň ochrany údajov (napr. zavedením kontrol a zamedzením automatických pokusov orgánov verejnej moci o prístup k údajom spôsobom, ktorý nie je v súlade s normami EÚ).

54. V prípade potreby si môžete v spolupráci s dovozcom údajov pozrieť nasledujúci (orientačný) zoznam faktorov, aby ste zistili, ktoré dodatočné opatrenia by boli najefektívnejšie na ochranu prenášaných údajov pred žiadosťami orgánov verejnej moci o prístup k údajom na základe problematických právnych predpisov uplatňovaných v praxi:

    - formát údajov, ktoré sa majú preniesť (t. j. obyčajný text/pseudonymizované alebo zašifrované),
    - povaha údajov (napr. vyššia úroveň ochrany je v EHP poskytovaná kategóriám údajov, na ktoré sa vzťahujú články 9 a 10 všeobecného nariadenia o ochrane údajov); [65]
    - dĺžka a zložitosť pracovného postupu spracúvania údajov, počet aktérov zapojených do spracúvania a vzťah medzi nimi (napr. prenosy zahŕňajú viacerých prevádzkovateľov alebo

---

[63] „Problematickými právnymi predpismi“ sa rozumejú právne predpisy, ktoré 1) príjemcovi osobných údajov z Európskej únie ukladajú povinnosti a/alebo môžu ovplyvniť prenášané údaje spôsobom, ktorý môže zasahovať do zmluvnej záruky nástrojov na prenos, ktorou je v podstate rovnocenná úroveň ochrany a 2) sú v rozpore s podstatou základných práv a slobôd uznaných Chartou základných práv EÚ alebo prekračujú rámec toho, čo je v demokratickej spoločnosti nevyhnutné a primerané na ochranu niektorého z významných cieľov, ktoré uznáva aj právo Únie alebo členských štátov EÚ, akými sú ciele, ktoré sú uvedené v článku 23 ods. 1 všeobecného nariadenia o ochrane údajov.

[64] Ak takýto prístup presahuje rámec toho, čo je nevyhnutné a primerané v demokratickej spoločnosti; pozri články 47 a 52 Charty základných práv Európskej únie, článok 23 ods. 1 všeobecného nariadenia o ochrane údajov a odporúčania EDPB 02/2020 o európskych základných zárukách pre opatrenia týkajúce sa sledovania, 10. novembra 2020, https://edpb.europa.eu/system/files/2021-04/edpb_recommendations_202002_europeanessentialguaranteessurveillance_sk.pdf.

[65] Pozri poznámku pod čiarou 42.

prevádzkovateľov aj sprostredkovateľov, alebo sú zapojení sprostredkovatelia, ktorí od vás prenesú údaje svojmu dovozcovi údajov so zreteľom na príslušné ustanovenia, ktoré sa na nich vzťahujú podľa právnych predpisov tretej krajiny určenia),[66]

- spôsob alebo parametre praktického uplatňovania právnych predpisov tretej krajiny vymedzené v kroku 3;

- možnosť, že údaje môžu byť predmetom následného prenosu v rámci tej istej tretej krajiny alebo dokonca do iných tretích krajín (napr. zapojenie ďalších sprostredkovateľov dovozcu údajov[67]).

-

Príklady *dodatočných* opatrení

55. Niektoré príklady technických, zmluvných a organizačných opatrení, ktoré možno vziať do úvahy, ak ešte nie sú zahrnuté v použitom nástroji na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov, možno nájsť v orientačných zoznamoch opísaných v prílohe 2.

***

56. Ak ste zaviedli účinné dodatočné opatrenia, ktoré v kombinácii s vybraným nástrojom na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov dosahujú úroveň ochrany, ktorá je v súčasnosti v podstate rovnocenná s úrovňou ochrany zaručenej v rámci EHP, môžu vaše prenosy pokračovať.

57. Ak nie ste schopní identifikovať alebo vykonať účinné dodatočné opatrenia, ktoré zabezpečia, aby sa na prenášané osobné údaje vzťahovala v podstate rovnocenná úroveň ochrany[68], nesmiete začať s prenosom osobných údajov do dotknutej tretej krajiny na základe nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov, ktorý využívate. Ak už vykonávate prenosy, musíte prenos údajov pozastaviť alebo ukončiť.[69] V súlade so zárukami obsiahnutými v nástroji na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov, ktorý využívate, by vám mal dovozca vrátiť údaje, ktoré ste už do tejto tretej krajiny preniesli, a ich kópie, alebo ich úplne zničiť.[70]

Príklad:

Právne predpisy tretej krajiny zakazujú dodatočné opatrenia, ktoré ste identifikovali (napr. zakazujú používanie šifrovania), alebo iným spôsobom bránia ich účinnosti. Nesmiete začať s prenosom osobných údajov do tejto krajiny alebo musíte zastaviť prebiehajúce prenosy do tejto krajiny.

---

[66] Vo všeobecnom nariadení o ochrane údajov sa prevádzkovateľom a sprostredkovateľom ukladajú osobitné povinnosti. K prenosom môže dochádzať medzi prevádzkovateľmi, medzi spoločnými prevádzkovateľmi, od prevádzkovateľa sprostredkovateľovi, a na základe povolenia prevádzkovateľa od sprostredkovateľa prevádzkovateľovi alebo od sprostredkovateľa sprostredkovateľovi.

[67] Pozri poznámku pod čiarou 26.

[68] Ak takýto prístup presahuje rámec toho, čo je nevyhnutné a primerané v demokratickej spoločnosti; pozri články 47 a 52 Charty základných práv Európskej únie, článok 23 ods. 1 všeobecného nariadenia o ochrane údajov a odporúčania EDPB 02/2020 o európskych základných zárukách pre opatrenia týkajúce sa sledovania, 10. novembra 2020, https://edpb.europa.eu/system/files/2021-04/edpb_recommendations_202002_europeanessentialguaranteessurveillance_sk.pdf.

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

[70] Pozri doložku 12 v prílohe k rozhodnutiu o štandardných zmluvných doložkách 87/2010; pozri (dobrovoľnú) dodatočnú doložku o ukončení v prílohe B k rozhodnutiu 2004/915/ES o štandardných zmluvných doložkách.

58. Príslušný dozorný orgán môže uložiť akékoľvek iné nápravné opatrenie (napr. pokutu), ak napriek tomu, že nemôžete preukázať v podstate rovnocennú úroveň ochrany v tretej krajine, začnete prenos alebo v ňom pokračujete.

2.5 Krok č. 5: Procesné kroky, ak ste identifikovali účinné dodatočné opatrenia

59. Procesné kroky, ktoré budete musieť podniknúť, ak ste identifikovali účinné dodatočné opatrenia, ktoré sa majú zaviesť, sa môžu líšiť v závislosti od nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov, ktorý využívate alebo ktorého použitie zvažujete.

2.5.1 Štandardné doložky o ochrane údajov [článok 46 ods. 2 písm. c) a d) všeobecného nariadenia o ochrane údajov]

60. Ak máte v úmysle okrem štandardných zmluvných doložiek zaviesť aj dodatočné opatrenia, nie je potrebné, aby ste požiadali príslušný dozorný orgán o povolenie doplniť tento druh doložiek alebo ďalších záruk, pokiaľ identifikované dodatočné opatrenia nie sú v priamom ani nepriamom rozpore so štandardnými zmluvnými doložkami a sú dostatočné na to, aby sa zabezpečilo, že sa nenaruší úroveň ochrany zaručená všeobecným nariadením o ochrane údajov.[71] Vývozca a dovozca údajov musia zabezpečiť, aby dodatočné doložky nebolo v žiadnom prípade možné vykladať spôsobom, ktorý by obmedzoval práva a povinnosti na základe štandardných zmluvných doložiek alebo akýmkoľvek iným spôsobom, ktorý by znižoval úroveň ochrany údajov. Mali by ste byť schopní to preukázať, rovnako ako aj jednoznačnosť všetkých doložiek v súlade so zásadou zodpovednosti a vašou povinnosťou zabezpečiť dostatočnú úroveň ochrany údajov. Príslušné dozorné orgány majú v prípade potreby právomoc preskúmať tieto dodatočné doložky (napr. v prípade sťažnosti alebo vyšetrovania z vlastného podnetu).

61. Ak máte v úmysle zmeniť samotné štandardné doložky o ochrane údajov alebo ak pridané dodatočné opatrenia sú priamo alebo nepriamo „v rozpore“ so štandardnými zmluvnými doložkami, nebude sa to považovať za spoliehanie sa na štandardné zmluvné doložky[72] a musíte požiadať o povolenie príslušný dozorný orgán v súlade s článkom 46 ods. 3 písm. a) všeobecného nariadenia o ochrane údajov.

---

[71] V odôvodnení 109 všeobecného nariadenia o ochrane údajov sa uvádza: „Možnosť pre prevádzkovateľa alebo sprostredkovateľa uplatniť štandardné doložky o ochrane údajov prijaté Komisiou alebo dozorným orgánom by prevádzkovateľom ani sprostredkovateľom nemali brániť v tom, aby zahrnuli štandardné doložky o ochrane údajov do širšej zmluvy, ako napríklad zmluvy medzi sprostredkovateľom a ďalším sprostredkovateľom, alebo k nim pridali ďalšie doložky alebo dodatočné záruky, pokiaľ nie sú priamo alebo nepriamo v rozpore so štandardnými zmluvnými doložkami prijatými Komisiou alebo dozorným orgánom alebo pokiaľ sa nedotýkajú základných práv alebo slobôd dotknutých osôb.“ Podobné ustanovenia sú stanovené v súboroch štandardných zmluvných doložiek prijatých Komisiou podľa smernice 95/46/ES.

[72] Pozri analogicky stanovisko EDPB 17/2020 k návrhu štandardných zmluvných doložiek, ktorý predložil slovinský dozorný orgán (článok 28 ods. 8 všeobecného nariadenia o ochrane údajov) k štandardným zmluvným doložkám podľa článku 28, ktoré už bolo prijaté a ktoré obsahuje podobné ustanovenie ("Navyše Výbor pripomína, že možnosť používať štandardné zmluvné doložky, ktoré prijal dozorný orgán, nebráni zmluvným stranám pridať ďalšie doložky alebo dodatočné záruky za predpokladu, že nie sú priamo ani nepriamo v rozpore s prijatými štandardnými zmluvnými doložkami, ani neporušujú základné práva alebo slobody dotknutých osôb. Okrem toho, ak sa štandardné doložky o ochrane údajov zmenia, nebude už platiť, že zmluvné strany využívajú prijaté štandardné zmluvné doložky“), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_en.pdf

2.5.2 Záväzné vnútropodnikové pravidlá [článok 46 ods. 2 písm. b) všeobecného nariadenia o ochrane údajov]

62. Odôvodnenie uvedené v rozsudku vo veci Schrems II sa vzťahuje aj na iné nástroje na prenos podľa článku 46 ods. 2 všeobecného nariadenia o ochrane údajov, keďže všetky tieto nástroje majú v zásade zmluvnú povahu, takže predpokladané záruky a záväzky prijaté ich stranami nemôžu zaväzovať orgány verejnej moci tretích krajín.[73]

63. Rozsudok vo veci Schrems II je relevantný pre prenosy osobných údajov na základe záväzných vnútropodnikových pravidiel, keďže právne predpisy tretích krajín môžu mať vplyv na ochranu poskytovanú takýmito nástrojmi.

64. Všetky povinnosti, ktoré je potrebné zahrnúť, budú uvedené v aktualizovaných referenciách WP256/257[74], s ktorými budú musieť všetky skupiny, ktoré využívajú záväzné vnútropodnikové pravidlá ako na nástroje na prenos, zosúladiť svoje súčasné a budúce záväzné vnútropodnikové pravidlá.

