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

Odporúčania č. 01/2020 o opatreniach, ktoré dopĺňajú nástroje na prenos s cieľom zabezpečiť súlad s úrovňou ochrany osobných údajov v EÚ

Prijaté 10. novembra 2020

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 cestovať s údajmi bez ohľadu na to, kam tieto údaje smerujú. 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 v musí byť podstate rovnocenná. 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 doplňujúce opatrenia, 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 verejným 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 doplňujúcich opatrení. Tieto odporúčania poskytujú vývozcom viacero krokov, ktoré treba podniknúť, možné zdroje informácií a niekoľko príkladov doplňujúcich 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 údaje, ktoré prenášate, sú primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa prenášajú do tretej krajiny a spracúvajú sa v nej.

Druhým krokom je **overiť nástroj na prenos, ktorý pri prenose využívate**, spomedzi nástrojov uvedených v kapitole V všeobecného nariadenia o ochrane údajov. Ak už Európska komisia potvrdila primeranosť krajiny, regiónu alebo sektora, do ktorého zasielate údaje, v jednom zo svojich rozhodnutí o primeranosti podľa článku 45 všeobecného nariadenia o ochrane údajov alebo na základe predchádzajúcej smernice 95/46, 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 pri prenosoch, ktoré sú pravidelné a opakujúce sa, využívať jeden z nástrojov na prenos uvedených v článku 46 všeobecného nariadenia o

ochrane údajov. Len v niektorých prípadoch príležitostných a neopakujúcich sa prenosov môžete využiť jednu z výnimiek stanovených v článku 49 všeobecného nariadenia o ochrane údajov, ak spĺňate podmienky.

Tretím krokom je **posúdiť**, či v **právnych predpisoch alebo postupoch tretej krajiny** existuje niečo, čo by v súvislosti s konkrétnym prenosom mohlo ovplyvniť účinnosť primeraných záruk nástrojov na prenos, ktoré využívate. Posúdenie by sa malo v prvom rade zamerať na právne predpisy tretej krajiny, ktoré sú relevantné pre váš prenos, a pre nástroj na prenos údajov podľa článku 46 všeobecného nariadenia o ochrane údajov, ktorý využívate a ktoré by mohli ohroziť ním poskytovanú úroveň ochrany. 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 dohľadu, pozri odporúčania EDPB týkajúce sa európskych základných záruk. Mali by sa starostlivo zvážiť najmä vtedy, keď sú právne predpisy upravujúce prístup orgánov verejnej moci k údajom nejednoznačné alebo nie sú verejne dostupné. Ak neexistujú právne predpisy upravujúce okolnosti, za ktorých majú orgány verejnej moci prístup k osobným údajom, a stále máte o prenos záujem, mali by ste preskúmať iné relevantné a objektívne faktory a nemali by ste sa spoliehať na subjektívne faktory, ako je pravdepodobnosť prístupu orgánov verejnej moci k vašim údajom spôsobom, ktorý nie je v súlade s normami EÚ. Toto posúdenie by ste mali vykonať s náležitou starostlivosťou a dôkladne zdokumentovať, keďže budete zodpovedať za rozhodnutie, ktoré na jeho základe prijmete.

Štvrtým krokom je **identifikovať a prijať doplňujúce 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 neúplný zoznam príkladov doplňujúcich opatrení a niektoré podmienky na dosiahnutie ich účinnosti. Podobne ako v prípade primeraných záruk obsiahnutých v nástrojoch na prenos podľa článku 46, niektoré doplňujúce opatrenia môžu byť účinné v niektorých krajinách, ale nie nevyhnutne v iných. Budete zodpovední za posúdenie ich účinnosti v súvislosti s prenosom a vzhľadom na právne predpisy tretej krajiny a nástroj na prenos, ktorý využívate, a ponesiete zodpovednosť za rozhodnutie, ktoré prijmete. Môže si to vyžadovať aj kombináciu niekoľkých doplňujúcich opatrení. V konečnom dôsledku môžete dospieť k záveru, že žiadne doplňujúce opatrenie nemôže zabezpečiť v podstate rovnocennú úroveň ochrany konkrétneho prenosu. V prípadoch, keď nie je vhodné žiadne doplňujúce opatrenie, musíte zabrániť prenosu, pozastaviť ho alebo ukončiť, aby nedošlo k ohrozeniu úrovne ochrany osobných údajov. Toto posúdenie doplňujúcich opatrení by ste mali vykonať s náležitou starostlivosťou a zdokumentovať ho.

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

Šiestym a posledným krokom bude prehodnocovanie úrovne ochrany údajov, ktoré prenášate do tretích krajín, v primeraných intervaloch a monitorovanie toho, 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 náležite zvážia opatrenia, 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 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.

[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.

(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 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 doplňujúcimi 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 doplňujúce 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 „dodatočné záruky“, „dodatočné opatrenia“ alebo „doplňujúce opatrenia“ 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 doplňujúcich opatrení. Cieľom týchto odporúčaní je poskytnúť vývozcom metodiku na určenie toho, či a aké dodatočné 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 EÚ. EDPB sa týmito odporúčaniami snaží podporovať konzistentné uplatňovanie všeobecného nariadenia o ochrane údajov a rozhodnutia Súdneho dvora v súlade s mandátom EDPB.[7]

PRIJAL TOTO ODPORÚČANIE:

[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] Právo na ochranu údajov sa preto poskytuje na vysokej úrovni 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. Pri prenose údajov do tretích krajín mimo EHP musí údaje sprevádzať úroveň ochrany, ktorá je v podstate rovnocenná úrovni zaručenej v rámci EÚ, aby sa zabezpečilo, že sa nenaruší úroveň ochrany zaručená všeobecným nariadením o ochrane údajov.

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 schopní preukázať toto úsilie dotknutým osobám, širokej verejnosti 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 zodpovednosť vývozcov a dovozcov zabezpečiť, aby sa spracovanie osobných údajov vykonávalo a naďalej vykonávalo 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 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,

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

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 PLÁN: UPLATŇOVANIE ZÁSADY ZODPOVEDNOSTI NA PRENOSY ÚDAJOV V PRAXI

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

7. Toto posúdenie a doplňujúce opatrenia, ktoré si zvolíte a budete vykonávať, budete musieť náležite zdokumentovať a takúto dokumentáciu na požiadanie sprístupniť príslušnému dozornému orgánu.[21]

2.1 Krok 1: Informovanosť o vlastných prenosoch

8. Ak chcete vedieť, čo sa od vás (vývozcu údajov) môže vyžadovať, aby ste mohli pokračovať v prenose alebo vykonávať nové prenosy osobných údajov[22], 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 s tretími krajinami a využívajúce viacerých sprostredkovateľov a subdodávateľov. Znalosť vlastných prenosov je nevyhnutným prvým krokom k splneniu vašich povinností v rámci zásady zodpovednosti.

