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

Doporučení č. 01/2020 o opatřeních, která doplňují nástroje pro předávání s cílem zajistit soulad s úrovní ochrany osobních údajů v EU

Přijato dne 10. listopadu 2020

Shrnutí

Obecné nařízení EU o ochraně osobních údajů (nařízení GDPR) bylo přijato, aby sloužilo dvojímu účelu: aby usnadnilo volný pohyb osobních údajů v rámci Evropské unie a současně aby ochránilo základní práva a svobody fyzických osob, zejména jejich práva na ochranu osobních údajů.

Ve svém nedávném rozsudku ve věci C-311/18 (Schrems II) nám Soudní dvůr Evropské unie (SDEU) připomíná, že ochrana osobních údajů v Evropském hospodářském prostoru (EHP) musí být zaručena všude tam, kam se předávají údaje. Předávání osobních údajů do třetích zemí nemůže být způsobem, jak znehodnotit nebo omezit ochranu, která je poskytována v EHP. Soudní dvůr tento závěr potvrzuje rovněž tím, že objasňuje, že úroveň ochrany v třetích zemích nemusí být stejná jako úroveň zaručená v EHP, ale musí být v zásadě rovnocenná. Soudní dvůr rovněž stvrzuje platnost standardních smluvních doložek jakožto nástroje pro předávání, který může sloužit k smluvnímu zajištění v zásadě rovnocenné úrovně ochrany údajů předávaných do třetích zemí.

Standardní smluvní doložky a jiné nástroje pro předávání uvedené v článku 46 obecného nařízení o ochraně osobních údajů nepůsobí v právním vakuu. Soudní dvůr konstatuje, že správci či zpracovatelé, kteří jsou vývozci údajů, jsou odpovědní za to, aby případ od případu a eventuálně ve spolupráci s dovozcem ve třetí zemi ověřili, zda právo nebo praxe dané třetí země nesnižuje účinnost vhodných záruk, které poskytují nástroje pro předávání uvedené v článku 46 obecného nařízení o ochraně osobních údajů. V těchto případech Soudní dvůr stále ponechává otevřenou možnost, aby vývozci zavedli další opatření, která zaplní tyto nedostatky v oblasti ochrany a zajistí dodržení úrovně požadované právem EU. Soudní dvůr neupřesňuje, o jaká opatření by mohlo jít. Zdůrazňuje však, že vývozci je budou muset určit případ od případu. To je v souladu se zásadou odpovědnosti uvedenou v čl. 5 odst. 2 obecného nařízení o ochraně osobních údajů, která správcům ukládá povinnost, aby nesli odpovědnost za soulad se zásadami obecného nařízení o ochraně osobních údajů týkajícími se zpracování osobních údajů a aby byli schopni tento soulad prokázat.

Evropský sbor pro ochranu osobních údajů (EDPB) přijal tato doporučení, protože chce pomoci vývozcům (ať už jde o správce či zpracovatele, soukromé subjekty či veřejné orgány, kteří zpracovávají osobní údaje spadající do oblasti působnosti obecného nařízení o ochraně osobních údajů) v jejich složitém úkolu posoudit třetí země a případně určit vhodná další opatření. Tato doporučení nabízí vývozcům řadu kroků, podle kterých mají postupovat, možné zdroje informací a několik příkladů dalších opatření, která by mohla být zavedena.

Jako **první krok** vám vývozcům sbor EDPB radí, abyste **se seznámili s tím, jaké údaje předáváte**. Zmapování všech případů předávání osobních údajů do třetích zemí může být složité. Je však nezbytné být si vědomi toho, kam osobní údaje směřují, abyste mohli zajistit, že se jim dostává v zásadě rovnocenné úrovně ochrany, ať už jsou zpracovávány kdekoliv. Musíte rovněž ověřit, že údaje, které předáváte, jsou přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou předávány a zpracovávány ve třetí zemi.

Druhým krokem je **ověřit, zda nástroje pro předávání, které při předávání používáte**, jsou uvedeny ve výčtu v kapitole V obecného nařízení o ochraně osobních údajů. Pokud Evropská komise již prohlásila danou zemi, region nebo odvětví, jemuž předáváte údaje, za území či odvětví s odpovídající ochranou, a to prostřednictvím jednoho ze svých rozhodnutí o odpovídající ochraně podle článku 45 obecného nařízení o ochraně osobních údajů nebo podle starší směrnice 95/46, je-li toto rozhodnutí i nadále platné, nemusíte podnikat žádné další kroky, pouze monitorovat, zda je rozhodnutí o odpovídající ochraně i nadále platné. Pokud nebylo vydáno rozhodnutí o odpovídající ochraně, musíte k pravidelným a opakovaným předáním používat jeden z nástrojů pro předávání podle článku

46 obecného nařízení o ochraně osobních údajů. Pouze v případě příležitostného a neopakovaného předávání údajů můžete využít jednu z odchylek uvedenou v článku 49 obecného nařízení o ochraně osobních údajů, splňujete-li dané podmínky.

Třetím krokem je **posoudit**, zda **ve třetí zemi existují právní předpisy nebo praxe**, které snižují účinnost vhodných záruk nástrojů pro předávání, které používáte, a to v souvislosti s vaším konkrétním předáváním údajů. Vaše posouzení by se mělo primárně zaměřovat na právní předpisy třetích zemí, které jsou relevantní pro vaše předání a pro nástroj pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, jejž používáte, a které mohou znehodnotit úroveň ochrany. Pokud jde o hodnocení prvků, které je třeba vzít v úvahu při posuzování právních předpisů třetí země týkajících se přístupu k údajům ze strany orgánů veřejné moci za účelem sledování, viz doporučení EDPB o evropských základních zárukách (*EDPB European Essential Guarantees recommendations*). Obezřetný postup je zejména na místě tehdy, pokud právní předpis upravující přístup k údajům ze strany orgánů veřejné moci je víceznačný nebo pokud není veřejně k dispozici. Pokud zcela chybí právní předpisy upravující okolnosti, za kterých mohou orgány veřejné moci získávat přístup k osobním údajům a pokud přesto chcete provést předání údajů, měli byste prozkoumat jiné relevantní a objektivní faktory a nespoléhat se na subjektivní faktory, jako je pravděpodobnost přístupu orgánů veřejné moci k vašim údajům způsobem, který není v souladu se standardy EU. Toto posouzení byste měli provést s náležitou pečlivostí a důkladně je zdokumentovat, protože ponesete zodpovědnost za rozhodnutí, které na základě tohoto posouzení přijmete.