65. Súdny dvor zdôraznil, že je zodpovednosťou vývozcu údajov a dovozcu údajov, aby posúdili, či sa v príslušnej tretej krajine dodržiava úroveň ochrany, ktorú vyžaduje právo EÚ, s cieľom určiť, či je v praxi možné dodržať záruky, ktoré poskytujú štandardné zmluvné doložky alebo záväzné vnútropodnikové pravidlá. V opačnom prípade by ste mali posúdiť, či dokážete prijať dodatočné opatrenia na zabezpečenie úrovne ochrany, ktorá je v podstate rovnocenná s úrovňou ochrany, ktorá sa poskytuje v EHP, a či do týchto dodatočných opatrení nebudú zasahovať právne predpisy alebo postupy tretej krajiny, ktoré by zabránili ich účinnosti.

2.5.3 Zmluvné doložky ad hoc [článok 46 ods. 3 písm. a) všeobecného nariadenia o ochrane údajov]

66. Odôvodnenie uvedené v rozsudku vo veci Schrems II sa vzťahuje aj na iné nástroje na prenos podľa článku 46 ods. 2 všeobecného nariadenia o ochrane údajov, keďže všetky tieto nástroje majú v zásade zmluvnú povahu, takže predpokladané záruky a záväzky prijaté ich stranami nemôžu zaväzovať orgány verejnej moci tretích krajín.[75] Rozsudok vo veci Schrems II je preto relevantný pre prenosy osobných údajov na základe zmluvných doložiek ad hoc, keďže právne predpisy tretích krajín môžu mať vplyv na ochranu poskytovanú takýmito nástrojmi.

2.6 6. krok: Prehodnotenie v primeraných intervaloch

67. Musíte priebežne, a v prípade potreby v spolupráci s dovozcami údajov, monitorovať vývoj v tretej krajine, do ktorej ste preniesli osobné údaje, ktorý by mohol ovplyvniť vaše pôvodné posúdenie úrovne ochrany a rozhodnutia, ktoré ste prípadne prijali v súvislosti s vašimi prenosmi. Zodpovednosť predstavuje sústavnú povinnosť (článok 5 ods. 2 všeobecného nariadenia o ochrane údajov).

---

[73] SDEÚ, C-311/18 (Schrems II), bod 132.

[74] Pracovná skupina zriadená podľa článku 29, Pracovný dokument, ktorým sa vytvára tabuľka s prvkami a zásadami, ktoré sa nachádzajú v záväzných vnútropodnikových pravidlách, naposledy revidovaný a prijatý 6. februára 2018; WP 256 rev.01; Pracovná skupina zriadená podľa článku 29, Pracovný dokument, ktorým sa vytvára tabuľka s prvkami a zásadami, ktoré sa nachádzajú v záväzných vnútropodnikových pravidlách pre sprostredkovateľov, naposledy revidovaný a prijatý 6. februára 2018, WP 257 rev.01.

[75] SDEÚ, C-311/18 (Schrems II), bod 132.

68. Mali by ste zaviesť dostatočne spoľahlivé mechanizmy, aby ste zabezpečili, že okamžite pozastavíte alebo ukončíte prenosy, ak:

    - dovozca porušil alebo nie je schopný plniť záväzky, ktoré prijal v rámci nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov,
    - dodatočné opatrenia už v tejto tretej krajine nie sú účinné.

3 ZÁVER

69. Vo všeobecnom nariadení o ochrane údajov sa stanovujú pravidlá spracúvania osobných údajov v EHP, čím sa umožňuje voľný pohyb osobných údajov v rámci EHP. V kapitole V všeobecného nariadenia o ochrane údajov sa upravuje prenos osobných údajov do tretích krajín a stanovuje sa vysoká úroveň: prenos nesmie ohroziť úroveň ochrany fyzických osôb, ktorú zaručuje všeobecné nariadenie o ochrane údajov (článok 44 všeobecného nariadenia o ochrane údajov). V rozsudku SDEÚ C-311/18 (Schrems II) sa zdôrazňuje potreba zabezpečiť kontinuitu úrovne ochrany osobných údajov prenášaných do tretej krajiny podľa všeobecného nariadenia o ochrane údajov.[76]

70. Aby ste zabezpečili v podstate rovnocennú úroveň ochrany údajov, musíte v prvom rade dôkladne poznať vlastné prenosy. Musíte tiež skontrolovať, že údaje, ktoré prenášate, sú primerané, relevantné a obmedzené vo vzťahu k tomu, čo je nevyhnutné vzhľadom na účely, na ktoré sa prenášajú.

71. Ďalej musíte identifikovať nástroj na prenos, ktorý využívate pri svojich prenosoch. Ak tento nástroj na prenos nie je rozhodnutím o primeranosti, musíte v každom jednotlivom prípade overiť, či právne predpisy alebo postupy tretej krajiny určenia ohrozujú záruky obsiahnuté v nástroji na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov v súvislosti s vašimi prenosmi. Ak samotný nástroj na prenos údajov podľa článku 46 všeobecného nariadenia o ochrane údajov nezabezpečuje v prípade osobných údajov, ktoré prenášate, úroveň ochrany, ktorá je v podstate rovnocenná, túto medzeru môžu vyplniť dodatočné opatrenia.

72. Ak nie ste schopní identifikovať alebo vykonať účinné dodatočné opatrenia, ktoré zabezpečia, aby sa na prenášané osobné údaje vzťahovala v podstate rovnocenná úroveň ochrany, nesmiete začať s prenosom osobných údajov do dotknutej tretej krajiny na základe nástroja na prenos, pre ktorý ste sa rozhodli. Ak už vykonávate prenosy, musíte prenos osobných údajov bezodkladne pozastaviť alebo ukončiť.

73. Príslušný dozorný orgán má právomoc pozastaviť alebo ukončiť prenos osobných údajov do tretej krajiny, ak ochrana prenášaných údajov, ktorú vyžaduje právo EÚ, najmä články 45 a 46 všeobecného nariadenia o ochrane údajov a Charta základných práv Európskej únie, nie je zaručená.

Za Európsky výbor pre ochranu údajov
predsedníčka
(Andrea Jelinek)

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

PRÍLOHA 1: VYMEDZENIE POJMOV

- „Tretia krajina“ je každá krajina, ktorá nie je členským štátom EHP.
- „EHP“ je Európsky hospodársky priestor a zahŕňa členské štáty Európskej únie a Island, Nórsko a Lichtenštajnsko. Všeobecné nariadenie o ochrane údajov sa na Island, Nórsko a Lichtenštajnsko vzťahuje na základe Dohody o EHP, najmä na základe jej prílohy XI a protokolu 37.
- „Všeobecné nariadenie o ochrane údajov“ je nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).
- „Charta“ je Charta základných práv Európskej únie, Ú. v. EÚ C 326, 26.10.2012, s. 391 – 407.
- „SDEÚ“ alebo „Súdny dvor“ je Súdny dvor Európskej únie. Ide o súdny orgán Európskej únie a v spolupráci so súdmi členských štátov zabezpečuje jednotné uplatňovanie a výklad práva Únie.
- „Vývozca údajov“ je prevádzkovateľ alebo sprostredkovateľ v rámci EHP, ktorý prenáša osobné údaje prevádzkovateľovi alebo sprostredkovateľovi v tretej krajine.
- „Dovozca údajov“ je prevádzkovateľ alebo sprostredkovateľ v tretej krajine, ktorý prijíma osobné údaje prenášané z EHP alebo k nim získava prístup.
- „Nástroj na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov“ sú primerané záruky podľa článku 46 všeobecného nariadenia o ochrane údajov, ktoré vývozcovia údajov zavedú pri prenose osobných údajov do tretej krajiny, ak neexistuje rozhodnutie o primeranosti podľa článku 45 ods. 3 všeobecného nariadenia o ochrane údajov. Článok 46 ods. 2 a 3 všeobecného nariadenia o ochrane údajov obsahuje zoznam nástrojov na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov, ktoré môžu prevádzkovatelia a sprostredkovatelia používať.
- „Štandardné zmluvné doložky [*SCCs*]“ sú štandardné doložky o ochrane údajov, ktoré prijala Európska komisia pre prípad prenosov osobných údajov medzi prevádzkovateľmi alebo sprostredkovateľmi v rámci EHP a prevádzkovateľmi alebo sprostredkovateľmi mimo EHP. Štandardné zmluvné doložky prijaté Európskou komisiou sú nástrojom na prenos podľa všeobecného nariadenia o ochrane údajov podľa článku 46 ods. 2 písm. c) a ods. 5 všeobecného nariadenia o ochrane údajov.

PRÍLOHA 2: PRÍKLADY DODATOČNÝCH OPATRENÍ

74. Nasledujúce opatrenia sú príkladmi dodatočných opatrení, ktoré môžete zvážiť v kroku 4 „Prijatie dodatočných opatrení“. Tento zoznam nie je úplný. Môžete skúmať ďalšie dodatočné opatrenia. Budúci technologický, právny alebo organizačný vývoj môže viesť k vzniku nových dodatočných opatrení, ktoré by ste mali zvážiť. Výber a vykonávanie jedného alebo viacerých z týchto opatrení nemusí nevyhnutne a systematicky zabezpečiť, že váš prenos spĺňa štandard v podstate rovnocennej úrovne ochrany, ktorý vyžaduje právo Únie. Mali by ste vybrať také dodatočné opatrenia, ktoré dokážu účinne zaručiť túto úroveň ochrany pri vašich prenosoch.

75. Akékoľvek dodatočné opatrenie možno považovať za účinné v zmysle rozsudku SDEÚ „Schrems II“ len vtedy a v rozsahu, v akom samé alebo v kombinácii s inými opatreniami rieši konkrétne nedostatky zistené pri vašom posúdení situácie v tretej krajine, pokiaľ ide o jej právne predpisy a postupy uplatniteľné na váš prenos. Ak v konečnom dôsledku nedokážete zabezpečiť v podstate rovnocennú úroveň ochrany, nesmiete prenášať osobné údaje.

76. Pokiaľ ste prevádzkovateľom alebo sprostredkovateľom, možno od vás už vyžadovať, aby ste prijali niektoré z opatrení opísaných v tejto prílohe, aby ste dosiahli súlad so všeobecným nariadením o ochrane údajov. To znamená, že podobné opatrenia bude možno potrebné zaviesť v prípade osobných údajov spracúvaných v EHP, prenášaných dovozcovi údajov, na ktoré sa vzťahuje rozhodnutie o primeranosti, alebo do iných tretích krajín.[77]

2.1 Technické opatrenia

77. V tomto oddiele sa uvádza orientačný opis príkladov technických opatrení, ktoré môžu dopĺňať záruky uvedené v článku 46 všeobecného nariadenia o ochrane údajov na účely zabezpečenia súladu s úrovňou ochrany vyžadovanou podľa práva EÚ v súvislosti s prenosom osobných údajov do tretej krajiny. Tieto opatrenia budú potrebné najmä vtedy, keď právne predpisy danej krajiny ukladajú dovozcovi údajov povinnosti, ktoré sú v rozpore so zárukami uvedenými v článku 46 všeobecného nariadenia o ochrane údajov a najmä ktoré môžu spochybniť zmluvnú záruku v podstate rovnocennej úrovne ochrany pred prístupom orgánov verejnej moci uvedenej tretej krajiny k týmto údajom.[78]

78. Na účely lepšej zrozumiteľnosti táto časť opisuje najprv niekoľko príkladov scenárov, v prípade ktorých by niektoré technické opatrenia mohli byť potenciálne účinné na zabezpečenie v podstate rovnocennej úrovne ochrany. Časť pokračuje niekoľkými scenármi, v prípade ktorých nie sú identifikované technické opatrenia na zabezpečenie tejto úrovne ochrany.