[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] Pozri Usmernenia 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_sk.
[20] Usmernenia EDPB 2/2020 k článku 46 ods. 2 písm. a) a článku 46 ods. 3 písm. b) nariadenia 2016/679 v súvislosti s prenosmi osobných údajov medzi orgánmi verejnej moci a subjektmi, v rámci EHP a mimo EHP, pozri https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en.
[21] Článok 5 ods. 2 všeobecného nariadenia o ochrane údajov a článok 24 ods. 1 všeobecného nariadenia o ochrane údajov.
[22] Upozorňujeme, že za prenos sa považuje aj vzdialený prístup subjektu z tretej krajiny k údajom nachádzajúcim sa v EHP.

9. Ak sa chcete plne informovať 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.[23] 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) nariadenia GPDR o vašich prenosoch ich osobných údajov do tretích krajín.[24]

10. Pri mapovaní prenosov nezabudnite zohľadniť aj následné prenosy, napríklad či sprostredkovatelia mimo EHP prenášajú osobné údaje, ktoré ste im zverili, subdodávateľovi v inej tretej krajine alebo v tej istej tretej krajine[25].

11. V súlade so zásadou „minimalizácie údajov" podľa všeobecného nariadenia o ochrane údajov[26] musíte overiť, či sú údaje, ktoré prenášate, primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa prenášajú do tretej krajiny a spracúvajú v nej.

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. Majte na pamäti, 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.[27] Konkrétnejšie, ak používate medzinárodnú cloudovú infraštruktúru, musíte posúdiť, či sa vaše údaje budú prenášať do tretích krajín a do ktorých, pokiaľ poskytovateľ cloudu vo svojej zmluve jasne neuvádza, že údaje sa v tretích krajinách vôbec nespracúvajú.

[23] 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).

[24] 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.

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

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

[27] 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.

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.[28]

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).[29]

18. Európska komisia uverejňuje zoznam svojich rozhodnutí o primeranosti na svojej webovej stránke.[30]

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.**[31] Stále však musíte monitorovať, či rozhodnutia o primeranosti týkajúce sa prenosov nebudú zrušené alebo vyhlásené za neplatné.[32]

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 rozhodnutia, takže vnútroštátny súd môže podať návrh na začatie prejudiciálneho konania na SDEÚ na účely preskúmania tejto platnosti.[33]

---

[28] 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.

[29] Článok 45 ods. 1 všeobecného nariadenia o ochrane údajov.

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

[31] 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.

[32] 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)].

[33] 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, žiadny právny základ neopodstatňuje spracúvanie údajov ako také 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

Príklad: Občan EÚ, pán Schrems, podal v júni 2013 sťažnosť írskej komisii pre ochranu údajov (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 „bezpečného prístavu“ Spojené štáty zabezpečujú primeranú úroveň ochrany prenášaných osobných údajov (rozhodnutie o bezpečnom prístave). 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 bezpečného prístavu.[34]

Nástroje na prenos údajov 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 na prenos údajov podľa všeobecného nariadenia o ochrane údajov si zvolíte, musíte zabezpečiť, aby sa na prenášané osobné údaje celkovo vzťahovala v podstate rovnocenná 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 krajín. Situácia v tretej krajine, do ktorej zasielate údaje, si môže stále vyžadovať, aby ste doplnili tieto nástroje na prenos a záruky, ktoré obsahujú, dodatočnými opatreniami („doplňujúce opatrenia“) s cieľom zabezpečiť v podstate rovnocennú úroveň ochrany.[35]

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.

rozhodnutia Komisie o primeranosti, podali návrh na začatie prejudiciálneho konania na Súdny dvor Európskej únie na účely preskúmania jeho platnosti.

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

[35] C-311/18 (Schrems II), body 130 a 133. Pozri tiež bod 2.3.

25. Článok 49 všeobecného nariadenia o ochrane údajov má výnimočnú povahu. Výnimky, ktoré obsahuje, sa preto musia vykladať reštriktívne a týkajú sa najmä spracovateľských činností, ktoré sú príležitostné a neopakujú sa. Európsky výbor pre ochranu údajov vydal Usmernenia č. 2/2018 o výnimkách podľa článku 49 nariadenia (EÚ) 2016/679. [36]

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 právnym základom pre váš prenos nemôže byť ani rozhodnutie o primeranosti, ani výnimka podľa článku 49, musíte pokračovať v kroku 3.

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

28. Výber nástroja na prenos údajov podľa článku 46 všeobecného nariadenia o ochrane údajov nemusí postačovať. Nástroj na prenos musí zabezpečiť, aby prenos neohrozil úroveň ochrany zaručenú všeobecným nariadením o ochrane údajov.[37] Inými slovami, nástroj na prenos musí byť v praxi účinný.

29. Účinný znamená, že prenášaným osobným údajom sa v tretej krajine poskytuje úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v rámci EHP.[38] To neplatí v prípade, ak dovozca údajov nemôže plniť povinnosti vyplývajúce zo zvoleného nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov preto, že mu v tom bránia právne predpisy a postupy tretej krajiny, ktoré sa na prenos vzťahujú.

30. Preto musíte posúdiť, v prípade potreby aj v spolupráci s dovozcom, či právne predpisy alebo postupy tretej krajiny obsahujú niečo, čo by mohlo v kontexte vášho konkrétneho prenosu ovplyvniť účinnosť primeraných záruk nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov, ktorý využívate. Váš dovozca údajov by vám v prípade potreby mal poskytnúť relevantné zdroje a informácie týkajúce sa tretej krajiny, v ktorej je usadený, a právnych predpisov, ktoré sa na prenos vzťahujú. Môžete sa odvolať aj na iné zdroje informácií, napríklad na tie, ktorých neúplný zoznam je uvedený v prílohe 3.[39]

31. V posúdení by sa mali zohľadniť všetky subjekty zapojené do prenosu (napr. prevádzkovatelia, sprostredkovatelia a subdodávatelia 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 následný prenos, ku ktorému môže dochádzať.

32. Na tento účel budete musieť preskúmať charakteristiky každého z vašich prenosov a určiť, ako sa na tieto prenosy vzťahuje vnútroštátny právny poriadok krajiny, do ktorej sa údaje prenášajú (alebo sa následne prenášajú).

---

[36] Viac informácií k tejto téme nájdete na adrese https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_sk.
[37] Článok 44 všeobecného nariadenia o ochrane údajov.
[38] C-311/18 (Schrems II), body 105 a druhý záver.
[39] Pozri tiež bod 43.

33. Uplatniteľný právny rámec bude závisieť od okolností prenosu, najmä:

- účely, na ktoré sa údaje prenášajú a spracúvajú (napr. marketing, ľudské zdroje, uchovávanie, podpora IT, klinické skúšanie),
- typy subjektov zapojených do spracúvania údajov (verejné/súkromné; prevádzkovatelia/sprostredkovatelia),
- sektor, 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),
- či sa údaje budú uchovávať v tretej krajine alebo či dochádza len k vzdialenému prístupu k údajom uchovávaným v rámci EÚ/EHP,
- formát údajov, ktoré sa majú preniesť (t. j. obyčajný text/pseudonymizované alebo zašifrované40),
- možnosť, že údaje môžu byť predmetom následného prenosu z tretej krajiny do ďalšej tretej krajiny.[41]

34. Pri uplatniteľných právnych predpisov budete musieť posúdiť, či nejaký z nich zasahuje do záväzkov obsiahnutých vo vami zvolenom nástroji na prenos údajov podľa článku 46 všeobecného nariadenia o ochrane údajov. Mali by ste overiť, či sa záväzky umožňujúce dotknutým osobám uplatňovať ich práva v súvislosti s medzinárodnými prenosmi (ako sú žiadosti o prístup, opravu a vymazanie prenesených údajov) môžu účinne uplatňovať v praxi a či ich právne predpisy v tretej krajine určenia neobmedzujú.