Čtvrtým krokem je **určit a přijmout další opatření**, která jsou nezbytná k zajištění, aby úroveň ochrany předávaných údajů byla v zásadě rovnocenná se standardem EU. Tento krok je nezbytný pouze v případě, pokud při posuzování zjistíte, že právní předpis třetí strany je v rozporu s účinností nástroje pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, který v souvislosti s předáváním údajů používáte nebo který chcete používat. Součástí těchto doporučení (v příloze 2) je orientační seznam příkladů dalších opatření s některými podmínkami, které jsou nutné k zajištění jejich účinnosti. Stejně jako v případě vhodných záruk poskytovaných nástroji pro předávání podle článku 46 mohou být některá další opatření účinná v některých zemích, ale ne nutně v jiných. Ponesete zodpovědnost za posouzení jejich účinnosti v souvislosti s předáním a s ohledem na právo dané třetí země a na nástroj pro předávání, který používáte, a budete zodpovědní za rozhodnutí, jež přijmete. Je možné, že budete také muset kombinovat několik dalších opatření. V konečném důsledku můžete dospět k závěru, že žádné další opatření nemůže zajistit v zásadě rovnocennou úroveň ochrany konkrétně vašeho předávání údajů. V těchto případech, kdy není vyhovující žádné další opatření, musíte zabránit předávání, pozastavit je nebo je ukončit, abyste předešli narušení úrovně ochrany osobních údajů. Rovněž byste měli s náležitou pečlivostí provést posouzení dalších opatření a toto posouzení zdokumentovat.

Pátým krokem je **podniknout** veškeré **kroky v rámci formálního postupu**, které mohou být nezbytné pro přijetí vašich dalších opatření, a to v závislosti na tom, který nástroj pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů používáte. Tyto formality jsou v těchto doporučeních dále upřesněny. Možná bude také zapotřebí, abyste některé z nich prodiskutovali se svými příslušnými dozorovými úřady.

V rámci **šestého a posledního kroku** musíte opětovně ve vhodných intervalech zhodnotit úroveň ochrany zaručenou údajům, jež předáváte do třetích zemí, a sledovat, zda nedošlo nebo nedojde k jakýkoliv změnám, které na tuto úroveň mohou mít vliv. V souladu se zásadou odpovědnosti je třeba soustavně dohlížet na úroveň ochrany osobních údajů.

Dozorové úřady budou i nadále vykonávat svůj mandát v oblasti sledování uplatňování obecného nařízení o ochraně osobních údajů a budou tento mandát vynucovat. Dozorové úřady budou věnovat náležitou pozornost opatřením, která vývozci přijímají, aby zajistili, že údajům, které předávají, je zajištěna v zásadě rovnocenná úroveň ochrany. Jak připomíná Soudní dvůr, dozorové úřady dočasně nebo trvale zakáží předávání údajů v případech, kdy v návaznosti na provedení šetření nebo obdržení stížnosti dospějí k závěru, že nelze zajistit v zásadě rovnocennou úroveň ochrany.

Dozorové úřady budou i nadále vypracovávat pokyny pro vývozce a koordinovat svoji činnost v rámci EDPB s cílem zajistit jednotné uplatňování právních předpisů EU v oblasti ochrany údajů.

Obsah

Evropský sbor pro ochranu osobních údajů

s ohledem na čl. 70 odst. 1 písm. e) nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „obecné nařízení o ochraně osobních údajů“),

s ohledem na Dohodu o Evropském hospodářském prostoru (EHP), a zejména na přílohu XI a protokol 37 k této dohodě ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018[1],

s ohledem na články 12 a 22 svého jednacího řádu,

vzhledem k těmto důvodům:

(1) Soudní dvůr Evropské unie (SDEU) ve svém rozsudku ze dne 16. července 2020 ve věci *Data Protection Commissioner v. Facebook Ireland LTD, Maximillian Schrems*, C-311/18 dospěl k závěru, že čl. 46 odst. 1 a čl. 46 odst. 2 písm. c) obecného nařízení o ochraně osobních údajů musí být vykládány v tom smyslu, že vhodné záruky, vymahatelná práva a účinná právní ochrana vyžadované uvedenými ustanoveními musí zajistit, aby se na práva osob, jejichž osobní údaje jsou předávány do třetí země na základě standardních doložek o ochraně osobních údajů, vztahovala úroveň ochrany, která je v zásadě rovnocenná úrovni ochrany zaručené v Evropské unii tímto nařízením ve spojení s Listinou základních práv Evropské unie.[2]

(2) Jak zdůraznil Soudní dvůr, musí být zaručena úroveň ochrany fyzických osob, která je v zásadě rovnocenná úrovni zaručené v rámci Evropské unie obecným nařízením o ochraně osobních údajů ve spojení s Listinou, bez ohledu na ustanovení kapitoly V, podle které předávání osobních údajů do třetí země probíhá. Ustanovení kapitoly V mají zajistit kontinuitu vysoké úrovně této ochrany, jsou-li osobní údaje předávány do třetí země.[3]

(3) V 108. bodě odůvodnění a čl. 46 odst. 1 obecného nařízení o ochraně osobních údajů se stanoví, že nebude-li přijato rozhodnutí o odpovídající ochraně EU, měl by správce nebo zpracovatel v zájmu odstranění nedostatků v oblasti ochrany údajů ve třetí zemi přijmout opatření, která subjektu údajů poskytnou vhodné záruky. Správce nebo zpracovatel mohou stanovit vhodné záruky, aniž by bylo zapotřebí jakékoliv zvláštní povolení od dozorového úřadu, a to prostřednictvím použití jednoho z nástrojů pro předávání uvedeného v čl. 46 odst. 2 obecného nařízení o ochraně osobních údajů, jako jsou standardní doložky o ochraně údajů.

[1] Pokud se v tomto dokumentu hovoří o „členských státech”, rozumějí se tím „členské státy EHP“.
[2] Rozsudek SDEU ze dne 16. července 2020, *Data Protection Commissioner v. Facebook Ireland LTD, Maximillian Schrems*, (dále jenC-311/18 (Schrems II)), druhé konstatování.
[3] C-311/18 (Schrems II), body 92 a 93.