[77] Článok 5 ods. 2 všeobecného nariadenia o ochrane údajov, článok 32 všeobecného nariadenia o ochrane údajov.
[78] C-311/18 (Schrems II), bod 135.

Príklady scenárov odkazujúcich na prípady, v ktorých sú identifikované *účinné* opatrenia

79. Uvedené opatrenia majú zabezpečiť, aby prístup orgánov verejnej moci v tretích krajinách k prenášaným údajom nezasahoval do účinnosti primeraných záruk obsiahnutých v nástrojoch na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov. Tieto opatrenia by boli potrebné na zaručenie v podstate rovnocennej úrovne ochrany, aká je zaručená v EHP, aj keď je prístup orgánov verejnej moci v súlade s právom krajiny dovozcu, kde v praxi taký prístup presahuje rámec toho, čo je nevyhnutné a primerané v demokratickej spoločnosti.[79] Cieľom týchto opatrení je zabrániť potenciálnemu neoprávnenému prístupu tým, že sa orgánom zabráni identifikovať dotknuté osoby, získať informácie o nich, osobitne ich vyčleniť v inom kontexte alebo spojiť prenášané údaje s inými súbormi údajov, ktoré môžu mať k dispozícii a ktoré môžu okrem iného obsahovať online identifikátory zo zariadení, aplikácií, nástrojov a protokolov, ktoré dotknuté osoby používajú v iných kontextoch.

80. Orgány verejnej moci v tretích krajinách sa môžu usilovať o prístup k prenášaným údajom

    a) Počas prenosu prostredníctvom prístupu ku komunikačným linkám používaným na prenos údajov do prijímajúcej krajiny. Tento prístup môže byť pasívny, pričom v takom prípade sa obsah komunikácie po prípadnom výbere jednoducho skopíruje. Prístup však môže byť aktívny, a to v tom zmysle, že orgány verejnej moci sa do procesu komunikácie zapájajú nielen tým, že čítajú obsah, ale aj manipulujú s jeho časťami alebo ich potláčajú.

    b) Počas úschovy u určeného príjemcu údajov buď prístupom k samotným spracovateľským zariadeniam, alebo tým, že sa od príjemcu údajov vyžaduje, aby vyhľadal a získal relevantné údaje a poskytol ich orgánom.

81. V tomto oddiele sa posudzujú scenáre, v ktorých sa uplatňujú opatrenia, ktoré sú účinné v oboch prípadoch. Vzhľadom na okolnosti konkrétneho prenosu sa môžu uplatňovať rôzne dodatočné opatrenia, ktoré môžu byť dostatočné, ak sa v právnych predpisoch prijímajúcej krajiny predpokladá len jeden druh prístupu. Preto je potrebné, aby vývozca údajov s podporou dovozcu údajov dôkladne analyzoval povinnosti, ktoré mu boli uložené.

Napríklad dovozcovia údajov z USA, na ktorých sa vzťahuje hlava 50 zákonníka USA § 1881a (článok 702 FISA), majú priamu povinnosť poskytnúť prístup k dovezeným osobným údajom, ktoré majú k dispozícii, v úschove alebo pod kontrolou, alebo ich odovzdať. To sa môže vzťahovať aj na akékoľvek kryptografické kľúče potrebné na zabezpečenie zrozumiteľnosti údajov.

82. Scenáre opisujú konkrétne okolnosti a opatrenia, ktoré majú slúžiť ako príklad. Akékoľvek zmeny scenárov môžu viesť k odlišným záverom. Scenáre sa týkajú situácií, v ktorých sa dospelo k záveru, že ako prvoradé sú potrebné dodatočné opatrenia, t. j. keď sa v praxi na predmetný prenos uplatňujú problematické právne predpisy tretej krajiny.

[79] Pozri články 47 a 52 Charty základných práv Európskej únie, článok 23 ods. 1 všeobecného nariadenia o ochrane údajov a odporúčania EDPB 02/2020 o európskych základných zárukách pre opatrenia týkajúce sa sledovania, 10. novembra 2020, https://edpb.europa.eu/system/files/2021-04/edpb_recommendations_202002_europeanessentialguaranteessurveillance_sk.pdf.

83. Prevádzkovatelia možno budú musieť uplatňovať niektoré alebo všetky tu opísané opatrenia bez ohľadu na úroveň ochrany stanovenú v právnych predpisoch vzťahujúcich sa na dovozcu údajov, pretože sú za konkrétnych okolností prenosu potrebné na dodržiavanie článkov 25 a 32 všeobecného nariadenia o ochrane údajov. Inými slovami, od vývozcov sa môže vyžadovať, aby vykonali opatrenia opísané v tomto dokumente, aj keď sa na ich dovozcov údajov vzťahuje rozhodnutie o primeranosti, rovnako ako sa od prevádzkovateľov a sprostredkovateľov môže vyžadovať, aby ich vykonávali, keď sa údaje spracúvajú v rámci EHP.

Prípad použitia 1: Uchovávanie údajov na zálohovanie a iné účely, ktoré si nevyžadujú prístup k nezašifrovaným údajom [data in the clear]

84. Vývozca údajov využíva na uchovávanie osobných údajov, napr. na účely zálohovania, poskytovateľa hostingových služieb v tretej krajine.

Ak

1. sa osobné údaje pred poskytnutím spracúvajú pomocou silného šifrovania a overuje sa totožnosť dovozcu,
2. šifrovací algoritmus a jeho parametre (napr. dĺžka kľúča, príp. prevádzkový režim) zodpovedanú najnovším poznatkom [state-ot-the-art] a možno ich považovať za odolné voči kryptoanalýze vykonávanej orgánmi verejnej moci v prijímajúcej krajine s prihliadnutím na dostupné zdroje a technické kapacity (napr. výpočtová kapacita pre útoky hrubou silou)[80];
3. sila šifrovania a dĺžka kľúča zohľadňuje konkrétne časové obdobie, počas ktorého sa musí zachovať dôvernosť šifrovaných osobných údajov,[81]
4. šifrovací algoritmus je vykonaný správne a prostredníctvom riadne udržiavaného softvéru bez známych zraniteľností, ktorého súlad so špecifikáciou zvoleného algoritmu bol overený, napr. certifikáciou;
5. kľúče sú spoľahlivo riadené (vytvárané, spravované, uložené, príp. prepojené s totožnosťou zamýšľaného príjemcu a zrušené) [82],a

---

[80] Pri hodnotené sily šifrovacích algoritmov, ich súladu s najnovšími poznatkami a ich odolnosti voči kryptoanalýze v priebehu času sa môžu vývozcovia údajov spoľahnúť na technické usmernenia zverejnené oficiálnymi orgánmi EÚ a jej členských štátov pre kybernetickú bezpečnosť. Pozri napr. Správa ENISA <<Aké sú „najnovšie poznatky" v IT bezpečnosti?>>, 2019, https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security; usmernenie nemeckého Spolkového úradu pre bezpečnosť informácií v jeho dokumente Technical Guidelines of the TR-02102 series and "Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 – Project 645421, D5.4, ECRYPT-CSA, 02/2018" at https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

[81] Ochranná schopnosť kryptografických algoritmov časom klesá v dôsledku objavenia nových kryptoanalytických techník, vzniku nových výpočtových paradigiem, akými sú kvantové výpočty, a všeobecného zvýšenia dostupnej výpočtovej kapacity, pokiaľ sa nepreukáže, že použité algoritmy sú teoreticky bezpečné. Táto obava sa týka najmä algoritmov verejného kľúča, ktoré sa v čase písania bežne používajú. V dôsledku toho musí vývozca údajov zohľadniť, že orgány verejnej moci sa môžu pokúsiť o prístup k zašifrovaným údajom za okolností opísaných v odseku č. 80 a uložiť ich, kým ich zdroje nebudú dostatočné na dešifrovanie. Dodatočné opatrenie možno považovať za účinné len vtedy, ak by také dešifrovanie a následné ďalšie spracúvanie v tom čase už nepredstavovalo porušenie práv dotknutých osôb, napríklad preto, že údaje už nemožno použiť na ich priamu alebo nepriamu identifikáciu.

[82] Osobitná publikácia NIST 800-57, Odporúčanie pre manažment kľúčov https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

6. kľúče zostávajú výlučne pod kontrolou vývozcu údajov alebo subjektu, ktorému vývozca v EHP dôveruje, alebo jurisdikcie, ktorá ponúka v podstate rovnocennú úroveň ochrany, aká je zaručená v rámci EHP.

potom sa EDPB domnieva, že vykonané šifrovanie predstavuje účinné dodatočné opatrenie.

Prípad použitia 2: Prenos pseudonymizovaných údajov

85. Vývozca údajov najprv pseudonymizuje údaje, ktoré má k dispozícii, a potom ich prenesie do tretej krajiny na účely analýzy, napr. na účely výskumu.

Ak

1. vývozca údajov prenáša osobné údaje spracúvané takým spôsobom, že osobné údaje už nemožno priradiť konkrétnej dotknutej osobe, ani ich nemožno použiť na osobitný výber dotknutej osoby z väčšej skupiny bez použitia dodatočných informácií[83];
2. takými dodatočnými informáciami disponuje výlučne vývozca údajov a v členskom štáte alebo v tretej krajine ich oddelene uchováva subjekt, ktorému vývozca dôveruje v EHP alebo v rámci jurisdikcie, ktorá ponúka v podstate rovnocennú úroveň ochrany, aká je zaručená v EHP,
3. poskytnutiu alebo neoprávnenému použitiu týchto dodatočných informácií bránia primerané technické a organizačné záruky, zabezpečuje sa, aby si vývozca údajov zachoval výlučnú kontrolu nad algoritmom alebo úložiskom umožňujúcim opätovnú identifikáciu pomocou dodatočných informácií; a
4. prevádzkovateľ na základe dôkladnej analýzy príslušných údajov a so zohľadnením informácií, ktoré môžu mať orgány verejnej moci prijímajúcej krajiny k dispozícii a použiť, potvrdil, že pseudonymizované osobné údaje nemožno priradiť k identifikovanej alebo identifikovateľnej fyzickej osobe, a to ani v prípade, že také informácie sú uvedené krížovým odkazom [cross-referenced];

potom sa EDPB domnieva, že vykonaná pseudonimyzácia predstavuje účinné dodatočné opatrenie.

86. Upozorňujeme, že v mnohých situáciách môžu faktory špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu fyzickej osoby, jej fyzické umiestnenie alebo jej interakciu s internetovou službou v konkrétnych časových okamihoch[84]

[83] V súlade s článkom 4 bodom 5 všeobecného nariadenia o ochrane údajov: „‚pseudonymizácia' znamená spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatreniam s cieľom zabezpečiť, aby osobné údaje neboli priradené k identifikovanej alebo identifikovateľnej fyzickej osobe;" Dodatočné údaje môžu pozostávať z tabuliek, ktoré vedľa seba uvádzajú pseudonymy s identifikačnými atribútmi, ktoré nahrádzajú, kryptografické kľúče alebo iné parametre na transformáciu atribútov alebo ďalšie údaje, ktoré umožňujú priradiť pseudonymizované údaje k identifikovaným alebo identifikovateľným fyzickým osobám.

[84] Článok 4 bod 1 všeobecného nariadenia o ochrane údajov: „‚osobné údaje' sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len ‚dotknutá osoba'); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby;"

umožniť identifikáciu tejto osoby, aj keď sa jej meno, adresa alebo iné jednoznačné identifikátory vynechajú.

87. Platí to najmä vtedy, keď sa údaje týkajú využívania informačných služieb (čas prístupu, postupnosť prístupu k funkciám, charakteristika použitého zariadenia atď.). Tieto služby by mohli byť rovnako ako v prípade dovozcu osobných údajov povinné poskytnúť prístup tým istým orgánom verejnej moci v ich jurisdikcii, ktoré potom pravdepodobne budú mať k dispozícii údaje o využívaní týchto informačných služieb osobami, na ktoré sa zameriavajú.