35. Budete musieť posúdiť príslušné pravidlá všeobecnej povahy, pokiaľ majú vplyv na účinné uplatňovanie záruk obsiahnutých v nástroji na prenos údajov podľa článku 46 všeobecného nariadenia o ochrane údajov a na základné práva jednotlivcov (najmä právo na nápravu priznané dotknutej osobe v prípade prístupu orgánov verejnej moci tretích krajín k prenášaným údajom).

36. V každom prípade by ste mali venovať osobitnú pozornosť všetkým príslušným právnym predpisom, najmä právnym predpisom, ktorými sa stanovujú požiadavky na sprístupnenie 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). Ak sú tieto požiadavky alebo právomoci obmedzené na to, čo je nevyhnutné a primerané v demokratickej spoločnosti[42], nesmú zasahovať do záväzkov obsiahnutých v nástroji na prenos údajov podľa článku 46 všeobecného nariadenia o ochrane údajov, ktorý využívate.

37. Normy EÚ, ako sú články 47 a 52 Charty základných práv Európskej únie, sa musia použiť ako referencia na posúdenie toho, či je takýto prístup orgánov verejnej moci obmedzený na to, čo je nevyhnutné a primerané v demokratickej spoločnosti a či sa dotknutým osobám poskytuje účinná náprava.

[40] Niektoré tretie krajiny nepovoľujú dovoz šifrovaných údajov.
[41] Ak prevádzkovateľ udelil svoje predchádzajúce osobitné alebo všeobecné písomné povolenie v súlade s článkom 28 ods. 2 všeobecného nariadenia o ochrane údajov.
[42] Pozri články 47 a 52 Charty základných práv Európskej únie, článok 23 ods. 1 všeobecného nariadenia o ochrane údajov a odporúčania EDPB č. 02/2020 o európskych základných zárukách týkajúcich sa opatrení sledovania, 10. novembra 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

38. 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.[43] Napríklad situácia v oblasti právneho štátu v tretej krajine môže byť relevantná pri posudzovaní účinnosti dostupných mechanizmov, ktoré majú jednotlivci k dispozícii na dosiahnutie (súdnej) nápravy v prípade nezákonného prístupu vlády k osobným údajom. Existencia komplexného zákona o ochrane údajov alebo nezávislého orgánu pre ochranu osobných údajov, ako aj dodržiavanie medzinárodných nástrojov zabezpečujúcich záruky ochrany údajov môžu prispieť k zabezpečeniu proporcionality zasahovania zo strany vlády.[44]

***

39. V odporúčaniach EDPB o európskych základných zárukách sa uvádzajú prvky, ktoré treba posúdiť pri určovaní toho, či právny rámec upravujúci prístup orgánov verejnej moci v tretej krajine, či už ide o národné bezpečnostné agentúry alebo orgány presadzovania práva, možno považovať za odôvodnený zásah (a teda nie za zásah do záväzkov prijatých v rámci nástroja na prenos údajov podľa článku 46 všeobecného nariadenia o ochrane údajov) alebo nie. Mali by sa starostlivo zvážiť najmä vtedy, keď sú právne predpisy upravujúce prístup orgánov verejnej moci k údajom nejednoznačné alebo nie sú verejne dostupné.

40. Pokiaľ ide o prenos údajov na základe nástrojov na prenos podľa článku 46, odporúčania EDPB o európskych základných zárukách môžu slúžiť ako usmernenie pre vývozcu a dovozcu údajov pri posudzovaní toho, či takéto právomoci neodôvodnene zasahujú do povinností dovozcu údajov zabezpečiť v podstate rovnocennú úroveň ochrany.

41. 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.

42. Posúdenie musí vychádzať predovšetkým z právnych predpisov, ktoré sú verejne dostupné. V niektorých situáciách to však nestačí, pretože právne predpisy v tretích krajinách nemusia byť dostatočné. Ak aj napriek tomu stále uvažujete o prenose, mali by ste preskúmať ďalšie relevantné a objektívne faktory[45] a nespoliehať sa na subjektívne faktory, ako je pravdepodobnosť prístupu orgánov verejnej moci k vašim údajom spôsobom, ktorý nie je v súlade s normami EÚ. Toto posúdenie by ste mali vykonať s náležitou starostlivosťou a dôkladne zdokumentovať, keďže budete zodpovedať za rozhodnutie, ktoré na jeho základe prijmete.[46]

43. Posúdenie môžete doplniť o informácie získané z iných zdrojov[47], ako sú napríklad:

    - prvky preukazujúce, že orgán tretej krajiny sa bude usilovať o prístup k údajom s vedomím alebo bez vedomia dovozcu údajov vzhľadom na nahlásené precedensy, právne predpisy a postupy,

[43] C-311/18 (Schrems II), bod 104.
[44] Napríklad: Dohovor č. 108 (Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov, ETS č. 108) alebo Dohovor č. 108+ (modernizovaný Dohovor o ochrane jednotlivcov pri spracovaní osobných údajov, CETS č. 223) stanovujú vymáhateľné, medzinárodné právne prostriedky nápravy v prípade porušenia ochrany údajov a prispievajú k zabezpečeniu minimálnej úrovne ochrany osobných údajov a rešpektovania súkromného života.
[45] Pozri bod 43, ako aj prílohu 3.
[46] Článok 5 ods. 2 všeobecného nariadenia o ochrane údajov.
[47] Pozri aj prílohu 3.

- prvky preukazujúce, že orgán tretej krajiny bude mať prístup k údajom prostredníctvom dovozcu údajov alebo priamym zachytávaním údajov z komunikačného kanála vzhľadom na nahlásené precedensy, zákonné právomoci a technické, finančné a ľudské zdroje, ktoré má k dispozícii.