(4) Soudní dvůr vyjasnil, že cílem standardních doložek o ochraně osobních údajů přijatých Komisí není nic jiného než poskytnout správcům a zpracovatelům usazeným v Evropské unii smluvní záruky uplatňované jednotně ve všech třetích zemích. Tyto standardní doložky o ochraně osobních údajů nemohou s ohledem na svou smluvní povahu být závazné pro orgány veřejné moci třetích zemí, neboť ty stranami dané smlouvy nejsou. Může se tedy stát, že vývozci údajů budou muset doplnit záruky obsažené v těchto standardních doložkách o ochraně osobních údajů o další opatření s cílem zajistit dodržování úrovně ochrany v dané třetí zemi vyžadované unijním právem. Soudní dvůr odkázal na 109. bod odůvodnění obecného nařízení o ochraně osobních údajů, který tuto možnost zmiňuje, a vybízí správce a zpracovatele, aby ji využili.[4]

(5) Soudní dvůr uvedl, že je především na správci či zpracovateli, aby případ od případu – a eventuálně ve spolupráci s dovozcem údajů – ověřili, zda právo třetí země, do které jsou údaje předávány, zajišťuje v souladu s unijním právem v zásadě rovnocennou ochranu osobních údajů předávaných na základě standardních doložek o ochraně osobních údajů, a v případě potřeby poskytl k zárukám poskytovaným těmito doložkami další záruky.[5]

(6) Nemohou-li správce nebo zpracovatel usazení v Unii přijmout další opatření dostatečná pro zajištění v zásadě rovnocenné ochrany v souladu s unijním právem, mají tento správce nebo zpracovatel, či případně příslušný dozorový úřad, povinnost pozastavit nebo ukončit předávání osobních údajů do dotyčné třetí země.[6]

(7) Obecné nařízení o ochraně osobních údajů ani Soudní dvůr nestanoví ani neupřesňují „další záruky“ či „další opatření“ k zárukám poskytovaným nástroji pro předávání podle čl. 46. odst. 2 obecného nařízení o ochraně osobních údajů, které správci a zpracovatelé mohou přijmout, aby zajistili soulad s úrovní ochrany požadovanou podle unijního práva v dané třetí zemi.

(8) Sbor EDPB se z vlastního podnětu rozhodl, že tuto otázku prozkoumá a nabídne správcům a zpracovatelům v pozici vývozců doporučení ohledně procesu, podle kterého mohou postupovat při určování a přijímání dalších opatření. Cílem těchto doporučení je stanovit metodiku pro vývozce, aby určili, zda a která další opatření bude pro jejich předávání zapotřebí zavést. Je povinností především vývozců zajistit, aby předávané údaje získaly v třetí zemi takovou úroveň ochrany, která je v zásadě rovnocenná úrovni zaručené v rámci EU. Prostřednictvím těchto doporučení se sbor EDPB snaží podporovat soudržné uplatňování obecného nařízení o ochraně osobních údajů a rozsudek Soudního dvora v souladu s mandátem sboru EDPB[7].

PŘIJAL TOTO DOPORUČENÍ:

[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] Čl. 70 odst. 1 písm. e) obecného nařízení o ochraně osobních údajů.

1 ODPOVĚDNOST V RÁMCI PŘEDÁVÁNÍ ÚDAJŮ

1. Primární právo EU považuje právo na ochranu údajů za jedno ze základních práv.[8] Proto se právu na ochranu údajů přikládá vysoká úroveň ochrany a omezení je možné přijmout pouze tehdy, pokud jsou stanovena zákonem a respektují podstatu tohoto práva a pokud jsou přiměřená, nezbytná a pokud skutečně odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého.[9] Právo na ochranu osobních údajů není absolutním právem, nýbrž musí být posuzováno v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality vyváženo s ostatními základními právy.[10]

2. Úroveň ochrany, která je v zásadě rovnocenná s úrovní zaručenou v rámci EU, musí být údajům poskytována i v situaci, kde budou údaje předány do třetích zemí mimo EHP s cílem zajistit, že není znehodnocena úroveň ochrany zaručená obecným nařízením o ochraně osobních údajů.

3. Právo na ochranu údajů je aktivní povahy. Ukládá povinnost vývozcům a dovozcům (ať už jsou správci a/nebo zpracovateli, či nikoliv) učinit více než jen uznání nebo pasivní soulad s tímto právem.[11] Správci a zpracovatelé musí aktivně a soustavně usilovat o zajištění souladu s právem na ochranu údajů prováděním právních, technických a organizačních opatření zaručujících účinnost. Správci a zpracovatelé musí být rovněž schopni doložit toto úsilí subjektům údajů, široké veřejnosti a dozorovým úřadům v oblasti ochrany údajů. Jde o tzv. zásadu odpovědnosti.[12]

4. Zásada odpovědnosti, která je nezbytná k zajištění účinného uplatňování úrovně ochrany, kterou přiznává obecné nařízení o ochraně osobních údajů, platí i pro předávání údajů do třetích zemí[13], protože se samo o sobě jedná o jednu z forem zpracování údajů.[14] Jak zdůraznil Soudní dvůr ve svém rozsudku, musí být zaručena úroveň ochrany, která je v zásadě rovnocenná úrovni zaručené v rámci Evropské unie obecným nařízením o ochraně osobních údajů ve spojení s Listinou, bez ohledu na ustanovení uvedené kapitoly, podle které předávání osobních údajů do třetí země probíhá.[15]

5. V rozsudku Schrems II Soudní dvůr zdůraznil povinnost vývozců a dovozců zajistit, že zpracování osobních údajů bylo a bude i nadále prováděno v souladu s úrovní ochrany stanovenou právem EU v oblasti ochrany údajů a pozastavit předávání údajů a/nebo odstoupit od smlouvy, jestliže dovozce údajů nemůže nebo již nemůže zajistit dodržování standardních doložek o ochraně osobních údajů obsažených v příslušné smlouvě mezi vývozcem a dovozcem.[16] Správce či zpracovatel v pozici vývozce musejí zajistit, aby dovozci případně spolupracovali s vývozcem při plnění těchto povinností tím, že ho budou informovat například o veškerých změnách ovlivňujících úroveň ochrany obdržených osobních