88. Okrem toho, vzhľadom na to, že využívanie niektorých informačných služieb je vo svojej podstate verejné, alebo vzhľadom na ich využiteľnosť subjektmi so značnými zdrojmi, prevádzkovatelia budú musieť byť obzvlášť obozretní, keďže orgány verejnej moci v ich jurisdikcii majú pravdepodobne k dispozícii údaje o využívaní informačných služieb osobou, na ktorú sa zameriavajú.

89. Ak sa v priebehu uskutočňovania pseudonymizácie atribúty obsiahnuté v osobných údajoch transformujú pomocou kryptografického algoritmu, platí usmernenie v poznámkach pod čiarou 80 a 81. Do budúcnosti sa odporúča vzdať sa výhradného používania kryptografie a uplatňovať transformácie na základe mechanizmov vyhľadávania v tabuľke.

Prípad použitia 3: Šifrovanie údajov na účely ich ochrany pred prístupom orgánov verejnej moci tretej krajiny dovozcu pri ich prenose medzi vývozcom a jeho dovozcom

90. Vývozca údajov chce preniesť údaje na miesto určenia, ktorého právne predpisy a/alebo postupy umožňujú orgánom verejnej moci prístup k údajom počas ich prenosu medzi krajinou vývozcu a krajinou určenia.

Ak

1. vývozca údajov prenáša osobné údaje k dovozcovi údajov v jurisdikcii, ktorej právne predpisy a/alebo postupy umožňujú orgánom verejnej moci prístup k údajom počas ich prenosu prostredníctvom internetu do tejto tretej krajiny bez európskych základných záruk týkajúcich sa týchto prístupov, použije sa šifrovanie prenosu, pri ktorom sa zabezpečí, aby použité šifrovacie protokoly boli najmodernejšie a poskytli účinnú ochranu pred aktívnymi a pasívnymi útokmi za pomoci zdrojov, o ktorých je známe, že nimi disponujú orgány verejnej moci tejto tretej krajiny,
2. strany zapojené do komunikácie sa dohodnú na dôveryhodnej certifikačnej autorite alebo infraštruktúre verejného kľúča;
3. proti aktívnym a pasívnym útokom na odosielacie a prijímacie systémy zabezpečujúce šifrovanie prenosu sa použijú špecifické ochranné a najmodernejšie opatrenia, vrátane testov softvérových zraniteľností a možných únikových ciest,
4. v prípade, že samotné šifrovanie prenosu neposkytuje primeranú bezpečnosť vzhľadom na skúsenosti so slabými miestami infraštruktúry alebo použitého softvéru, osobné údaje sa tiež šifrujú medzi koncovými bodmi na aplikačnej úrovni pomocou najmodernejších metód šifrovania;
5. šifrovací algoritmus a jeho parametre (napr. dĺžka kľúča, prípadný prevádzkový režim) zodpovedajú najnovším poznatkom a možno ich považovať za odolné voči kryptoanalýze vykonávanej orgánmi verejnej moci, keď sú údaje prenášané do tejto tretej krajiny s

prihliadnutím na zdroje a technické možnosti (napr. výpočtová kapacita pre útoky hrubou silou), ktoré majú k dispozícii (pozri poznámku pod čiarou 80 vyššie),[85]

6. intenzita šifrovania zohľadňuje konkrétne časové obdobie, počas ktorého sa musí zachovať dôvernosť šifrovaných osobných údajov;
7. šifrovací algoritmus je vykonaný správne a prostredníctvom riadne udržiavaného softvéru bez známych zraniteľností, ktorého súlad so špecifikáciou zvoleného algoritmu bol overený, napr. certifikáciou,
8. kľúče sú spoľahlivo riadené (vytvorené, spravované, uložené, prípadne prepojené s totožnosťou zamýšľaného príjemcu a zrušené) vývozcom alebo subjektom, ktorému vývozca dôveruje v rámci jurisdikcie poskytujúcej v podstate rovnocennú úroveň ochrany;

potom sa EDPB domnieva, že šifrovanie prenosu, príp. v kombinácii so šifrovaním obsahu medzi koncovými bodmi, predstavuje účinné dodatočné opatrenie.

Prípad použitia 4: Chránený príjemca

91. Vývozca údajov prenáša osobné údaje dovozcovi údajov v tretej krajine, ktorý je osobitne chránený právnymi predpismi danej krajiny, napr. na účely spoločného poskytovania lekárskeho ošetrenia pacientovi alebo právnych služieb klientovi.

Ak

1. právne predpisy tretej krajiny oslobodzujú tuzemského dovozcu údajov od potenciálne neoprávneného prístupu k údajom, ktoré tento príjemca uchováva na daný účel, napr. na základe povinnosti zachovávať služobné tajomstvo, ktorá sa vzťahuje na dovozcu údajov;
2. sa táto výnimka vzťahuje na všetky informácie, ktoré má príjemca údajov k dispozícii a ktoré možno použiť na obchádzanie ochrany dôverných informácií (kryptografické kľúče, heslá, iné prihlasovacie údaje atď.);
3. dovozca údajov nevyužíva služby sprostredkovateľa spôsobom, ktorý by orgánom verejnej správy umožňoval prístup k údajom, ktoré má sprostredkovateľ k dispozícii, a dovozca údajov ani nepostúpi údaje inému subjektu, ktorý nie je chránený, na základe nástrojov na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov;
4. osobné údaje sa pred prenosom zašifrujú čo najmodernejšou metódou, ktorá zaručuje, že dešifrovanie nebude možné bez dešifrovacieho kľúča (šifrovanie medzi koncovými bodmi) [end-to-end encryption] počas celého obdobia, počas ktorého je potrebné údaje chrániť;
5. dešifrovací kľúč je vo výhradnej úschove dovozcu chránených údajov a prípadne samotného vývozcu alebo iného subjektu, ktorému vývozca dôveruje a ktorý sa nachádza v EHP alebo v jurisdikcii, ktorá ponúka v podstate rovnocennú úroveň ochrany, aká je zaručená v EHP, a primerane zabezpečený proti neoprávnenému použitiu alebo poskytnutiu prostredníctvom technických a organizačných opatrení zodpovedajúcich najnovším poznatkom a
6. vývozca údajov spoľahlivo určil, že šifrovací kľúč, ktorý zamýšľa použiť, zodpovedá dešifrovaciemu kľúču, ktorý má príjemca k dispozícii;

potom sa EDPB domnieva, že vykonané šifrovanie prenosu predstavuje účinné dodatočné opatrenie.

[85] Pozri poznámku pod čiarou 80, pokiaľ ide o niektoré odkazy na technické usmernenia uverejnené oficiálnymi orgánmi EÚ a jej členských štátov pre kybernetickú bezpečnosť.

Prípad použitia 5: Oddelené spracúvanie alebo spracúvanie viacerými stranami

92. Vývozca údajov chce, aby osobné údaje spracúvali spoločne dvaja alebo viacerí nezávislí sprostredkovatelia, ktorí sa nachádzajú v rôznych jurisdikciách bez toho, aby im poskytol obsah údajov. Pred poskytnutím údajov rozdelí údaje takým spôsobom, aby žiadna časť prijatá jednotlivým sprostredkovateľom nestačila na úplnú alebo čiastočnú rekonštrukciu osobných údajov. Vývozca údajov získa výsledok spracúvania od každého sprostredkovateľa nezávisle a získané časti zlučuje, aby dospel ku konečnému výsledku, ktorý môže predstavovať osobné alebo agregované údaje.

Ak

1. vývozca údajov spracúva osobné údaje takým spôsobom, že sú rozdelené na dve alebo viac častí, ktoré už nie je možné vykladať alebo priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií;
2. každá z častí sa prenesie samostatnému sprostredkovateľovi, ktorý sa nachádza v inej jurisdikcii;
3. sprostredkovatelia dobrovoľne spracúvajú údaje spoločne, napr. pomocou bezpečného výpočtu viacerých strán takým spôsobom, aby žiadnej z nich neboli poskytnuté informácie, ktoré nemajú pred výpočtom;
4. algoritmus použitý pri spoločnom výpočte je zabezpečený proti aktívnym protivníkom;
5. prevádzkovateľ na základe dôkladnej analýzy príslušných údajov a so zohľadnením chýbajúcich častí informácií, ktoré môžu mať orgány verejnej moci prijímajúcej krajiny k dispozícii a použiť, zistil, že časti osobných údajov, ktoré poskytuje sprostredkovateľom, nemožno priradiť k identifikovanej alebo identifikovateľnej fyzickej osobe, a to ani v prípade, že také informácie sú uvedené krížovým odkazom;
6. neexistuje dôkaz o spolupráci medzi orgánmi verejnej moci so sídlom v príslušných jurisdikciách, v ktorých sa nachádza každý zo sprostredkovateľov, čo by im umožnilo prístup ku všetkým súborom osobných údajov, ktoré majú sprostredkovatelia, ako aj rekonštrukciu a využitie obsahu osobných údajov v nezašifrovanom formáte za okolností, keď by takéto využívanie nerešpektovalo podstatu základných práv a slobôd dotknutých osôb. Podobne by orgány verejnej moci žiadnej z týchto krajín nemali mať právomoc na prístup k osobným údajom, ktoré majú k dispozícii sprostredkovatelia vo všetkých dotknutých jurisdikciách;

potom sa EDPB domnieva, že vykonané oddelené spracúvanie predstavuje účinné dodatočné opatrenie.

Príklady scenárov odkazujúcich na prípady, v ktorých nie sú identifikované *účinné* opatrenia

93. Opatrenia opísané v niektorých z ďalej uvedených scenárov by neboli účinné pri zabezpečovaní v podstate rovnocennej úrovne ochrany údajov prenášaných do tretej krajiny. Preto by sa nepovažovali za vhodné dodatočné opatrenia.

Prípad použitia 6: Prenos poskytovateľom cloudových služieb alebo iným sprostredkovateľom, ktorí potrebujú prístup k nešifrovaným údajom

94. Vývozca údajov prenáša osobné údaje či už elektronickým poskytnutím alebo ich sprístupnením poskytovateľovi cloudových služieb alebo inému sprostredkovateľovi, aby osobné údaje spracúval podľa jeho pokynov v tretej krajine (napr. za poskytnutia technickej podpory alebo akéhokoľvek druhu cloudového spracúvania) a tieto údaje nie sú – alebo nemôžu byť – pseudonymizované, ako je opísané v Prípade použitia 2, alebo šifrované, ako je opísané v Prípade použitia 1, pretože spracúvanie si vyžaduje prístup k nešifrovaným údajom,

Ak

1. prevádzkovateľ prenáša údaje poskytovateľovi cloudových služieb alebo inému sprostredkovateľovi;
2. poskytovateľ cloudových služieb alebo iný sprostredkovateľ potrebuje prístup k nešifrovaným údajom, aby mohol vykonať pridelenú úlohu; a
3. právomoc udelená orgánom verejnej moci prijímajúcej krajiny na prístup k predmetným prenášaným údajom presahuje rámec toho, čo je nevyhnutné a primerané v demokratickej spoločnosti, keďže na predmetné prenosy sa v praxi vzťahujú problematické právne predpisy tretej krajiny (pozri krok 3).[86]

EDPB nie je teda vzhľadom na súčasný stav poznatkov schopný navrhnúť účinné technické opatrenie, ktoré by pri takom prístupe zabránilo porušovaniu základných práv dotknutých osôb. EDPB nevylučuje, že ďalší technologický vývoj môže priniesť opatrenia na dosiahnutie zamýšľaného obchodného účelu bez toho, aby sa vyžadoval prístup k nešifrovaným údajom.