44. Z posúdenia môže napokon vyplynúť, že nástroj na prenos údajov podľa článku 46 všeobecného nariadenia o ochrane údajov, ktorý využívate, a primerané záruky, ktoré obsahuje:

- účinne zabezpečuje, že sa prenášaným osobným údajom v tretej krajine poskytuje úroveň ochrany, ktorá je v podstate rovnocenná úrovni zaručenej v rámci EHP. Právne predpisy a postupy tretej krajiny, ktoré sa vzťahujú na prenos, umožňujú dovozcovi údajov splniť si svoje povinnosti v rámci zvoleného nástroja na prenos údajov. 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 vzhľadom na právne predpisy a/alebo postupy tretej krajiny, ktoré sa vzťahujú na prenos. Súdny dvor 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 doplňujúcich opatrení alebo za neuskutočnenie prenosu osobných údajov.[48]

SDEÚ napríklad 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 zákona FISA nie je v podstate rovnocenná zárukám požadovaným podľa práva EÚ. V dôsledku toho, ak dovozca údajov alebo akýkoľvek ďalší príjemca, ktorému môže dovozca údajov poskytnúť údaje, patrí do rozsahu pôsobnosti článku 702 zákona FISA[49], štandardné zmluvné doložky alebo iné nástroje na prenos podľa všeobecného nariadenia o ochrane údajov možno pri takomto prenose použiť len vtedy, ak dodatočné doplňujúce technické opatrenia znemožnia prístup k prenášaným údajom alebo dosiahnu jeho neúčinnosť.

2.4 4. krok: Prijatie doplňujúcich opatrení

45. 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 doplňujúce opatrenia, ktoré by po doplnení k zárukám obsiahnutým v nástrojoch na prenos údajov mohli zabezpečiť, aby sa prenášaným údajom v tretej krajine poskytla úroveň ochrany, ktorá je v podstate rovnocenná úrovni ochrany zaručenej v rámci EÚ.[50] „Doplňujúce opatrenia“ sú vo svojej

[48] SDEÚ, C-311/18 (Schrems II), body 134 – 135.
[49] Článok 702 zákona FISA sa uplatňuje, ak sa údaje získavajú „od poskytovateľa elektronických komunikačných služieb alebo s jeho pomocou“ [článok 702 zákona FISA = hlava 50 § 1881a písm. h) ods. 2) písm. A) bod vi) zákonníka USA], ktorý je vymedzený v hlave 50 zákonníka USA § 1881 písm. b) ods. 4 ako
„A) telekomunikačný prepravca, ako je vymedzený v článku 153 hlavy 47;
B) poskytovateľ elektronických komunikačných služieb, ako je vymedzený v článku 2510 hlavy 18;
C) poskytovateľ počítačových služieb na diaľku, ako je vymedzený v článku 2711 hlavy 18;
D) každý iný poskytovateľ komunikačných služieb, ktorý má prístup k telefonickej alebo elektronickej komunikácii keď sa takáto komunikácia prenáša alebo uchováva; alebo
E) úradník, zamestnanec alebo zástupca subjektu uvedeného v pododsekoch A, B, C alebo D.“
[50] C-311/18 (Schrems II), bod 96.

podstate doplnkom k zárukám, ktoré už poskytuje nástroj na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov.[51]

46. Pri použití osobitného nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov musíte v každom jednotlivom prípade určiť, ktoré doplňujúce opatrenia by mohli byť účinné v prípade súboru prenosov do konkrétnej tretej krajiny. Budete môcť vychádzať z predchádzajúcich hodnotení v rámci krokov (1, 2 a 3 vyššie) a na základe ich zistení skontrolovať potenciálnu účinnosť doplňujúcich opatrení pri zabezpečovaní požadovanej úrovne ochrany.

47. V zásade môžu mať doplňujúce 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.

48. Samotné zmluvné a organizačné opatrenia vo všeobecnosti nestačia na zabránenie prístupu orgánov verejnej moci tretej krajiny k osobným údajom (ak neodôvodnene zasahuje do povinností dovozcu údajov zabezpečiť v podstate rovnocennú úroveň ochrany). Môžu sa vyskytnúť situácie, keď len technické opatrenia môžu zabrániť účinnému prístupu orgánov verejnej moci v tretích krajinách k osobným údajom, najmä na účely sledovania, alebo takýto prístup znemožniť.[52] V takýchto situáciách môžu zmluvné alebo organizačné opatrenia dopĺňať technické opatrenia a posilňovať celkovú úroveň ochrany údajov, napr. vytváraním prekážok pre pokusy orgánov verejnej moci o prístup k údajom spôsobom, ktorý nie je v súlade s normami EÚ.

49. Môžete preskúmať, príp. aj v spolupráci s dovozcom údajov, tento (neúplný) zoznam faktorov s cieľom určiť, ktoré doplňujúce opatrenia by boli najúčinnejšie pri ochrane prenášaných údajov:

- formát údajov, ktoré sa majú preniesť (t. j. obyčajný text/pseudonymizované alebo zašifrované),
- povaha údajov,
- dĺžka a zložitosť pracovného postupu spracovania údajov, počet aktérov zapojených do spracúvania a vzťah medzi nimi [napr. prenosy zahŕňajú viacerých prevádzkovateľov alebo 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)],[53]
- možnosť, že údaje môžu byť predmetom následného prenosu v rámci tej istej tretej krajiny alebo dokonca do iných tretích krajín (napr. zapojenie subdodávateľov dovozcu údajov[54]).

[51] Odôvodnenie 109 všeobecného nariadenia o ochrane údajov a vec C-311/18 (Schrems II), bod 133.

[52] 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 č. 02/2020 o európskych základných zárukách týkajúcich sa opatrení sledovania, 10. novembra 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[53] 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.

[54] Pozri poznámku pod čiarou č. 25.

Príklady doplňujúcich opatrení

50. Niektoré príklady technických, zmluvných a organizačných opatrení, ktoré prichádzajú do úvahy, možno nájsť v neúplných zoznamoch opísaných v prílohe 2.

***

51. Ak ste zaviedli účinné doplňujúce opatrenia, ktoré v kombinácii s zvoleným nástrojom na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov dosiahnu úroveň ochrany, ktorá je v súčasnosti v podstate rovnocenná úrovni ochrany zaručenej v rámci EHP, vaše prenosy môžu pokračovať.

52. Ak nie ste schopní identifikovať alebo vykonať účinné doplňujúce opatrenia, ktoré zabezpečia, aby sa na prenášané osobné údaje vzťahovala v podstate rovnocenná úroveň ochrany[55], nesmiete začať s prenosom osobných údajov do dotknutej tretej krajiny na základe nástroja na prenos údajov podľa článku 46 všeobecného nariadenia o ochrane údajov, ktorý využívate. Ak už vykonávate prenosy, musíte prenos osobných údajov pozastaviť alebo ukončiť.[56] V súlade so zárukami obsiahnutými v nástroji na prenos údajov 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.[57]

Príklad: právne predpisy tretej krajiny zakazujú doplňujúce 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.

53. Ak sa rozhodnete pokračovať v prenose bez ohľadu na skutočnosť, že dovozca nie je schopný splniť záväzky prijaté v rámci nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov, mali by ste to oznámiť príslušnému dozornému orgánu v súlade s osobitnými ustanoveniami zahrnutými do príslušného nástroja na prenos podľa článku 46 všeobecného nariadenia o ochrane údajov.[58] Príslušný dozorný orgán pozastaví alebo zakáže prenosy údajov v prípadoch, keď zistí, že nie je možné zabezpečiť v podstate rovnocennú úroveň ochrany.[59]

54. 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.