[8] Čl. 8 odst. 1 Listiny základních práv a čl. 16 odst. 1 SFEU, 1. bod odůvodnění, čl. 1 odst. 2 obecného nařízení o ochraně osobních údajů.
[9] Čl. 52 odst. 1 Listiny základních práv Evropské unie.
[10] 4. bod odůvodnění obecného nařízení o ochraně osobních údajů a věc C-507/17 Google LLC právní nástupkyně Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL), bod 60.
[11] C-92/09 a C-93/02, Volker und Markus Schecke GbR v. Land Hessen, stanovisko generální advokátky Sharpstonové ze dne 17. června 2010, bod 71.
[12] Čl. 5 odst. 2 a čl. 28 odst. 3 písm. h) obecného nařízení o ochraně osobních údajů.
[13] Článek 44 a 101. bod odůvodnění obecného nařízení o ochraně osobních údajů, jakož i čl. 47 odst. 2 písm. d) obecného nařízení o ochraně osobních údajů.
[14] Rozsudek SDEU ze dne 6. října 2015 ve věci *Maximillian Schrems v. Data Protection Commissioner*, (dále jen 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.

údajů v zemi dovozce.[17] Tyto povinnosti jsou uplatněním zásady odpovědnosti uvedené v obecném nařízení o ochraně osobních údajů na předávání údajů.[18]

2 POSTUP: UPLATNĚNÍ ZÁSADY ODPOVĚDNOSTI NA PŘEDÁVÁNÍ ÚDAJŮ V PRAXI

6. Následuje seznam kroků, které je třeba podniknout v zájmu zjištění, zda vy (jako vývozce údajů) musíte zavést další opatření, abyste mohli v souladu s předpisy předávat údaje do zemí mimo EHP. Zájmenem „vy“ se v tomto dokumentu rozumí správce nebo zpracovatel, který je vývozcem údajů a který zpracovává osobní údaje v rámci oblasti působnosti obecného nařízení o ochraně osobních údajů – včetně zpracování ze strany soukromých a veřejných subjektů, pokud předávají údaje soukromým subjektům.[19] Pokud jde o předávání osobních údajů, k němuž dochází mezi orgány veřejné moci, jsou zvláštní pokyny stanoveny v *Pokynech č. 2/2020 k čl. 46 odst. 2 písm. a) a čl. 46 odst. 3 písm. b) nařízení 2016/679 v případě předávání osobních údajů mezi orgány a subjekty veřejné moci v EHP i mimo něj.*[20]

7. Budete muset toto posouzení a další opatření, pro která se rozhodnete a která zavedete, náležitě zdokumentovat a tuto dokumentaci na žádost zpřístupnit příslušnému dozorovému úřadu.[21]

2.1 Krok 1: Seznamte se s tím, jaké údaje předáváte

8. Pokud se chcete dozvědět, jaká opatření se od vás (vývozce údajů) mohou vyžadovat, abyste mohli pokračovat v předávání údajů nebo provádět nová předání osobních údajů[22], musíte se v prvním kroku ujistit, že jste si plně vědomi, jaké údaje předáváte (seznamte se s tím, jaké údaje předáváte). Zaznamenávání a mapování veškerých předání může být složité pro subjekty, které se účastní většího počtu, rozmanitého a pravidelného předávání se třetími zeměmi a používají mnoho různých zpracovatelů a dílčích zpracovatelů. Seznámit se s tím, jaké údaje předáváte, je významným prvním krokem ke splnění vašich povinnosti v rámci zásady odpovědnosti.

9. Abyste získali úplný přehled o tom, které údaje předáváte, můžete využít záznamů o činnostech zpracování, které jste možná povinni vést jako správce nebo zpracovatel v souladu s článkem 30 obecného nařízení o ochraně osobních údajů.[23] Rovněž vám mohou být nápomocná předchozí

[17] C-311/18 (Schrems II), bod 134.
[18] Čl. 5 odst. 2 a čl. 28 odst. 3 písm. h) obecného nařízení o ochraně osobních údajů.
[19] Pokyny EDPB č. 3/2018 k místní působnosti obecného nařízení o ochraně osobních údajů (článek 3) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_cs.
[20] Pokyny EDPB č. 2/2020 k čl. 46 odst. 2 písm. a) a čl. 46 odst. 3 písm. b) nařízení 2016/679 v případě předávání osobních údajů mezi orgány a subjekty veřejné moci v EHP i mimo něj, viz https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en.
[21] Čl. 5 odst. 2 obecného nařízení o ochraně osobních údajů a čl. 24 odst. 1 obecného nařízení o ochraně osobních údajů.
[22] Upozorňujeme, že v případě vzdáleného přístupu ze strany subjektu ze třetí země k údajům uloženým v EHP se také jedná o předávání údajů.
[23] Viz článek 30 obecného nařízení o ochraně osobních údajů, zejména pak odst. 1 písm. e) a odst. 2 písm. c). Kromě toho by vaše záznamy o zpracování měly obsahovat popis činností zpracování (včetně, ale nikoliv výlučně kategorií subjektů údajů, kategorií osobních údajů a účelů zpracování a zvláštních informací o předání údajů). Někteří správci a zpracovatelé jsou osvobozeni od povinnosti vést záznamy o zpracování (čl. 30 odst. 5 obecného nařízení o ochraně osobních údajů). Pro pokyny k této výjimce viz pracovní skupina zřízená podle článku 29,

opatření za účelem splnění povinností informovat subjekty údajů v souladu s čl. 13 odst. 1 písm. f) a čl. 14 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů o tom, že předáváte jejich osobní údaje do třetích zemí.[24]

10. Při mapování předávání nezapomeňte také zohlednit další předávání, například zda vaši zpracovatelé mimo EHP nepředávají osobní údaje, které jste jim svěřili, dílčímu zpracovateli v jiné třetí zemi nebo v téže třetí zemi[25].

11. V souladu se zásadou „minimalizace údajů" podle obecného nařízení o ochraně osobních údajů,[26] musíte ověřit, že údaje, které předáváte, jsou přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou předávány a zpracovávány ve třetí zemi.

12. Tyto činnosti musí být provedeny před samotným předáním údajů a musí být aktualizovány před znovuzahájením předávání po pozastavení operací předávání údajů: musíte se seznámit s tím, kde se mohou nacházet osobní údaje, které jste vyvezli, nebo kde je dovozci zpracovávají (mapa míst určení).