95. V uvedených scenároch, keď sú nešifrované osobné údaje technicky nevyhnutné na poskytovanie služby sprostredkovateľom, nepredstavuje šifrovanie prenosu a šifrovanie údajov na úložisku [data-at-rest] ani spolu dodatočné opatrenie, ktorým sa zabezpečuje v podstate rovnocenná úroveň ochrany, ak má dovozca údajov k dispozícii kryptografické kľúče.

Prípad použitia 7: Prenos osobných údajov na obchodné účely, a to aj prostredníctvom vzdialeného prístupu

96. Vývozca údajov prenáša osobné údaje subjektom – v tretej krajine, aby sa použili na spoločné obchodné účely – či už elektronickým poskytnutím alebo ich sprístupnením pre diaľkový prístup dovozcu údajov – a tieto údaje nie sú – alebo nemôžu byť – pseudonymizované, ako je opísané v Prípade použitia 2, alebo zašifrované, ako je opísané v Prípade použitia 1, pretože spracúvanie si vyžaduje prístup k nešifrovaným údajom. Typická konštelácia môže pozostávať z prevádzkovateľa alebo sprostredkovateľa usadeného na území členského štátu, ktorý prenáša osobné údaje prevádzkovateľovi alebo sprostredkovateľovi v tretej krajine patriacej do tej istej skupiny podnikov alebo skupiny podnikov zapojených do spoločnej hospodárskej činnosti. Dovozca údajov môže napríklad použiť údaje, ktoré získa, na poskytovanie personálnych služieb vývozcovi údajov, pričom potrebuje údaje o ľudských zdrojoch, alebo na telefonickú či e-mailovú komunikáciu so zákazníkmi vývozcu údajov, ktorí žijú v Európskej únii.

[86] Pozri články 47 a 52 Charty základných práv Európskej únie, článok 23 ods. 1 všeobecného nariadenia o ochrane údajov a odporúčania EDPB 02/2020 o európskych základných zárukách pre opatrenia týkajúce sa sledovania, 10. novembra 2020.**Error! Hyperlink reference not valid.**

Ak

1. vývozca údajov prenáša osobné údaje dovozcovi údajov v tretej krajine tak, že ich sprístupňuje v bežne používanom informačnom systéme spôsobom, ktorý dovozcovi umožňuje priamy prístup k údajom podľa vlastného výberu, alebo ich prenáša priamo, jednotlivo alebo hromadným spôsobom prostredníctvom komunikačnej služby;
2. dovozca[87] spracúva nešifrované údaje v tretej krajine (aj pre vlastné účely, ak je dovozca prevádzkovateľom),
3. právomoc udelená orgánom verejnej moci prijímajúcej krajiny na prístup k prenášaným údajom presahuje rámec toho, čo je nevyhnutné a primerané v demokratickej spoločnosti, keďže v praxi sa na predmetné prenosy vzťahujú problematické právne predpisy tretej krajiny (pozri krok 3),

EDPB si teda nevie predstaviť účinné technické opatrenie, ktoré by pri takom prístupe zabránilo porušovaniu základných práv dotknutých osôb.

97. V uvedených scenároch, keď sú nešifrované osobné údaje technicky nevyhnutné na poskytovanie služby sprostredkovateľom, nepredstavuje šifrovanie prenosu a šifrovanie údajov na úložisku ani spolu dodatočné opatrenie, ktorým sa zabezpečuje v podstate rovnocenná úroveň ochrany, ak má dovozca údajov k dispozícii kryptografické kľúče.

2.2 Dodatočné zmluvné opatrenia

98. Tieto opatrenia budú vo všeobecnosti pozostávať z jednostranných, dvojstranných alebo mnohostranných[88] zmluvných záväzkov.[89] Ak sa použije nástroj na prenos údajov podľa článku 46 všeobecného nariadenia o ochrane údajov, vo väčšine prípadov už obsahuje niekoľko (väčšinou zmluvných) záväzkov zo strany vývozcu údajov a dovozcu údajov, ktorých cieľom je slúžiť ako záruka pre osobné údaje.[90]

99. V niektorých situáciách môžu tieto opatrenia dopĺňať a posilňovať záruky poskytované nástrojom na prenos a príslušnými právnymi predpismi tretej krajiny, ak vzhľadom na okolnosti prenosu tieto nespĺňajú všetky podmienky požadované na zabezpečenie úrovne ochrany, ktorá je v podstate rovnocenná úrovni zaručenej v rámci EÚ. Vzhľadom na povahu zmluvných opatrení, ktoré vo všeobecnosti nie sú spôsobilé zaviazať orgány tejto tretej krajiny, pokiaľ nie sú zmluvnou stranou[91], by sa tieto opatrenia mali kombinovať s ďalšími technickými a organizačnými opatreniami na poskytnutie požadovanej úrovne ochrany údajov. Výber a vykonávanie jedného

[87] Či už ide o prevádzkovateľa alebo sprostredkovateľa v tretej krajine, ktorý prijíma osobné údaje prenášané z EHP alebo k nim získava prístup.
[88] Napr. v rámci záväzných vnútropodnikových pravidiel, ktoré by mali v každom prípade regulovať niektoré z ďalej uvedených opatrení.
[89] Budú súkromného charakteru a nebudú sa považovať za medzinárodné dohody podľa medzinárodného práva verejného. Zvyčajne taktiež nezaväzujú orgán verejnej moci tretej krajiny ako stranu, ktorá nie je zmluvnou stranou zmluvy uzatvorenej so súkromnými subjektmi v tretích krajinách, ako zdôraznil Súdny dvor vo svojom rozsudku C-311/18 (Schrems II), bod 125.
[90] Pozri rozsudok vo veci C-311/18 (Schrems II), bod 137, v ktorom Súdny dvor v dôsledku toho uznal, že štandardné zmluvné doložky obsahujú „účinné mechanizmy, ktoré v praxi umožňujú zabezpečiť, aby bola dodržaná úroveň ochrany vyžadovaná právom Únie a aby sa prenosy osobných údajov založené na takýchto doložkách v prípade ich porušenia alebo nemožnosti ich dodržať pozastavili alebo zakázali“ (pozri tiež bod 148).
[91] C-311/18 (Schrems II), bod 125.

alebo viacerých z týchto opatrení nemusí nevyhnutne a systematicky zabezpečiť, že váš prenos spĺňa štandard v podstate rovnocennej úrovne ochrany, ktorý vyžaduje právo Únie.

100. V závislosti od toho, aké zmluvné opatrenia sú už zahrnuté do zvoleného nástroja na prenos údajov podľa článku 46 všeobecného nariadenia o ochrane údajov, môžu byť užitočné aj dodatočné zmluvné opatrenia, aby sa vývozcovia údajov so sídlom v EHP dozvedeli o novom vývoji, ktorý má vplyv na ochranu údajov prenášaných do tretích krajín.

101. Ako už bolo uvedené, zmluvné opatrenia nebudú môcť vylúčiť uplatňovanie právnych predpisov tretej krajiny, ktorá nespĺňa štandard EDPB pokiaľ ide o európske základne záruky, v prípadoch, keď právne predpisy ukladajú dovozcom povinnosť dodržiavať príkazy na poskytnutie údajov, ktoré dostávajú od orgánov verejnej moci.[92]

102. Niektoré príklady týchto potenciálnych zmluvných opatrení sú uvedené v ďalšom texte a rozčlenené podľa ich charakteru:

Opatrenie, ktorým sa stanovuje zmluvná povinnosť používať osobitné technické opatrenia

103. V závislosti od konkrétnych okolností prenosov (vrátane praktického uplatňovania právnych predpisov tretej krajiny) môže byť potrebné, aby sa v zmluve stanovilo, že uskutočňovanie prenosov si vyžaduje prijatie osobitných technických opatrení (pozri vyššie navrhované technické opatrenia).

104. Podmienky účinnosti:

- Táto doložka by mohla byť účinná v situáciách, keď vývozca identifikoval potrebu technických opatrení. Vyžadovalo by si to právnu formu, aby sa zabezpečilo, že aj dovozca sa v prípade potreby zaviaže zaviesť potrebné technické opatrenia.

Povinnosti týkajúce sa transparentnosti:

105. Vývozca by mohol k zmluve doplniť prílohy s informáciami, ktoré by dovozca pri vynaložení maximálneho úsilia poskytol pred uzavretím zmluvy, o prístupe orgánov verejnej moci k údajom v krajine určenia, vrátane oblasti spravodajských informácií za predpokladu, že právne predpisy sú v súlade s európskymi základnými zárukami EDPB. To by vývozcovi údajov mohlo pomôcť splniť jeho povinnosť zdokumentovať posúdenie úrovne ochrany v tretej krajine. Môže tiež zdôrazniť povinnosť dovozcu pomáhať vývozcovi pri jeho posúdení a byť zodpovedný za poskytovanie informácií, ktoré sú objektívne, spoľahlivé, relevantné, overiteľné a verejne dostupné alebo inak prístupné.

106. Od dovozcu by sa napríklad mohlo vyžadovať:

(1) vymenovanie zákonov a iných právnych predpisov krajiny určenia, ktoré sa vzťahujú na dovozcu alebo jeho (ďalších) sprostredkovateľov, ktoré by orgánom verejnej moci umožnili prístup k osobným údajom, ktoré sú predmetom prenosu, najmä v oblastiach spravodajských informácií, presadzovania práva, administratívneho a regulačného dohľadu, vo vzťahu k prenášaným údajom;

---

[92] Rozsudok SDEÚ vo veci C-311/18 (Schrems II), bod 132.

(2) ak neexistujú právne predpisy upravujúce prístup orgánov verejnej moci k údajom, poskytnutie informácií a štatistík na základe skúseností dovozcu alebo správ z rôznych zdrojov (napr. partnerov, otvorených zdrojov, vnútroštátnej judikatúry a rozhodnutí orgánov dohľadu) o prístupe orgánov verejnej moci k osobným údajom v situáciách podobných danému prenosu údajov (t. j. v konkrétnej regulačnej oblasti; o druhu subjektov, ku ktorým dovozca údajov patrí;...) atď.;

(3) uvedenie, aké opatrenia sa príp. prijímajú na zabránenie prístupu k prenášaným údajom;

(4) poskytnutie dostatočne podrobných informácií o všetkých žiadostiach orgánov verejnej moci o prístup k osobným údajom, ktoré dovozca prijal počas určitého obdobia[93], najmä v oblastiach uvedených v bode 1, a uvedenie informácií o prijatých žiadostiach, požadovaných údajoch, žiadajúcom orgáne a právnom základe pre poskytnutie údajov a v akom rozsahu dovozca žiadosti o údaje vyhovel;[94]

(5) uvedenie, či a do akej miery dovozcovi bránia právne predpisy poskytovať informácie uvedené v bodoch 1 až 5.

107. Tieto informácie by sa mohli poskytovať formou štruktúrovaných dotazníkov, ktoré by dovozca vyplnil, podpísal a boli by doplnené o zmluvnú povinnosť dovozcu oznámiť v stanovenej lehote akúkoľvek prípadnú zmenu týchto informácií, ako je to v súčasnosti v prípade postupov náležitej starostlivosti [due diligence].

108. Podmienky účinnosti:

- Dovozca musí byť schopný poskytnúť vývozcovi tieto druhy informácií podľa svojho najlepšieho vedomia a pri vynaložení maximálneho úsilia na ich získanie.
- Táto povinnosť uložená dovozcovi je prostriedkom na zabezpečenie toho, aby si vývozca bol a zostal vedomý rizík spojených s prenosom údajov do tretej krajiny. Vývozcovi to umožní upustiť od uzavretia zmluvy, alebo ak sa informácie zmenia po jej uzavretí, splniť si povinnosť pozastaviť prenos a/alebo vypovedať zmluvu, ak právne predpisy tretej krajiny, použité záruky uvedené v článku 46 všeobecného nariadenia o ochrane údajov a akékoľvek ďalšie záruky, ktoré mohol prijať, už nemôžu zabezpečiť úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany v EHP. Táto povinnosť však nemôže byť dôvodom na to, aby dovozca poskytol osobné údaje, ani sa na jej základe nemôže očakávať, že nebudú predložené žiadne ďalšie žiadosti o prístup [access requests].