[55] 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 č. 02/2020 o európskych základných zárukách týkajúcich sa opatrení sledovania, 10. novembra 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

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

[57] 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] Pozri dokument Často kladené otázky k rozsudku Súdneho dvora Európskej únie vo veci C-311/18 – Data Protection Commissioner/Facebook Ireland Ltd a Maximillian Schrems, prijatý 23. júla 2020, najmä otázky 5, 6 a 9. Pozri tiež doložku 4 písm. g) rozhodnutia Komisie 2010/87/EÚ, a doložku 5 písm. a) rozhodnutia Komisie 2001/497/ES a doložku II písm. c) prílohy „Súbor II“ k rozhodnutiu Komisie 2004/915/ES.

[59] C-311/18 (Schrems II), body 113 a 121.

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

55. Procesné kroky, ktoré budete musieť podniknúť, ak ste identifikovali účinné doplňujúce opatrenia, ktoré sa majú zaviesť, sa môžu líšiť v závislosti od nástroja na prenos údajov 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]

56. Ak máte v úmysle okrem štandardných zmluvných doložiek zaviesť aj doplňujúce opatrenia, nie je potrebné, aby ste požiadali príslušný dozorný orgán o povolenie doplniť tento druh doložiek alebo dodatočných záruk, pokiaľ identifikované doplňujúce 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.[60] 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 doplňujúce doložky (napr. v prípade sťažnosti alebo vyšetrovania z vlastného podnetu).

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

[60] 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.

[61] 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_sk.pdf.

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

58. 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.[62]

59. 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. O konkrétnom vplyve rozsudku vo veci Schrems II na záväzné vnútropodnikové pravidlá sa stále diskutuje. EDPB čo najskôr poskytne podrobnejšie informácie o tom, či je potrebné do záväzných vnútropodnikových pravidiel zahrnúť akékoľvek dodatočné záväzky v referenčných dokumentoch WP256/257.[63]

60. 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 doplňujúce opatrenia na zabezpečenie úrovne ochrany, ktorá je v podstate rovnocenná s úrovňou ochrany, ktorá sa poskytuje v EHP, a či do týchto doplňujúcich 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]

61. 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.[64] 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. O konkrétnom vplyve rozsudku vo veci Schrems II na zmluvné doložky *ad hoc* sa stále diskutuje. EDPB čo najskôr poskytne viac podrobností.

2.6 6. krok: Prehodnotenie v primeraných intervaloch

62. Musíte priebežne monitorovať, prípadne v spolupráci s dovozcami údajov, 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).

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

[63] 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.

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

63. 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,
- doplňujúce opatrenia už v tejto tretej krajine nie sú účinné.

3 ZÁVER

64. 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.[65]

65. Aby ste zabezpečili v podstate rovnocennú úroveň ochrany údajov, musíte v prvom rade dôkladne poznať vlastné prenosy. Musíte tiež skontrolovať, či údaje, ktoré prenášate, sú primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa prenášajú do tretej krajiny a spracúvajú sa v nej.

66. 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 doplňujúce opatrenia.

67. Ak nie ste schopní identifikovať alebo vykonať účinné doplňujúce 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.

68. 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)

[65] 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 údajov podľa článku 46 všeobecného nariadenia o ochrane údajov, ktoré môžu prevádzkovatelia a sprostredkovatelia používať.
- „Štandardné zmluvné doložky“ sú štandardné doložky o ochrane údajov (alebo „štandardné zmluvné doložky“), 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 DOPLŇUJÚCICH OPATRENÍ

69. Nasledujúce opatrenia sú príkladmi doplňujúcich opatrení, ktoré môžete zvážiť v kroku 4 „Prijatie doplňujúcich opatrení“. Tento zoznam nie je úplný. 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 doplňujúce opatrenia, ktoré dokážu účinne zaručiť túto úroveň ochrany pri vašich prenosoch.

70. Akékoľvek doplňujúce opatrenie možno považovať za účinné v zmysle rozsudku Súdneho dvora Európskej únie „Schrems II“ len a ak sa ním riešia konkrétne nedostatky zistené pri posúdení právnej situácie v tretej krajine. Ak v konečnom dôsledku nedokážete zabezpečiť v podstate rovnocennú úroveň ochrany, nesmiete prenášať osobné údaje.

71. Ako prevádzkovateľ alebo sprostredkovateľ už možno musíte vykonávať niektoré z opatrení opísaných v tejto prílohe, aj keď sa na vášho dovozcu údajov vzťahuje rozhodnutie o primeranosti, rovnako ako sa od vás môže vyžadovať, aby ste ich vykonávali pri spracúvaní údajov v rámci EHP.[66]

Technické opatrenia

72. V tomto oddiele sa uvádza neúplný 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 .[67]

73. V záujme väčšej jasnosti sa v tomto oddiele najprv špecifikujú technické opatrenia, ktoré by mohli byť potenciálne účinné v určitých scenároch/prípadoch použitia na zabezpečenie v podstate rovnocennej úrovne ochrany. Ďalej sa tu uvádzajú niektoré scenáre/prípady použitia, v ktorých nebolo možné identifikovať žiadne technické opatrenia na zabezpečenie tejto úrovne ochrany.

Scenáre, pri ktorých možno identifikovať *účinné* opatrenia

74. 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 údajov podľa článku 46 všeobecného nariadenia o ochrane údajov. Tieto opatrenia sa uplatňujú aj vtedy, ak je prístup orgánov verejnej moci v súlade s právnymi predpismi krajiny dovozcu, ak takýto prístup presahuje rámec toho, čo je nevyhnutné a primerané v demokratickej spoločnosti[68]. 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

[66] Článok 5 ods. 2 všeobecného nariadenia o ochrane údajov, článok 32 všeobecného nariadenia o ochrane údajov.
[67] C-311/18 (Schrems II), bod 135.
[68] Pozri články 47 a 52 Charty základných práv Európskej únie, článok 23 ods. 1 všeobecného nariadenia o ochrane údajov a odporúčania EDPB č. 02/2020 o európskych základných zárukách týkajúcich sa opatrení sledovania.

obsahovať online identifikátory zo zariadení, aplikácií, nástrojov a protokolov, ktoré dotknuté osoby používajú v iných kontextoch.

75. 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.

76. V tomto oddiele sa posudzujú scenáre, v ktorých sa uplatňujú opatrenia, ktoré sú účinné v oboch prípadoch. Vzhľadom na okolností konkrétneho prenosu sa môžu uplatňovať rôzne doplňujúce 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 zákona 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.

77. V týchto scenároch sa opisujú konkrétne okolnosti a prijaté opatrenia. Akékoľvek zmeny scenárov môžu viesť k odlišným záverom.