13. Mějte na paměti, že vzdálený přístup ze třetí země (například v rámci podpory) a/nebo skladování na cloudu nacházejícím se mimo EHP se rovněž považuje za předání.[27] Konkrétněji pak pokud používáte mezinárodní cloudovou infrastrukturu, musíte posoudit, zda vaše údaje budou předány do třetích zemí a kam, ledaže poskytovatel cloudu jasně uvede ve své smlouvě, že údaje vůbec nebudou zpracovávány ve třetích zemích.

2.2 Krok 2: Určete nástroje pro předávání, které používáte

14. V druhém kroku, který musíte učinit, určíte nástroje pro předávání, které používáte, a to mezi nástroji vyjmenovanými a stanovenými v kapitole V obecného nařízení o ochraně osobních údajů.

Rozhodnutí o odpovídající ochraně

15. Evropská komise může na základě svých **rozhodnutí o odpovídající ochraně** týkajících se některých nebo všech třetích zemí, jimž předáváte osobní údaje, uznat, že tyto země zajišťují dostatečnou úroveň ochrany osobních údajů.[28]

Poziční dokument o výjimkách z povinnosti vést záznamy o činnostech zpracování v souladu s čl. 30 odst. 5 obecného nařízení o ochraně osobních údajů (schváleno sborem EDPB dne 25. května 2018).

[24] Podle pravidel transparentnosti obecného nařízení o ochraně osobních údajů musíte informovat subjekty údajů o předávání osobních údajů do třetích zemí (čl. 13 odst. 1 písm. f) a čl. 14 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů). Zejména je musíte informovat o tom, zda existuje rozhodnutí o odpovídající ochraně vydané Evropskou komisí, či nikoliv, nebo v případě předání uvedených v článcích 46 a 47 obecného nařízení o ochraně osobních údajů nebo v čl. 49 odst. 1 druhém pododstavci obecného nařízení o ochraně osobních údajů odkázat na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny. Informace poskytnuté subjektu údajů musejí být správné a aktuální, zejména s ohledem na judikaturu Soudního dvora týkající se předávání.

[25] Pokud správce udělil předchozí konkrétní nebo obecné písemné povolení v souladu s čl. 28 odst. 2 obecného nařízení o ochraně osobních údajů.

[26] Čl. 5 odst. 1 písm. c) obecného nařízení o ochraně osobních údajů.

[27] Viz často kladenou otázku č. 11 *„je třeba připomenout, že i poskytnutí přístupu k údajům ze třetí země, například pro administrativní účely, také znamená předání"*, EDPB, Často kladené otázky k rozsudku Soudního dvora Evropské unie ve věci C-311/18 – Data Protection Commissioner v. Facebook Ireland Ltd a Maximillian Schrems, 23. července 2020.

[28] Evropská komise má pravomoc určit na základě článku 45 obecného nařízení o ochraně osobních údajů, zda daná země mimo EU poskytuje odpovídající úroveň ochrany osobních údajů. Obdobně má Evropská komise pravomoc určit, zda odpovídající úroveň ochrany poskytuje mezinárodní organizace.

16. Toto rozhodnutí o odpovídající ochraně má ten účinek, že osobní údaje mohou směřovat ze zemí EHP do dané třetí země, aniž by byl nezbytný jakýkoliv nástroj pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů.

17. Rozhodnutí o odpovídající ochraně se mohou týkat země jako celku nebo mohou být omezena na její část. Rozhodnutí o odpovídající ochraně mohou zahrnovat veškeré předávání údajů do dané země nebo mohou být omezena na některé druhy předávání (např. v jednom odvětví).[29]

18. Evropská komise zveřejňuje seznam svých rozhodnutí o odpovídající ochraně na svých webových stránkách.[30]

19. Pokud předáváte osobní údaje do třetích zemí, regionů nebo odvětví, na které se vztahuje rozhodnutí Komise o odpovídající ochraně (v rozsahu v jakém se vztahuje na dané předání), **nemusíte podnikat žádné další kroky uvedené v těchto doporučeních.**[31] Musíte však i nadále monitorovat, zda nebyla zrušena či zneplatněna rozhodnutí o odpovídající ochraně, která jsou relevantní pro vaše předávání.[32]

20. Rozhodnutí o odpovídající ochraně však nebrání subjektům údajů podat stížnost. Nebrání ani dozorovým úřadům předložit věc vnitrostátnímu soudu, pokud mají pochybnosti o platnosti rozhodnutí, aby tak vnitrostátní soud mohl předložit žádost o rozhodnutí o předběžné otázce SDEU za účelem přezkoumání platnosti rozhodnutí.[33]

Příklad: Občan EU, pan Schrems, podal v červnu 2013 stížnost irské Komisi pro ochranu údajů (*Data Protection Commission*, DPC) a požádal tento dozorový úřad, aby trvale nebo dočasně zakázal předávání jeho osobních údajů ze strany společnosti Facebook Ireland do USA, protože se domníval, že právní předpisy a praxe v USA nezajišťují odpovídající ochranu osobních údajů uložených na území této země před sledováním prováděným zde orgány veřejné moci. Úřad DPC stížnost zamítl z důvodu, že ve svém rozhodnutí 2000/520 Komise konstatovala, že v rámci režimu „bezpečného přístavu" zajišťují USA odpovídající úroveň ochrany předaných osobních údajů (rozhodnutí o bezpečném přístavu). Pan Schrems toto rozhodnutí úřadu DPC napadl a irský vrchní soud postoupil otázku platnosti rozhodnutí 2000/520 Soudnímu dvoru Evropské unie (SDEU). SDEU následně rozhodl o prohlášení neplatnosti rozhodnutí Komise 2000/520 o odpovídající ochraně poskytované podle zásad „bezpečného přístavu".[34]

[29] Čl. 45 odst. 1 obecného nařízení o ochraně osobních údajů.

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

[31] Pokud jste vy a dovozce údajů zavedli opatření za účelem souladu s ostatními povinnostmi podle obecného nařízení o ochraně osobních údajů; v opačném případě tato opatření zaveďte.