***

109. Vývozca by tiež mohol doplniť doložky, ktorými dovozca osvedčuje, že 1) zámerne nevytvoril zadné dvierka [back doors] alebo podobné prvky programovania, ktoré by sa mohli použiť na prístup do systému a/alebo k osobným údajom; 2) úmyselne nevytvoril ani nezmenil svoje obchodné postupy spôsobom, ktorý by uľahčil prístup k osobným údajom alebo systémom; a 3)

[93] Dĺžka obdobia by mala závisieť od rizika pre práva a slobody dotknutých osôb, ktorých údaje sú predmetom predmetného prenosu – napr. posledný rok pred uzatvorením nástroja na prenos údajov s vývozcom údajov.
[94] Splnenie tejto povinnosti samo osebe nepredstavuje poskytnutie primeranej úrovne ochrany. Zároveň si akékoľvek nevhodné poskytnutie, ku ktorému skutočne došlo, vyžaduje zavedenie dodatočných opatrení.

že vnútroštátne právo alebo vládna politika nevyžaduje, aby dovozca vytvoril alebo udržiaval zadné dvierka alebo aby uľahčil prístup k osobným údajom alebo systémom, alebo aby dovozca vlastnil alebo odovzdal šifrovací kľúč.[95]

110. Podmienky účinnosti:

- Existencia právnych predpisov alebo vládnych politík, ktoré bránia dovozcom poskytovať tieto informácie, môže viesť k neúčinnosti tejto doložky. Dovozca teda nebude môcť uzavrieť zmluvu alebo bude musieť vývozcovi oznámiť, že nie je schopný pokračovať v plnení svojich zmluvných záväzkov.
- Zmluva musí obsahovať sankcie a/alebo možnosť vývozcu v krátkom čase vypovedať zmluvu v prípadoch, keď dovozca neinformuje o existencii zadných dvierok alebo podobných programovacích alebo manipulovaných obchodných postupov, alebo akúkoľvek požiadavku na zavedenie niektorého z týchto prvkov, alebo ak okamžite neinformuje vývozcu, hneď ako sa dozvie o ich existencii.
- Za okolností, keď dovozca údajov poskytol prenesené osobné údaje v rozpore so záväzkami obsiahnutými v rámci vybraného nástroja na prenos, môže zmluva zahŕňať aj odškodnenie dotknutej osoby zo strany dovozcu údajov za akúkoľvek spôsobenú materiálnu a nemateriálnu ujmu.

***

111. Vývozca by mohol posilniť svoju právomoc vykonávať audity[96] alebo kontroly zariadení na spracúvanie údajov dovozcu na mieste a/alebo na diaľku s cieľom overiť, či sa údaje poskytol orgánom verejnej moci a za akých podmienok (prístup nie nad rámec toho, čo je nevyhnutné a primerané v demokratickej spoločnosti), napríklad stanovením krátkej lehoty a mechanizmov zabezpečujúcich rýchly zásah kontrolných orgánov a posilnením autonómie vývozcu pri výbere kontrolných orgánov.

112. Podmienky účinnosti:

- Rozsah auditu by sa mal z právneho a technického hľadiska vzťahovať na každé spracúvanie osobných údajov prenášaných v tretej krajine sprostredkovateľmi alebo ďalšími sprostredkovateľmi dovozcu, aby bol plne účinný.
- Záznamy o prístupe a iné podobné záznamy by mali byť odolné voči falšovaniu (napr. mali by byť nezmeniteľné pomocou najmodernejších techník šifrovania, akými je hašovanie, a tiež by sa mali pravidelne odosielať vývozcovi), aby audítori mohli nájsť dôkazy o poskytnutí. V záznamoch o prístupe a iných podobných záznamoch by sa tiež malo rozlišovať medzi prístupmi z dôvodu bežných obchodných operácií a prístupmi z dôvodu príkazov alebo žiadostí o prístup.

[95] Táto doložka je dôležitá na zaručenie primeranej úrovne ochrany prenášaných osobných údajov a zvyčajne by sa mala vyžadovať.

[96] Pozri napríklad doložku 5 písm. f) štandardných zmluvných doložiek medzi prevádzkovateľmi a spracovateľmi rozhodnutia 2010/87/EÚ, audity by sa mohli vykonávať aj v rámci kódexu správania alebo certifikácie.

***

113. Ak sa pôvodne posúdili právne predpisy a postupy tretej krajiny dovozcu a dospelo sa k záveru, že poskytujú úroveň ochrany v podstate rovnocennú s úrovňou, aká sa poskytuje v EÚ pri údajoch prenášaných vývozcom, vývozca by mohol ešte posilniť povinnosť dovozcu údajov bezodkladne informovať vývozcu údajov v prípade zmeny situácie o tom, že nie je schopný splniť zmluvné záväzky a v dôsledku toho dodržať požadovaný štandard „v podstate rovnocennej úrovne ochrany údajov“.[97]

114. Táto neschopnosť splniť záväzky môže vyplývať zo zmien v právnych predpisoch alebo postupoch tretej krajiny.[98] V týchto doložkách by sa mohli stanoviť konkrétne a prísne lehoty a postupy na rýchle pozastavenie prenosu údajov a/alebo vypovedanie zmluvy a vrátenie alebo vymazanie získaných údajov zo strany dovozcu. Sledovanie prijatých žiadostí, ich rozsahu a účinnosti opatrení prijatých v reakcii na ne by malo vývozcovi poskytnúť dostatočné informácie na výkon jeho povinnosti pozastaviť alebo ukončiť prenos a/alebo vypovedať zmluvu.

115. Podmienky účinnosti:

- Oznámenie sa musí uskutočniť pred udelením prístupu k údajom. V opačnom prípade v čase, keď vývozca dostane oznámenie, práva jednotlivca už mohli byť porušené, ak sa žiadosť zakladá na právnych predpisoch tejto tretej krajiny, ktoré presahujú povolenú úroveň ochrany údajov poskytovanú podľa právnych predpisov EÚ. Oznámenie môže slúžiť aj na predchádzanie budúcim porušeniam a na to, aby vývozca mohol plniť svoju povinnosť pozastaviť prenos osobných údajov do tretej krajiny a/alebo vypovedať zmluvu.
- Dovozca údajov musí monitorovať akýkoľvek právny alebo politický vývoj, ktorý by mohol viesť k tomu, že nebude schopný plniť svoje povinnosti, a bezodkladne informovať vývozcu údajov o všetkých takýchto zmenách a vývoji, a ak je to možné, ešte pred ich vykonaním, aby sa vývozcovi údajov umožnilo získať späť údaje od dovozcu údajov.
- V doložkách by sa mal stanoviť rýchly mechanizmus, prostredníctvom ktorého vývozca údajov povolí dovozcovi údajov urýchlene zabezpečiť alebo vrátiť údaje vývozcovi údajov, alebo ak to nie je možné, vymazať alebo bezpečne zašifrovať údaje bez toho, aby nevyhnutne čakal na pokyny vývozcu, ak bolo splnené určité konkrétne kritérium[99], na ktorom sa vývozca údajov dohodne s dovozcom údajov. Dovozca by mal zaviesť tento mechanizmus od začiatku prenosu údajov a pravidelne ho testovať, aby sa zabezpečilo jeho uplatňovanie v krátkom čase.
- Ďalšie doložky by mohli vývozcovi umožniť monitorovať dodržiavanie týchto povinností dovozcom prostredníctvom auditov, kontrol a iných overovacích opatrení a presadzovať ich

[97] Doložka 5 písm. a) a doložka 5 písm. d) bod i) rozhodnutia o štandardných zmluvných doložkách 2010/87/EÚ.

[98] Pozri C-311/18 (Schrems II), bod 139, v ktorom Súdny dvor tvrdí, že „hoci samotná doložka 5 písm. d) bod i) umožňuje príjemcovi prenosu osobných údajov v prípade právnych predpisov, ktoré takýto postup odôvodňujú, akým je zákaz trestnoprávnej povahy v záujme zachovania dôvernosti vyšetrovania v rámci presadzovania práva, neoznámiť prevádzkovateľovi usadenému v Únii, že orgán presadzovania práva podal právne záväznú žiadosť na sprístupnenie osobných údajov, v súlade s doložkou 5 písm. a) prílohy rozhodnutia 2010/87 je prinajmenšom povinný prevádzkovateľa informovať, že nemôže zabezpečiť dodržiavanie štandardných doložiek o ochrane údajov.“

[99] Toto kritérium by malo zabezpečiť, aby sa dotknutým osobám naďalej poskytovala úroveň ochrany rovnocenná s úrovňou zaručenou v EHP.

prostredníctvom sankcií voči dovozcovi a/alebo schopnosti vývozcu pozastaviť prenos a/alebo okamžite vypovedať zmluvu.

***

116. Pokiaľ to umožňujú vnútroštátne právne predpisy tretej krajiny, zmluva by mohla posilniť povinnosti dovozcu týkajúce sa transparentnosti využitím metódy „pravidelné automatické potvrdenia“ [warrant canary], v rámci ktorej sa dovozca zaväzuje pravidelne uverejňovať (napr. aspoň raz za 24 hodín) kryptograficky podpísanú správu informujúcu vývozcu, že k určitému dátumu a času dovozca nedostal žiadny príkaz na poskytnutie osobných údajov či podobné príkazy. Ak nedôjde k aktualizácii tohto oznámenia, vývozcovi tým bude oznámené, že dovozca mohol takýto príkaz dostať.

117. Podmienky účinnosti:

- Predpisy tretej krajiny musia umožniť dovozcovi údajov vydať takýto druh pasívneho oznámenia vývozcovi.
- Vývozca údajov musí automaticky monitorovať pravidelné automatické potvrdenia.
- Dovozca údajov musí zabezpečiť, aby jeho súkromný kľúč na podpis pravidelného automatického potvrdenia bol bezpečný a aby nemohol byť na základe právnych predpisov tretej krajiny nútený vydávať nepravdivé pravidelné automatické potvrdenia. Na tento účel by mohlo byť vhodné, ak by boli potrebné viaceré podpisy rôznych osôb a/alebo ak by pravidelné automatické potvrdenia vydávala osoba mimo jurisdikcie tretej krajiny.

Povinnosť prijať konkrétne opatrenia

118. Dovozca by sa mohol zaviazať, že podľa práva krajiny určenia preskúma zákonnosť akéhokoľvek príkazu na poskytnutie údajov, najmä či je v rámci právomocí udelených žiadajúcemu orgánu verejnej moci, a že príkaz napadne, ak po dôkladnom posúdení dospeje k záveru, že podľa právnych predpisov krajiny určenia na to existujú dôvody. Pri napadnutí príkazu by mal dovozca údajov požiadať o predbežné opatrenia na pozastavenie účinkov príkazu dovtedy, kým súd nerozhodne vo veci samej. Dovozca by mal povinnosť neposkytnúť požadované osobné údaje dovtedy, kým sa to nebude vyžadovať podľa uplatniteľných procesných pravidiel. Dovozca údajov by sa tiež zaviazal, že pri odpovedi na príkaz poskytne minimálne prípustné množstvo informácií, a to na základe primeraného výkladu tohto príkazu.