78. 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 nezakódovaným údajom

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

Ak

1. sa osobné údaje pred prenosom spracúvajú pomocou silného šifrovania;
2. šifrovací algoritmus a jeho parametre (napr. dĺžka kľúča, príp. prevádzkový režim) sú čo najmodernejšie 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);

3. intenzita šifrovania zohľadňuje konkrétne časové obdobie, počas ktorého sa musí zachovať dôvernosť šifrovaných osobných údajov;
4. šifrovací algoritmus sa bezchybne vykonáva riadne udržiavaným softvérom, ktorého súlad so špecifikáciou zvoleného algoritmu bol overený, napr. certifikáciou;
5. kľúče sú spoľahlivo spravované (vytvárané, spravované, uložené, príp. prepojené s totožnosťou zamýšľaného príjemcu a zrušené); a
6. kľúče sa uchovávajú výlučne pod kontrolou vývozcu údajov alebo iných subjektov poverených touto úlohou, ktoré majú sídlo v EHP alebo tretej krajine, na území alebo v jednom či viacerých určených sektoroch v tretej krajine, alebo v rámci medzinárodnej organizácie, pre ktorú Komisia v súlade s článkom 45 všeobecného nariadenia o ochrane údajov stanovila, že zabezpečuje primeranú úroveň ochrany;

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

Prípad použitia 2: Prenos pseudonymizovaných údajov

80. 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[69];
2. tieto dodatočné informácie uchováva výlučne vývozca údajov a uchovávajú sa oddelene v členskom štáte alebo v tretej krajine, na území alebo v jednom či viacerých určených sektoroch v tretej krajine alebo v rámci medzinárodnej organizácie, pre ktorú Komisia v súlade s článkom 45 všeobecného nariadenia o ochrane údajov stanovila, že zabezpečuje primeranú úroveň ochrany;
3. sprístupneniu 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 prostredníctvom dôkladnej analýzy príslušných údajov a pri zohľadnení informácií, ktoré orgány verejnej moci prijímajúcej krajiny môžu mať k dispozícii, stanovil, že pseudonymizované osobné údaje nemožno priradiť identifikovanej alebo identifikovateľnej fyzickej osobe, a to ani v prípade, že sa na ne vzťahujú krížové odkazy;

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

81. Upozorňujeme, že v mnohých situáciách môžu faktory špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu fyzickej osoby, jej fyzické umiestnenie alebo

[69] V súlade s článkom 4 ods. 5 všeobecného nariadenia o ochrane údajov: „‚pseudonymizácia' je 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 opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe;".

jej interakciu s internetovou službou v konkrétnych časových okamihoch[70] umožniť identifikáciu tejto osoby, aj keď sa jej meno, adresa alebo iné jednoznačné identifikátory vynechajú.

82. 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.

83. 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.

Prípad použitia 3: Šifrované údaje, ktoré iba prechádzajú tretími krajinami

84. Vývozca údajov chce preniesť údaje do miesta určenia uznaného ako krajina, ktorá poskytuje primeranú ochranu v súlade s článkom 45 všeobecného nariadenia o ochrane údajov. Údaje sú smerované cez tretiu krajinu.

Ak

1. vývozca údajov prenáša osobné údaje dovozcovi údajov v jurisdikcii, ktorá zabezpečuje primeranú ochranu, údaje sa prenášajú cez internet a údaje môžu byť geograficky smerované cez tretiu krajinu, ktorá neposkytuje v podstate rovnocennú úroveň ochrany;
2. sa používa kódovanie prenosu, pri ktorom sa zabezpečí, aby použité šifrovacie protokoly boli čo najmodernejšie a poskytovali účinnú ochranu pred aktívnymi a pasívnymi útokmi so zdrojmi, o ktorých je známe, že sú k dispozícii orgánom verejnej moci tretej krajiny;
3. dešifrovanie je možné len mimo danej tretej krajiny;
4. strany zapojené do komunikácie sa dohodnú na dôveryhodnej verejnej certifikačnej autorite alebo infraštruktúre;
5. proti aktívnym a pasívnym útokom na šifrovanie prenosu sa používajú osobitné ochranné a čo najmodernejšie opatrenia;
6. 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;
7. šifrovací algoritmus a jeho parametre (napr. dĺžka kľúča, príp. prevádzkový režim) sú čo najmodernejšie a možno ich považovať za odolné voči kryptoanalýze vykonávanej orgánmi verejnej moci v krajine tranzitu s prihliadnutím na dostupné zdroje a technické kapacity (napr. výpočtová kapacita pre útoky hrubou silou);
8. intenzita šifrovania zohľadňuje konkrétne časové obdobie, počas ktorého sa musí zachovať dôvernosť šifrovaných osobných údajov;

[70] Článok 4 ods. 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;"

9. šifrovací algoritmus sa bezchybne vykonáva riadne udržiavaným softvérom, ktorého súlad so špecifikáciou zvoleného algoritmu bol overený, napr. certifikáciou;
10. existencia zadných dvierok (v hardvéri alebo softvéri) bola vylúčená;
11. kľúče sú spoľahlivo spravované (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 s šifrovaním obsahu medzi koncovými bodmi, predstavuje účinné doplňujúce opatrenie.

Prípad použitia 4: Chránený príjemca

85. 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 spracovateľa 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) počas celého obdobia, počas ktorého je potrebné údaje chrániť;
5. dešifrovací kľúč je vo výhradnej úschove chráneného dovozcu údajov a je primerane zabezpečený proti neoprávnenému použitiu alebo zverejneniu technickými a organizačnými opatreniami, ktoré sú čo najmodernejšie; 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 doplňujúce opatrenie.

Prípad použitia 5: Oddelené spracovanie alebo spracovanie viacerými stranami

86. 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 prenosom údajov rozdelí údaje takým spôsobom, aby žiadna časť prijatá jednotlivým sprostredkovateľom nestačila na úplnú alebo čiastočnú rekonštrukciu osobných údajov. Vývozca údajov získa výsledok spracovania od každého sprostredkovateľa nezávisle a získané časti zlučuje, aby dospel ku konečnému výsledku, ktorý môže predstavovať osobné alebo súhrnné 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 spracovávajú 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 nepriateľom;
5. 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 nezakódovanom 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;
6. prevádzkovateľ prostredníctvom dôkladnej analýzy daných údajov s prihliadnutím na všetky informácie, ktoré môžu mať orgány verejnej moci prijímajúcich krajín k dispozícii, zistil, že jednotlivé osobné údaje, ktoré zasiela sprostredkovateľom, nemožno priradiť identifikovanej alebo identifikovateľnej fyzickej osobe, a to ani v prípade, že sa na ne vzťahujú krížové odkazy;

potom sa EDPB domnieva, že vykonané oddelené spracovanie predstavuje účinné doplňujúce opatrenie.

Scenáre, pri ktorých nebolo možné identifikovať *žiadne účinné* opatrenia

87. 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 doplňujúce opatrenia.

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

88. Vývozca údajov využíva poskytovateľa cloudových služieb alebo iného sprostredkovateľa na spracúvanie osobných údajov v súlade s jeho pokynmi v tretej krajine.