[32] Evropská komise je povinna pravidelně přezkoumávat veškerá rozhodnutí o odpovídající ochraně a sledovat, zda třetí země, které z nich mají prospěch, i nadále zajišťují odpovídající úroveň ochrany (viz čl. 45 odst. 3 a čl. 45 odst. 4 obecného nařízení o ochraně osobních údajů). Rozhodnutí o odpovídající ochraně může prohlásit za neplatné i SDEU (viz jeho rozsudky ve věci C-362/14 (Schrems I) a C-311/18 (Schrems II)).

[33] C-311/18 (Schrems II), body 118–120. Dozorové úřady nesmějí rozhodnutí o odpovídající ochraně přehlížet a dočasně nebo trvale zakázat předávání osobních údajů do těchto zemí s odvoláním pouze na nedostatečnou úroveň ochrany. Mohou vykonávat pouze svou pravomoc dočasně nebo trvale zakázat předávání osobních údajů do dané třetí země z jiných důvodů (např. nedostatečná bezpečnostní opatření v rozporu s článkem 32 obecného nařízení o ochraně osobních údajů, zpracování údajů není založeno na žádném platném právním základu, a je tedy v rozporu s článkem 6 obecného nařízení o ochraně osobních údajů). Dozorové úřady mohou zcela nezávisle přezkoumat, zda je předávání těchto údajů v souladu s požadavky stanovenými obecným nařízením o ochraně osobních údajů a případně podat žalobu vnitrostátním soudům, aby tyto soudy mohly podat žádost o rozhodnutí o předběžné otázce Soudnímu dvoru Evropské unie za účelem přezkoumání platnosti rozhodnutí Komise o odpovídající ochraně, pokud o ní mají pochybnosti.

[34] Věc C-362/14 (Schrems I).

Nástroje pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů

21. V článku 46 obecného nařízení o ochraně osobních údajů se uvádí řada nástrojů pro předávání obsahujících *„vhodné záruky*“, které mohou vývozci využít k předání osobních údajů do třetích zemí, pokud neexistuje rozhodnutí o odpovídající ochraně. Hlavními druhy nástrojů pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů jsou tyto:

    - standardní doložky o ochraně údajů (SSD),
    - závazná podniková pravidla,
    - kodexy chování,
    - mechanismy pro vydání osvědčení,
    - ad hoc smluvní doložky.

22. Ať už se rozhodnete pro kterýkoliv nástroj pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, musíte zajistit, že celkově budou vámi předané osobní údaje požívat v zásadě rovnocenné úrovně ochrany.

23. Nástroje pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů obsahují hlavně vhodné záruky smluvní povahy, které se mohou vztahovat na předávání údajů do všech třetích zemí. Situace ve třetí zemi, do které předáváte údaje, může přesto vyžadovat, abyste tyto nástroje pro předávání a záruky, jež obsahují, doplnili o doplňující opatření („další opatření“) s cílem zajistit v zásadě rovnocennou úroveň ochrany.[35]

Výjimky

24. Kromě rozhodnutí o odpovídající ochraně a nástrojů pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů obsahuje obecné nařízení o ochraně osobních údajů třetí cestu, jak v jistých situacích umožnit předávání osobních údajů. Jsou-li splněny zvláštní podmínky, můžete stále předávat osobní údaje na základě výjimky uvedené v článku 49 obecného nařízení o ochraně osobních údajů.

25. Článek 49 obecného nařízení o ochraně osobních údajů je výjimečné povahy. Výjimky, které obsahuje, musí být vykládány restriktivně a musí se týkat zejména činností zpracování, které jsou příležitostné a neopakují se. Sbor EDPB vydal Pokyny 2/2018 k výjimkám podle článku 49 nařízení (EU) 2016/679. [36]

26. Než své předávání založíte na výjimce podle článku 49 obecného nařízení o ochraně osobních údajů, musíte ověřit, zda vaše předávání splňuje přísné podmínky, které toto ustanovení stanoví pro každé předání.

***

27. Pokud vaše předávání nemůže být zákonně založeno na rozhodnutí o odpovídající ochraně ani na výjimce podle článku 49, musíte pokračovat krokem 3.

[35] C-311/18 (Schrems II), body 130 a 133. Viz také bod 2.3 níže.
[36] Pro další pokyny k této problematice viz https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_cs.

2.3 Krok 3: Posuďte, zda je nástroj pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, který využíváte, účinný s ohledem na všechny okolnosti předávání

28. Vybrat si nástroj pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů někdy nemusí stačit. Nástroj pro předávání musí zajistit, aby úroveň ochrany zaručená obecným nařízením o ochraně osobních údajů nebyla předáním znehodnocena.[37] Jinými slovy, váš nástroj pro předávání musí být účinný i v praxi.

29. Pojmem „účinný“ se zde rozumí, že předávaným osobním údajům se ve třetí zemi poskytuje úroveň ochrany, která je v zásadě rovnocenná úrovni, která je zaručena v EHP.[38] Tak tomu není v případě, pokud je vývozci údajů znemožněno splnit své povinnosti v souladu se zvoleným nástrojem pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů kvůli právním předpisům a praxi v dané třetí zemi, které se použijí na předávání.

30. Proto musíte posoudit, případně též ve spolupráci s dovozcem, zda ve třetí zemi existuje právní předpis nebo praxe, která snižuje účinnost vhodných záruk nástrojů pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, které používáte, v souvislosti s konkrétně vaším předáváním údajů. Ve vhodných případech by vám dovozce údajů měl poskytnout příslušné zdroje a informace týkající se třetí země, ve které je usazen, a o právních předpisech, jimiž se předávání řídí. Můžete také využít jiné zdroje informací, například ty, které jsou uvedeny v orientačním výčtu v příloze 3.[39]

31. Vaše hodnocení by mělo zohledňovat veškeré subjekty, které se účastní předání (např. správce, zpracovatele a dílčí zpracovatele zpracovávající údaje ve třetí zemi), které jste určili v rámci mapování předávání údajů. Čím více správců, zpracovatelů či dovozců se do předávání zapojuje, tím složitější bude vaše posouzení. V tomto posouzení můžete také zohlednit veškerá další předání, ke kterým může dojít.

32. Za tímto účelem budete muset prozkoumat charakteristiky každého vašeho předání a určit, jak se na tato předání použije vnitrostátní právní řád země, do níž se údaje předávají (nebo do které se dále předávají).