119. Podmienky účinnosti:

- Právny poriadok tretej krajiny musí poskytovať účinné právne prostriedky na napadnutie príkazov na poskytnutie údajov.
- Táto doložka bude vždy poskytovať veľmi obmedzenú dodatočnú ochranu, keďže príkaz na poskytnutie údajov môže byť zákonný podľa právneho poriadku tretej krajiny, ale tento právny poriadok nemusí spĺňať normy EÚ. Toto zmluvné opatrenie budú musieť nevyhnutne dopĺňať iné dodatočné opatrenia.
- Napadnutie príkazov musí mať odkladný účinok podľa práva tretej krajiny. V opačnom prípade by orgány verejnej moci mali stále prístup k údajom jednotlivcov a akékoľvek následné opatrenie v prospech jednotlivca by malo obmedzený účinok, ktorý by mu umožnil požadovať náhradu škody za negatívne dôsledky vyplývajúce z poskytnutia údajov.

- Dovozca bude musieť byť schopný zdokumentovať a preukázať vývozcovi opatrenia, ktoré pri vynaložení svojho maximálneho úsilia prijal na splnenie tohto záväzku.

***

120. V rovnakej situácii, ako je opísané vyššie, by sa dovozca mohol zaviazať, že bude informovať žiadajúci orgán verejnej moci o nezlučiteľnosti príkazu so zárukami obsiahnutými v nástroji na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov[100] a o konflikte povinností dovozcu, ktorý z toho vyplýva. Dovozca by to súčasne a čo najskôr oznámil vývozcovi a/alebo príslušnému dozornému orgánu v rámci EHP, pokiaľ je to možné podľa právneho poriadku tretej krajiny.

121. Podmienky účinnosti:

- Takéto informácie o ochrane poskytovanej právom Únie a konflikt povinností by mali v právnom poriadku tretej krajiny viesť k určitému právnemu účinku, ako je súdne alebo správne preskúmanie príkazu alebo žiadosti o prístup, požiadavka súdneho príkazu a/alebo dočasné pozastavenie príkazu s cieľom poskytnúť údajom určitú ochranu.
- Právny systém krajiny nesmie brániť dovozcovi v tom, aby upovedomil vývozcu alebo aspoň príslušný dozorný orgán z EHP o prijatom príkaze alebo žiadosti o prístup.
- Dovozca bude musieť byť schopný zdokumentovať a preukázať vývozcovi opatrenia, ktoré pri vynaložení svojho maximálneho úsilia prijal na splnenie tohto záväzku.

Posilnenie postavenia dotknutých osôb za účelom uplatňovania ich práv

122. V zmluve by sa mohlo stanoviť, že k osobným údajom prenášaným v nešifrovanom formáte v bežnom obchodnom styku (vrátane prípadov poskytovania podpory) možno získavať prístup len s výslovným alebo implicitným súhlasom vývozcu a/alebo dotknutej osoby v prípade špecifického prístupu k údajom.

123. Podmienky účinnosti:

- Táto doložka by mohla byť účinná v situáciách, keď dovozcovia dostanú od orgánov verejnej moci žiadosti o dobrovoľnú spoluprácu, na rozdiel napríklad od prístupu orgánov verejnej moci k údajom, ku ktorému dochádza bez vedomia dovozcu údajov alebo proti jeho vôli.
- V niektorých situáciách dotknutá osoba nemusí byť schopná namietať proti prístupu alebo dať súhlas, ktorý spĺňa všetky podmienky stanovené v právnych predpisoch EÚ (slobodne daný, konkrétny, informovaný a jednoznačný) (napr. v prípade zamestnancov)[101].
- Vnútroštátne predpisy alebo politiky, ktoré ukladajú dovozcovi povinnosť neposkytnúť príkaz, ktorým sa požaduje prístup, môžu spôsobiť neúčinnosť tejto doložky, pokiaľ nie je možné ju

[100] V štandardných zmluvných doložkách sa napríklad stanovuje, že spracúvanie údajov vrátane ich prenosu sa vykonávalo a bude sa naďalej vykonávať v súlade s *„príslušným právom týkajúcim sa ochrany údajov“*. Toto právo je vymedzené ako *„právne predpisy chrániace základné práva a slobody jednotlivcov a najmä ich právo na súkromie vo vzťahu k spracovaniu osobných údajov, uplatniteľné na prevádzkovateľa údajov v členskom štáte, v ktorom je vývozca údajov usadený“*. SDEÚ potvrdzuje, že ustanovenia všeobecného nariadenia o ochrane údajov v spojení s Chartou základných práv Európskej únie sú súčasťou týchto právnych predpisov, pozri rozsudok SDEÚ C-311/18 (Schrems II), bod 138.

[101] Článok 4 bod 11 všeobecného nariadenia o ochrane údajov.

podporiť technickými metódami, ktoré vyžadujú, zásah vývozcu alebo dotknutej osoby na sprístupnenie nešifrovaných údajov. O takýchto technických opatreniach na obmedzenie prístupu možno uvažovať najmä vtedy, ak sa prístup poskytuje len v osobitných prípadoch poskytovania podpory alebo služieb, ale samotné údaje sa uchovávajú v rámci EHP.

***

124. Zmluva by mohla zaväzovať dovozcu a/alebo vývozcu, aby okamžite informovali dotknutú osobu o žiadosti alebo príkaze, ktoré dostali od orgánov verejnej moci tretej krajiny, alebo o neschopnosti dovozcu splniť si zmluvné záväzky s cieľom umožniť dotknutej osobe vyhľadať informácie a domáhať sa účinného prostriedku nápravy (napr. podaním sťažnosti príslušnému dozornému a/alebo súdnemu orgánu a využitím svojej aktívnej legitimácie na súdoch tretej krajiny), vrátane odškodnenia zo strany dovozcu údajov za akúkoľvek materiálnu a nemateriálnu ujmu, ktorú utrpela v dôsledku poskytnutia svojich osobných údajov prenášaných v rámci zvoleného nástroja na prenos v rozpore so záväzkami, ktoré obsahuje zmluva.

125. Podmienky účinnosti:

- Toto oznámenie by mohlo upozorňovať dotknutú osobu na možný prístup orgánov verejnej moci v tretích krajinách k jej údajom. Mohlo by tak umožniť dotknutej osobe, aby si od vývozcov vyžiadala dodatočné informácie a podala sťažnosť svojmu príslušnému dozornému orgánu. Touto doložkou by sa mohli riešiť a kompenzovať aj niektoré ťažkosti, s ktorými sa jednotlivec môže stretnúť pri preukazovaní svojej aktívnej legitimácie (locus standi) na súdoch tretích krajín s cieľom napadnúť prístup orgánov verejnej moci k jeho údajom.
- Vnútroštátne predpisy a politiky môžu zabrániť takémuto oznámeniu dotknutej osobe. Vývozca a dovozca by sa však napriek tomu mohli zaviazať, že budú informovať dotknutú osobu hneď, ako sa zrušia obmedzenia týkajúce sa poskytovania údajov, a vynaložia maximálne úsilie na to, aby získali výnimku zo zákazu poskytnutia. Vývozca alebo príslušný dozorný orgán by mohol dotknutej osobe oznámiť aspoň pozastavenie alebo ukončenie prenosu jej osobných údajov z dôvodu neschopnosti dovozcu splniť svoje zmluvné záväzky v dôsledku prijatia žiadosti o prístup.

***

126. Zmluva by mohla zaväzovať vývozcu a dovozcu, aby dotknutej osobe pomáhali pri uplatňovaní jej práv v jurisdikcii tretej krajiny prostredníctvom mechanizmov nápravy ad hoc a právneho poradenstva.

127. Podmienky účinnosti

- Niektoré vnútroštátne predpisy neumožňujú dovozcovi údajov poskytnúť tento druh pomoci priamo dotknutým osobám, hoci môžu dovoliť dovozcovi údajov zabezpečiť túto pomoc pre dotknuté osoby.
- Vo vnútroštátnych právnych predpisoch a politikách sa môžu stanoviť podmienky, ktoré môžu ohroziť účinnosť stanovených mechanizmov nápravy ad hoc.
- Právne poradenstvo by dotknutej osobe mohlo pomôcť, najmä vzhľadom na to, aké zložité a nákladné môže pre ňu byť pochopenie právneho systému tretej krajiny a vykonávanie právnych krokov zo zahraničia, potenciálne v cudzom jazyku. Táto doložka však vždy poskytne obmedzenú dodatočnú ochranu, keďže poskytovanie pomoci a právneho poradenstva

dotknutým osobám nemôže samo osebe napraviť neschopnosť právneho poriadku tretej krajiny poskytnúť takú úroveň ochrany, ktorá je v podstate rovnocenná úrovni zaručenej v rámci EHP. Toto zmluvné opatrenie bude musieť nevyhnutne dopĺňať iné dodatočné opatrenia.
- Toto dodatočné opatrenie by bolo účinné len za predpokladu, že právo tretej krajiny umožňuje prostriedky nápravy na vnútroštátnych súdoch alebo ak existuje mechanizmus prostriedkov nápravy ad hoc, vrátane proti opatreniam týkajúcim sa sledovania.

2.3 Organizačné opatrenia

128. Dodatočné organizačné opatrenia môžu pozostávať z vnútorných politík, organizačných metód a noriem, ktoré by prevádzkovatelia a sprostredkovatelia mohli uplatňovať na seba a ukladať dovozcom údajov v tretích krajinách. Môžu prispieť k zabezpečeniu konzistentnosti ochrany osobných údajov počas celého cyklu spracúvania. Organizačné opatrenia môžu takisto zlepšiť informovanosť vývozcov o rizikách a pokusoch o získanie prístupu k údajom v tretích krajinách a ich schopnosť reagovať na ne. Výber a vykonávanie jedného alebo viacerých z týchto opatrení nemusí nevyhnutne a systematicky zabezpečiť, že váš prenos spĺňa štandard v podstate rovnocennej úrovne ochrany, ktorý vyžaduje právo Únie. V závislosti od konkrétnych okolností prenosu a vykonaného posúdenia právnych predpisov tretej krajiny sú potrebné organizačné opatrenia na doplnenie zmluvných a/alebo technických opatrení s cieľom zabezpečiť úroveň ochrany osobných údajov, ktorá je v podstate rovnocenná úrovni zaručenej v rámci EHP.

129. Posúdenie najvhodnejších opatrení sa musí vykonať v jednotlivých prípadoch s prihliadnutím na to, že prevádzkovatelia a sprostredkovatelia musia dodržiavať zásadu zodpovednosti. EDPB ďalej uvádza niekoľko príkladov organizačných opatrení, ktoré môžu vývozcovia zaviesť, hoci tento zoznam nie je úplný a do úvahy môžu prichádzať aj iné vhodné opatrenia:

Vnútorné politiky týkajúce sa správy prenosov, najmä pokiaľ ide o skupiny podnikov

130. Prijatie primeraných vnútorných politík s jasným rozdelením zodpovedností za prenos údajov, kanály nahlasovania a štandardné prevádzkové postupy pre prípady utajených alebo oficiálnych žiadostí orgánov verejnej moci o prístup k údajom. Najmä v prípade prenosov medzi skupinami podnikov môžu tieto politiky okrem iného zahŕňať stanovenie osobitného tímu zloženého z odborníkov v oblasti IT, na právne predpisy na ochranu údajov a súkromia, aby sa zaoberal žiadosťami, ktoré sa týkajú osobných údajov prenášaných z EHP; informovanie vrcholového právneho a podnikového manažmentu a vývozcu údajov o prijatí takých žiadostí; procesné kroky na napadnutie neprimeraných alebo nezákonných žiadostí a poskytovanie transparentných informácií dotknutým osobám.