Ak

1. prevádzkovateľ prenáša údaje poskytovateľovi cloudových služieb alebo inému sprostredkovateľovi;
2. poskytovateľ cloudových služieb alebo iný sprostredkovateľ potrebuje prístup k nezakódovaným údajom, aby mohol vykonať pridelenú úlohu; a

3. právomoc získavať prístup k prenášaným údajom udelená orgánom verejnej moci prijímajúcej krajiny presahuje rámec toho, čo je nevyhnutné a primerané v demokratickej spoločnosti;[71]

potom EDPB vzhľadom na súčasný stav techniky nie je schopný navrhnúť účinné technické opatrenie, aby pri takomto prístupe zabránil porušovaniu práv dotknutých osôb. EDPB nevylučuje, že ďalší technologický vývoj môže priniesť opatrenia na dosiahnutie zamýšľaného obchodného účelu bez toho, aby sa vyžadoval prístup k nezakódovaným údajom.

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

Prípad použitia 7: Vzdialený prístup k údajom na obchodné účely

90. Vývozca údajov sprístupňuje subjektom v tretej krajine osobné údaje, ktoré sa majú použiť na spoločné obchodné účely. 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. Príjemca údajov môže napríklad použiť údaje, ktoré dostane, 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.

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 používa nezakódované údaje na vlastné účely;
3. právomoc získavať prístup k prenášaným údajom udelená orgánom verejnej moci prijímajúcej krajiny presahuje rámec toho, čo je nevyhnutné a primerané v demokratickej spoločnosti;

potom EDPB nie je schopný navrhnúť účinné technické opatrenie, aby pri takomto prístupe zabránil porušovaniu práv dotknutých osôb.

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

[71] Pozri články 47 a 52 Charty základných práv Európskej únie, článok 23 ods. 1 všeobecného nariadenia o ochrane údajov a odporúčania EDPB č. 02/2020 o európskych základných zárukách týkajúcich sa opatrení sledovania.

Dodatočné zmluvné opatrenia

92. Tieto opatrenia budú vo všeobecnosti pozostávať z jednostranných, dvojstranných alebo mnohostranných[72] zmluvných záväzkov.[73] 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.[74]

93. 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 schopné zaväzovať orgány tejto tretej krajiny, ak nie sú zmluvnou stranou zmluvy[75], by sa tieto opatrenia mali kombinovať s inými technickými a organizačnými opatreniami na zabezpečenie požadovanej úrovne ochrany údajov. 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.

94. 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.

95. 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.[76]

96. 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

97. ***V závislosti od konkrétnych okolností prenosov môže byť potrebné, aby sa v zmluve stanovilo, že uskutočňovanie prenosov si vyžaduje zavedenie osobitných technických opatrení (pozri vyššie navrhované technické opatrenia).***

[72] Napr. v rámci záväzných vnútropodnikových pravidiel, ktoré by mali v každom prípade regulovať niektoré z ďalej uvedených opatrení.

[73] 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.

[74] 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).

[75] C-311/18 (Schrems II), bod 125.

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

98. ***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:

99. ***Vývozca by mohol doplniť k zmluve prílohy s informáciami, ktoré by pri vynaložení maximálneho úsilia poskytol dovozca o prístupe orgánov verejnej moci k údajom v krajine určenia, a to aj v 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.***

100. Od dovozcu by sa napríklad mohlo vyžadovať:

(1) vymenovanie zákonov a iných právnych predpisov krajiny určenia, ktoré sa vzťahujú na dovozcu alebo jeho subdodávateľov, ktoré by orgánom verejnej správy 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;
(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;...);
(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[77], 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;[78]
(5) uvedenie, či a do akej miery je dovozcovi zo zákona zakázané poskytovať informácie uvedené v bodoch 1 až 5.

101. 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.

[77] 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.
[78] Splnenie tejto povinnosti samo osebe nepredstavuje poskytnutie primeranej úrovne ochrany. Zároveň si akékoľvek nevhodné zverejnenie, ku ktorému skutočne došlo, vyžaduje zavedenie doplňujúcich opatrení.

102. ***Podmienky účinnosti:***

- Dovozca musí byť schopný poskytnúť vývozcovi tieto druhy informácií podľa svojho najlepšieho vedomia a pri vynaložení maximálneho úsilia na ich získanie.[79]
- 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 prevod 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 EÚ. 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.

***

103. ***Vývozca by tiež mohol doplniť doložky, ktorými dovozca osvedčuje, že 1. zámerne nevytvoril zadné dvierka 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. že vnútroštátne právo alebo verejná 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.[80]***

104. ***Podmienky účinnosti:***

- Existencia právnych predpisov alebo verejných 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.[81]
- Zmluva musí obsahovať sankcie a/alebo možnosť vývozcu v krátkom čase vypovedať zmluvu v prípadoch, keď dovozca neodhalí existenciu 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.

***

105. ***Vývozca by mohol posilniť svoju právomoc vykonávať audity[82] alebo kontroly zariadení na spracovanie údajov dovozcu na mieste a/alebo na diaľku s cieľom overiť, či sa údaje sprístupnili 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***

[79] Pozri bod 32.5.

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

[81] Pozri bod 32.5.

[82] 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.

zabezpečujúcich rýchly zásah kontrolných orgánov a posilnením autonómie vývozcu pri výbere kontrolných orgánov.

106. ***Podmienky účinnosti:***

- Rozsah auditu by sa mal z právneho a technického hľadiska vzťahovať na každé spracúvanie osobných údajov prenášaných v tretej krajine sprostredkovateľmi alebo subdodávateľmi dovozcu, aby bol plne účinný.
- Záznamy o prístupe a iné podobné záznamy by mali byť zabezpečené proti manipulácii, aby audítori mohli nájsť dôkazy o poskytovaní údajov. 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.

***

107. ***Ak sa pôvodne posúdili právne predpisy a postupy tretej krajiny dovozcu a dospelo sa k záveru, že poskytujú úroveň ochrany v podstate rovnocennú úrovni ochrany, akú poskytuje EÚ pri údajoch prenášaných vývozcom, vývozca by mohol ešte viac posilniť povinnosť dovozcu údajov bezodkladne informovať vývozcu údajov o tom, že nie je schopný splniť zmluvné záväzky, a v dôsledku toho dodržiavať požadovanú úroveň „v podstate rovnocennej úrovne ochrany údajov“.***[83]..

108. Táto neschopnosť splniť záväzky môže vyplývať zo zmien v právnych predpisoch alebo postupoch tretej krajiny.[84] 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 prevod a/alebo vypovedať zmluvu.

109. ***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.

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

[84] 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.“*

- 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, 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 prostredníctvom sankcií voči dovozcovi a/alebo schopnosti vývozcu pozastaviť prevod a/alebo okamžite vypovedať zmluvu.

***

110. ***Pokiaľ to umožňujú vnútroštátne právne predpisy tretej krajiny, zmluva by mohla posilniť povinnosti dovozcu týkajúce sa transparentnosti využitím metódy „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 alebo podobných údajov. Ak nedôjde k aktualizácii tohto oznámenia, vývozcovi tým bude oznámené, že dovozca mohol takýto príkaz dostať.***

111. ***Podmienky účinnosti:***

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

Povinnosť prijať konkrétne opatrenia

112. ***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.***

113. ***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 bude musieť nevyhnutne dopĺňať iné doplňujúce 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.