33. Příslušná právní situace bude záviset na okolnostech předání, konkrétně:

- účelech, za kterými jsou údaje předávány a zpracovávány (např. marketing, lidské zdroje, ukládání, podpora IT, klinická hodnocení),
- druzích subjektů zapojených do zpracování (veřejné/soukromé, správce/zpracovatel),
- odvětví, ve kterém k předání dochází (např. reklamní technologie, telekomunikace, finančnictví atd.),
- kategoriích předávaných osobních údajů (např. osobní údaje týkající se dětí mohou v třetí zemi spadat do působnosti zvláštních právních předpisů),
- zda budou údaje uloženy ve třetí zemi nebo zda existuje pouze vzdálený přístup k uloženým údajům v rámci EU/EHP,
- formátu údajů určených k předání (tj. prostý text / pseudonymizované nebo zašifrované[40]),

[37] Článek 44 obecného nařízení o ochraně osobních údajů.
[38] C-311/18 (Schrems II), body 105 a druhý bod nálezu.
[39] Viz také bod 43 níže v tomto dokumentu.
[40] Některé třetí země neumožňují dovoz zašifrovaných údajů.

- možnosti, že údaje mohou být dále předány ze třetí země do jiné třetí země.[41]

34. V rámci platných právních předpisů budete muset posoudit, zda kterýkoliv z nich neporušuje závazky obsažené v nástroji pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, který jste si zvolili. Měli byste ověřit, zda je v praxi možné účinně uplatňovat závazky umožňující subjektům údajů vykonávat svá práva v souvislosti s mezinárodními předáváními (jako je žádost o přístup, opravu nebo smazání v souvislosti s předávanými údaji) a zda tomu nebrání právo v třetí zemi určení.

35. Budete muset posoudit platná pravidla obecné povahy, pokud mají dopad na účinné uplatňování záruk obsažených v nástroji pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů a základní práva fyzických osob (zejména právo na soudní ochranu přiznané subjektu údajů v případě přístupu k předávaným údajům ze strany orgánů veřejné moci třetí země).

36. V každém případě byste měli věnovat zvláštní pozornost všem relevantním právním předpisům, zejména těm, které stanoví požadavky na zpřístupnění osobních údajů orgánům veřejné moci nebo na poskytnutí pravomocí těmto orgánům veřejné moci získat přístup k osobním údajům (například pro účely prosazování trestního práva, regulačního dohledu a pro účely národní bezpečnosti). Pokud jsou tyto pravomoci omezeny na to, co je nezbytné a přiměřené v demokratické společnosti,[42] nemusí mít vliv na závazky obsažené v nástroji pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, který používáte.

37. Standardy EU, například články 47 a 52 Listiny základních práv EU, je třeba použít jako referenční bod k posouzení, zda se tento přístup ze strany orgánů veřejné moci omezuje na to, co je nezbytné a přiměřené v demokratické společnosti, a zda je subjektům údajů přiznána účinná soudní ochrana.

38. Při provádění tohoto posouzení jsou rovněž relevantní různé aspekty právního řádu dané třetí země, tj. prvky uvedené v čl. 45 odst. 2 obecného nařízení o ochraně osobních údajů.[43] Například stav právního státu v dané třetí zemi může být relevantní pro posouzení účinnosti mechanismů dostupných pro fyzické osoby, které chtějí získat (soudní) ochranu před nezákonným přístupem vlády k osobním údajům. Existence komplexního zákona na ochranu údajů nebo nezávislého úřadu pro ochranu osobních údajů, jakož i skutečnost, že je země stranou mezinárodních nástrojů zajišťujících záruky pro ochranu údajů, může přispět k zajištění přiměřenosti vládního zásahu.[44]

***

39. Doporučení EDPB o evropských základních zárukách stanoví prvky, které musejí být posouzeny za účelem určení, zda je možné považovat právní rámec upravující přístup k osobním údajům ze strany orgánů veřejné moci ve třetí zemi, ať už jde o agentury národní bezpečnosti nebo donucovací orgány, za odůvodněný zásah (a proto za zásah, který neohrožuje závazky přijaté v rámci nástroje pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů), či nikoliv. Obezřetný postup

[41] Pokud správce udělil předchozí konkrétní nebo obecné písemné povolení v souladu s čl. 28 odst. 2 obecného nařízení o ochraně osobních údajů.

[42] Viz články 47 a 52 Listiny základních práv EU, čl. 23 odst. 1 obecného nařízení o ochraně osobních údajů a doporučení EDPB č. 02/2020 o evropských základních zárukách týkajících se opatření v oblasti sledování, 10. listopadu 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[43] C-311/18 (Schrems II), bod 104.

[44] Například: úmluva č. 108 (Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat, ETS č. 108) nebo úmluva 108+ (Modernizovaná úmluva o ochraně osob se zřetelem na zpracování osobních dat, CETS č. 223) stanoví v případě porušení ochrany údajů vymahatelné, mezinárodní právní opravné prostředky a přispívá k zajištění minimální úrovně ochrany osobních údajů a respektování soukromého života.

je zejména na místě tehdy, pokud právní předpis upravující přístup k údajům ze strany orgánů veřejné moci je víceznačný nebo pokud není veřejně k dispozici.

40. Doporučení EDPB o evropských základních zárukách může posloužit jako vodítko pro situace předávání údajů na základě nástroje pro předávání podle článku 46 vývozcům a dovozcům údajů při posuzování, zda takovéto pravomoci neodůvodněně nezasahují do povinností dovozce údajů zajistit v zásadě rovnocennou úroveň ochrany.

41. To, že úroveň ochrany není v zásadě rovnocenná, bude zejména patrné, pokud právní předpis nebo praxe třetí země relevantní pro vaše předání nesplňuje požadavky evropských základních záruk.