131. Vypracovanie osobitných postupov odbornej prípravy pre zamestnancov zodpovedných za správu žiadostí o prístup k osobným údajom od orgánov verejnej moci, ktoré by sa mali pravidelne aktualizovať, aby zohľadňovali nový vývoj v oblasti legislatívy a jurisdikcie v tretej krajine a v rámci EHP. Postupy odbornej prípravy by mali zahŕňať požiadavky práva Únie, pokiaľ ide o prístup orgánov verejnej moci k osobným údajom, najmä v súlade s článkom 52 ods. 1 Charty základných práv Európskej únie. Informovanosť zamestnancov by sa mala zvyšovať najmä posudzovaním praktických príkladov žiadostí orgánov verejnej moci o prístup k údajom a uplatňovaním normy vyplývajúcej z článku 52 ods. 1 Charty základných práv Európskej únie na takéto praktické príklady. Takáto odborná príprava by mala zohľadňovať osobitnú situáciu dovozcu údajov, napr. právne predpisy a predpisy tretej krajiny, ktorým dovozca údajov podlieha, a mala by sa vypracovať v spolupráci s vývozcom údajov, ak je to možné.

132. Podmienky účinnosti:

- O týchto politikách možno uvažovať len v prípadoch, keď je žiadosť orgánov verejnej moci v tretej krajine zlučiteľná s právom EÚ.[102] Ak je žiadosť nezlučiteľná, tieto politiky by nestačili na zabezpečenie rovnocennej úrovne ochrany osobných údajov a, ako už bolo uvedené, prenosy sa musia zastaviť alebo sa musia zaviesť vhodné dodatočné opatrenia na zabránenie prístupu.

Opatrenia v oblasti transparentnosti a zodpovednosti

133. Zdokumentovanie a zaznamenanie žiadostí o prístup prijatých od orgánov verejnej moci a poskytnutej odpovede spolu s právnym zdôvodnením a zúčastnenými aktérmi (napr. ak bol vývozca informovaný a jeho odpoveď, posúdenie tímu zodpovedného za vybavovanie takýchto žiadostí atď.). Tieto záznamy by sa mali sprístupniť vývozcovi údajov, ktorý by ich zase mal poskytnúť dotknutým osobám.

134. Podmienky účinnosti:

- Vnútroštátne právne predpisy tretej krajiny môžu zabrániť poskytnutiu žiadostí alebo podstatných informácií o nich, a preto môžu viesť k tomu, že tento postup bude neúčinný. Dovozca údajov by mal informovať vývozcu o tom, že nie je schopný poskytnúť takéto dokumenty a záznamy, aby mal vývozca možnosť pozastaviť prenosy, ak by v dôsledku takej neschopnosti nebola poskytnutá primeraná úroveň ochrany.

***

135. Pravidelné uverejňovanie správ o transparentnosti alebo zhrnutí týkajúcich sa žiadostí vlády o prístup k údajom a druhu poskytnutej odpovede, pokiaľ to umožňujú miestne právne predpisy.

136. Podmienky účinnosti:

- Poskytnuté informácie by mali byť relevantné, jasné a čo najpodrobnejšie. Vnútroštátne právne predpisy tretej krajiny môžu zabrániť poskytnutiu podrobných informácií. V týchto prípadoch by mal dovozca údajov vynaložiť maximálne úsilie na zverejnenie štatistických informácií alebo podobného typu agregovaných informácií.

Organizačné metódy a opatrenia na minimalizáciu údajov

137. V kontexte prenosov môžu byť užitočné aj existujúce organizačné požiadavky v rámci zásady zodpovednosti, ako je prijatie prísnych a podrobných politík a osvedčených postupov v oblasti prístupu k údajom a dôvernosti údajov na základe prísnej zásady „vedieť len to potrebné“ [need-to-know], monitorované pravidelnými auditmi a presadzované prostredníctvom disciplinárnych opatrení. V tejto súvislosti by sa mala zohľadniť minimalizácia údajov, aby sa obmedzilo vystavenie osobných údajov neoprávnenému prístupu. Napríklad v niektorých prípadoch nemusí byť potrebný prenos určitých údajov (napr. v prípade vzdialeného prístupu k údajom v EHP v prípadoch poskytovania podpory, keď sa poskytne obmedzený prístup namiesto úplného

[102] Pozri vec C-362/14 (Schrems I), bod 94; C-311/18 (Schrems II), body 168, 174, 175 a 176.

prístupu; alebo ak si poskytovanie služby vyžaduje len prenos obmedzeného súboru údajov, a nie celej databázy).

138. Podmienky účinnosti:

- Mali by sa zaviesť pravidelné audity a prísne disciplinárne opatrenia s cieľom monitorovať opatrenia na minimalizáciu údajov a presadzovať ich dodržiavanie, a to aj v kontexte prenosu.
- Vývozca údajov vykoná posúdenie osobných údajov, ktoré má k dispozícii pred uskutočnením prenosu, s cieľom identifikovať tie súbory údajov, ktoré nie sú potrebné na účely prenosu, a teda sa nesprístupnia dovozcovi údajov.
- Opatrenia na minimalizáciu údajov by mali byť sprevádzané technickými opatreniami, aby sa zabezpečilo, že údaje nebudú predmetom neoprávneného prístupu. Napríklad použitie bezpečného výpočtu viacerých strán a šírenie šifrovaných súborov údajov medzi rôznymi dôveryhodnými subjektmi môže svojou podstatou zabrániť tomu, aby akýkoľvek jednostranný prístup viedol k poskytnutiu identifikovateľných údajov.

***

139. Vypracovanie najlepších postupov s cieľom primerane a včas zapojiť príp. zodpovednú osobu a útvar pre právny a vnútorný audit a poskytnúť im prístup k informáciám v záležitostiach týkajúcich sa medzinárodných prenosov osobných údajov.

140. Podmienky účinnosti:

- Prípadnej zodpovednej osobe a tímu pre právny a vnútorný audit sa pred prenosom poskytnú všetky relevantné informácie a konzultuje sa s nimi o nevyhnutnosti prenosu a prípadných ďalších zárukách.
- Príslušné informácie by mali zahŕňať napríklad posúdenie nevyhnutnosti prenosu konkrétnych osobných údajov, prehľad uplatniteľných právnych predpisov tretej krajiny a záruky, ktoré sa dovozca zaviazal uplatňovať.

Prijatie štandardov a najlepších postupov

141. Prijatie prísnej politiky v oblasti bezpečnosti údajov a ochrany údajov založenej na certifikátoch EÚ alebo na kódexoch správania alebo medzinárodných štandardov (napr. normy ISO) a najlepších postupoch (napr. ENISA) s náležitým prihliadnutím na najnovšie poznatky v súlade s rizikom kategórií spracúvaných údajov.

Iné

142. Prijatie a pravidelné preskúmanie vnútorných politík s cieľom posúdiť vhodnosť vykonaných doplnkových opatrení [complementary measures] a v prípade potreby určenie a zavedenie ďalších alebo alternatívnych riešení s cieľom zabezpečiť, aby sa pri prenášaných osobných údajoch zachovala úroveň ochrany v podstate rovnocenná ochrane, aká je zaručená v rámci EHP.

***

143. Záväzok dovozcu údajov nevykonávať žiadny následný prenos osobných údajov v rámci tej istej alebo inej tretej krajiny alebo pozastaviť prebiehajúce prenosy, ak v tretej krajine nemožno zaručiť úroveň ochrany osobných údajov v podstate rovnocennú ochrane, aká sa poskytuje v rámci EHP.[103]

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

PRÍLOHA 3: MOŽNÉ ZDROJE INFORMÁCIÍ NA ÚČELY POSÚDENIA TRETEJ KRAJINY

144. Váš dovozca údajov by mal byť schopný poskytnúť vám relevantné zdroje a informácie týkajúce sa tretej krajiny, v ktorej je usadený, vrátane právnych predpisov a postupov vzťahujúcich sa na dovozcu a prenášané údaje. Vy a dovozca môžete poukázať na niekoľko zdrojov informácií, ako sú informácie, ktoré sú orientačným spôsobom uvedené nižšie a v poradí podľa preferencie:

- judikatúra Súdneho dvora Európskej únie (SDEÚ) a Európskeho súdu pre ľudské práva (ESĽP)[104], ako sa uvádza v odporúčaniach o európskych základných zárukách;[105]
- rozhodnutia o primeranosti v krajine určenia, ak sa prenos opiera o iný právny základ;[106]
- uznesenia a správy od medzivládnych organizácií ako je Rada Európy,[107] iné regionálne orgány[108]; a orgány OSN a agentúr (napr. Rada OSN pre ľudské práva,[109] Výbor pre ľudské práva[110]);
- správy a analýzy od príslušných regulačných sietí, ako je napríklad Global Privacy Assembly (GPA);[111]
- vnútroštátna judikatúra alebo rozhodnutia prijaté nezávislými súdnymi alebo správnymi orgánmi príslušnými v oblasti ochrany súkromia a ochrany údajov tretích krajín;
- správy nezávislých kontrolných alebo parlamentných orgánov;
- správy založené na praktických skúsenostiach s predchádzajúcimi prípadmi žiadostí o poskytnutie údajov od orgánov verejnej moci alebo s neexistenciou takých žiadostí od subjektov pôsobiacich v rovnakom sektore ako dovozca;
- pravidelné automatické potvrdenia od iných subjektov spracúvajúcich údaje v rovnakej oblasti ako dovozca;
- správy vypracované alebo objednané obchodnými komorami, podnikateľskými, profesijnými a obchodnými združeniami, vládnymi diplomatickými, obchodnými a investičnými agentúrami

---

[104] Pozri prehľad judikatúry ESĽP o hromadnom sledovaní: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

[105] Odporúčania EDPB 02/2020 o európskych základných zárukách pre opatrenia týkajúce sa sledovania z 10. novembra 2020, https://edpb.europa.eu/system/files/2021-04/edpb_recommendations_202002_europeanessentialguaranteessurveillance_sk.pdf

[106] C-311/18 (Schrems II), bod 141; pozri rozhodnutia o primeranosti na adrese 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] Pozri napríklad správy Medziamerickej komisie pre ľudské práva (IACHR) o jednotlivých krajinách, https://www.oas.org/en/iachr/reports/country.asphttps://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx.

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

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

[111] Pozri napr. 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

vývozcu alebo iných tretích krajín vyvážajúcich do tretej krajiny, do ktorej sa uskutočňuje prenos;

- správy od akademických inštitúcií a organizácií občianskej spoločnosti (napr. mimovládnych organizácií);
- správy od súkromných poskytovateľov obchodných informácií o finančných, regulačných a reputačných rizikách pre spoločnosti;
- pravidelné automatické potvrdenia od samotného dovozcu;[112]
- správy o transparentnosti pod podmienkou, že výslovne uvádzajú skutočnosť, že neboli prijaté žiadne žiadosti o prístup. Správy o transparentnosti, ktoré sa o tomto bode nezmieňujú, by sa nepovažovali za dostatočné dôkazy, keďže tieto správy sa najčastejšie zameriavajú na žiadosti o prístup od orgánov presadzovania práva a poskytujú údaje len z tohto hľadiska, pričom sa nezmieňujú o prijatých žiadostiach o prístup na účely národnej bezpečnosti. To neznamená, že neboli prijaté žiadne žiadosti o prístup, ale skôr že tieto informácie nemožno zdieľať; [113]
- interné vyhlásenia alebo záznamy dovozcu, v ktorých sa výslovne uvádza, že počas dostatočne dlhého obdobia neboli prijaté žiadne žiadosti o prístup; a s uprednostnením vyhlásení a záznamov týkajúcich sa zodpovednosti dovozcu a/alebo vydávaných internými zamestnancami s určitou nezávislosťou, akými sú interní audítori, zodpovedné osoby, atď. [114]

[112] Pozri odsek 47, pokiaľ ide o podmienky na posúdenie zdokumentovaných praktických skúseností dovozcu s príslušnými predchádzajúcimi prípadmi žiadostí o prístup doručených od orgánov verejnej moci v tretej krajine.
[113] *Tamže.*
[114] *Tamže.*