***

114. ***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 údajov podľa článku 46 všeobecného nariadenia o ochrane údajov[85] 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.***

115. ***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 práv dotknutých osôb na uplatňovanie ich práv

116. ***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.***

117. ***Podmienky účinnosti:***

[85] V štandardných zmluvných doložkách sa napríklad stanovuje, že spracovanie 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.

- Táto doložka by mohla byť účinné 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)[86].
- Vnútroštátne predpisy alebo politiky, ktoré ukladajú dovozcovi povinnosť nezverejniť príkaz, ktorým sa požaduje prístup, môžu spôsobiť neúčinnosť tejto doložky, pokiaľ nie je možné ju 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.

***

118. ***Zmluva by mohla zaväzovať dovozcu a/alebo vývozcu, aby bezodkladne informovali dotknutú osobu o žiadosti alebo príkaze, ktoré dostali od orgánov verejnej moci tretej krajiny, alebo o neschopnosti dovozcu splniť zmluvné záväzky s cieľom umožniť dotknutej osobe vyhľadať informácie a domáhať sa účinnej nápravy (napr. podaním sťažnosti príslušnému dozornému a/alebo súdnemu orgánu a preukázaním svojej aktívnej legitimácie na súdoch tretej krajiny).***

119. ***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 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 zverejňovania údajov, a vynaložia maximálne úsilie na to, aby získali výnimku zo zákazu zverejnenia. 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 poskytnutie prístupu.

***

120. ***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.***

121. ***Podmienky účinnosti***

- Vo vnútroštátnych právnych predpisoch a politikách sa môžu stanoviť podmienky, ktoré môžu ohroziť účinnosť stanovených mechanizmov nápravy *ad hoc*.

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

- 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 EÚ. Toto zmluvné opatrenie bude musieť nevyhnutne dopĺňať iné doplňujúce opatrenia.

Toto doplňujúce opatrenie by bolo účinné len za predpokladu, že právo tretej krajiny umožňuje nápravu na vnútroštátnych súdoch alebo ak existuje mechanizmus nápravy *ad hoc*. V každom prípade by však nešlo o účinné doplňujúce opatrenie proti opatreniam sledovania, ak by neexistoval mechanizmus nápravy.

Organizačné opatrenia

122. 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 EÚ.

123. 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 opatrenia:

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

124. ***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 určenie osobitného tímu, ktorý by mal mať sídlo v rámci EHP a ktorý by pozostával z odborníkov na právne predpisy v oblasti IT a ochrany údajov a súkromia, s cieľom zaoberať sa žiadosťami, ktoré sa týkajú osobných údajov prenášaných z EÚ; oznámenie vrcholovému manažmentu v právnej a podnikovej oblasti a vývozcovi údajov po prijatí takýchto žiadostí; procesné kroky na napadnutie neprimeraných alebo nezákonných žiadostí a poskytovanie transparentných informácií dotknutým osobám.***

125. 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.

126. ***Podmienky účinnosti:***

- O týchto politikách možno uvažovať len v prípadoch, keď je žiadosť orgánov verejnej moci v tretej krajine zlučiteľná s právom EÚ.[87] 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 doplňujúce opatrenia na zabránenie prístupu.

Opatrenia v oblasti transparentnosti a zodpovednosti

127. ***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 mal v prípade potreby poskytnúť dotknutým osobám.***

128. ***Podmienky účinnosti:***

- Vnútroštátne právne predpisy tretej krajiny môžu zabrániť zverejneniu 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 doklady a záznamy, čím vývozcovi ponúkne možnosť pozastaviť prenosy, ak by takáto neschopnosť viedla k zníženiu úrovne ochrany.

***

129. ***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.***

130. ***Podmienky účinnosti:***

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

Organizačné metódy a opatrenia na minimalizáciu údajov

131. ***V kontexte prenosov môžu byť užitočné môžu 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 „need-to-know“, monitorované***

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

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 rámci EHP, napríklad v prípadoch poskytovania podpory, keď sa poskytne obmedzený prístup namiesto úplného prístupu; alebo ak si poskytovanie služby vyžaduje len prenos obmedzeného súboru údajov, a nie celej databázy).

132. ***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 údajov.
- 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 zverejneniu identifikovateľných údajov.

***

133. ***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.***

134. ***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 dodatočných 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 noriem a najlepších postupov

135. ***Prijatie prísnych politík v oblasti bezpečnosti údajov a ochrany údajov založených na certifikácii EÚ alebo kódexoch správania alebo medzinárodných normách (napr. normy ISO) a najlepších postupoch (napr. ENISA) s náležitým ohľadom na najnovší stav techniky v súlade s rizikom kategórií spracúvaných údajov a pravdepodobnosťou pokusov orgánov verejnej moci o prístup k nim.***

Iné

136. ***Prijatie a pravidelné preskúmanie vnútorných politík s cieľom posúdiť vhodnosť vykonaných doplnkových opatrení a v prípade potreby určenie a zavedenie dodatočných alebo alternatívnych***

riešení s cieľom zabezpečiť, aby sa pri prenášaných osobných údajoch zachovala úroveň ochrany rovnocenná ochrane, aká je zaručená v rámci EÚ.

***

137. ***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 rovnocennú ochrane, aká sa poskytuje v rámci EÚ.***[88]

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

PRÍLOHA 3: MOŽNÉ ZDROJE INFORMÁCIÍ NA ÚČELY POSÚDENIA TRETEJ KRAJINY

138. Váš dovozca údajov by vám mal byť schopný poskytnúť relevantné zdroje a informácie týkajúce sa tretej krajiny, v ktorej je usadený, a právnych predpisov, ktoré sa na neho vzťahujú. Môžete sa odvolať aj na viacero zdrojov informácií, napríklad na tie, ktorých neúplný zoznam je uvedený ďalej:

- judikatúra Súdneho dvora Európskej únie (SDEÚ) a Európskeho súdu pre ľudské práva (ESĽP)[89], ako sa uvádza v odporúčaniach týkajúcich sa základných európskych záruk,[90]
- rozhodnutia o primeranosti v krajine určenia, ak sa prenos opiera o iný právny základ,[91]
- uznesenia a správy od medzivládnych organizácií ako je Rada Európy,[92] iné regionálne orgány[93]; a orgány OSN a agentúr (napr. Rada OSN pre ľudské práva,[94] Výbor pre ľudské práva[95]),
- vnútroštátna judikatúra alebo rozhodnutia prijaté nezávislými súdnymi alebo správnymi orgánmi príslušnými v oblasti ochrany údajov a ochrany údajov tretích krajín,
- správy od akademických inštitúcií a organizácií občianskej spoločnosti (napr. mimovládnych organizácií a odborových združení).

[89] Pozri prehľad judikatúry ESĽP o hromadnom sledovaní: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf.
[90] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions.
[91] C-311/18 (Schrems II), bod 141; pozri rozhodnutia o primeranosti https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
[92] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions.
[93] Pozri napríklad správy Medziamerickej komisie pre ľudské práva (IACHR) o jednotlivých krajinách, https://www.oas.org/en/iachr/reports/country.asp.
[94] Pozri https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx.
[95] Pozri: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5.