42. Vaše posouzení musí být v první řadě založeno na veřejně dostupných právních předpisech. Avšak v některých situacích to nebude stačit, protože příslušné třetí země nemusí žádný takový právní předpis mít nebo může být nedostatečný. Pokud si v takovém případě přesto chcete naplánovat předání údajů, měli byste prozkoumat jiné relevantní a objektivní faktory[45] a nespoléhat se na ty subjektivní, jako je pravděpodobnost přístupu veřejných orgánů k vašim údajům způsobem, který není v souladu se standardy EU. Toto posouzení byste měli provést s náležitou pečlivostí a důkladně je zdokumentovat, protože ponesete zodpovědnost za rozhodnutí, které na základě tohoto posouzení přijmete.[46]

43. Své posouzení můžete provést na základě informací získaných z jiných zdrojů[47], například:

- prvky prokazující, že orgány třetí země budou usilovat o získání přístupu k údajům s vědomím či bez vědomí dovozce údajů s ohledem na oznámené precedenty, právní předpisy a praxi,
- prvky prokazující, že orgány třetí země budou schopny získat přístup k údajům prostřednictvím dovozce údajů nebo prostřednictvím přímého zachycení komunikačního kanálu s ohledem na oznámené precedenty, právní pravomoci a technické, finanční a lidské zdroje, které mají orgány k dispozici.

44. Ve svém posouzení můžete v konečném důsledku zjistit, že nástroj pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, který používáte, a vhodné záruky, které obsahuje:

- účinně zajišťuje, že předávaným osobním údajům se ve třetí zemi poskytuje úroveň ochrany, která je v zásadě rovnocenná úrovni zaručené v rámci EHP. Právní předpisy a postupy třetí země platné pro předávání údajů staví dovozce údajů do postavení, kdy musí splnit své povinnosti v souladu se zvoleným nástrojem pro předávání. Měli byste je opětovně hodnotit v pravidelných intervalech, nebo když zjistíte významné změny (viz krok 6),
- nezajišťuje účinně v zásadě rovnocennou úroveň ochrany. Dovozce údajů nemůže splnit své povinnosti kvůli právním předpisům třetí země a/nebo postupům, které platí pro předání. SDEU zdůraznil, že pokud nástroje pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů nejsou dostatečné, je povinností vývozce údajů, aby buď zavedl účinná další opatření, nebo aby osobní údaje nepředával.[48]

[45] Viz bod 43 níže v tomto dokumentu, jakož i přílohu 3.
[46] Čl. 5 odst. 2 obecného nařízení o ochraně osobních údajů.
[47] Viz také přílohu 3.
[48] SDEU, C-311/18 (Schrems II), body 134–135.

SDEU například rozhodl, že § 702 amerického zákona FISA nesplňuje minimální požadavky, které jsou v právu EU svázané se zásadou proporcionality, takže nelze mít za to, že jde o omezení na to, co je nezbytně nutné. To znamená, že úroveň ochrany programů povolených § 702 zákona FISA není v zásadě rovnocenná zárukám, které stanoví právo EU. Pokud tedy dovozce údajů nebo jakýkoliv další příjemce, jemuž dovozce údaje může zpřístupnit údaje, spadá do působnosti § 702 zákona FISA[49], je možné na toto předání použít standardní doložky o ochraně údajů (SSD) nebo jiné nástroje pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, jestliže další technická opatření znemožňují přístup k předaným údajům nebo jestliže činí tento přístup neúčinným.

2.4 Krok 4: Přijměte další opatření

45. Pokud v rámci posouzení v kroku 3 zjistíte, že váš nástroj pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů není účinný, budete muset zvážit, případně ve spolupráci s dovozcem, zda existují další opatření, která by v kombinaci se zárukami obsaženými v nástroji pro předávání mohla zajistit, aby byla předávaným údajům poskytnuta ve třetí zemi taková úroveň ochrany, která je v zásadě rovnocenná úrovni ochrany zaručené v Unii.[50] „Další opatření“ ze své podstaty doplňují záruky, které již poskytuje nástroj pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů.[51]

46. Musíte jednotlivě případ od případu určit, která další opatření by mohla být účinná pro soubor předání do dané třetí země při použití daného nástroje pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů. Budete moci vycházet ze svých předchozích posouzení v rámci jednotlivých kroků (1, 2 a 3 výše) a ověřit s ohledem na závěry těchto posouzení případnou účinnost dalších opatření při zaručování požadované úrovně ochrany.

47. V zásadě mohou být další opatření smluvní, technické nebo organizační povahy. Kombinace různých opatření tak, aby se navzájem podporovala a posilovala, může zvýšit úroveň ochrany, a proto může přispět k dosažení standardů EU.

48. Smluvní a organizační opatření sama o sobě zpravidla nestačí k tomu, aby se zabránilo přístupu k osobním údajům ze strany orgánů veřejné moci dané třetí země (pokud tento přístup neodůvodněně zasahuje do povinností dovozce údajů zajistit v zásadě rovnocennou úroveň ochrany). Může totiž dojít k situacím, kdy mohou přístup k osobním údajům ze strany orgánů veřejné moci ve třetích zemích, zejména za účelem sledování, znemožnit či učinit neúčinným pouze technická opatření.[52] V takovýchto

[49] § 702 zákona FISA se použije, pokud jsou údaje získány „od poskytovatele služeb elektronických komunikací nebo s jeho pomocí“ (§ 702 zákona FISA = hlava 50 § 1881a písm. h) odst. 2 pododstavec A podbod vi) Sbírky zákonů USA, který je pak definován v hlavě 50 § 1881 písm. b) odst. 4 Sbírky zákonů USA takto:
„(A) provozovatel telekomunikací ve smyslu definice uvedené v § 153 hlavy 47;
(B) poskytovatel služeb elektronických komunikací ve smyslu definice uvedené v § 2510 hlavy 18;
(C) poskytovatel výpočetní služby na dálku ve smyslu definice uvedené v § 2711 hlavy 18;
(D) jakýkoliv další poskytovatel komunikačních služeb, který má přístup k telegrafické nebo elektronické komunikaci, ať už v rámci vysílání těchto komunikací, nebo v rámci jejich skladování, nebo
(E) úředník, zaměstnanec nebo agent subjektu popsaného v pododstavcích (A), (B), (C) nebo (D).“.

[50] C-311/18 (Schrems II), bod 96.

[51] 109. bod odůvodnění obecného nařízení o ochraně osobních údajů a věc C-311/18 (Schrems II), bod 133.

[52] Pokud jde tento přístup nad rámec toho, co je nezbytné a přiměřené v demokratické společnosti; viz články 47 a 52 Listiny základních práv EU, čl. 23 odst. 1 obecného nařízení o ochraně osobních údajů a doporučení EDPB 02/2020 o evropských základních zárukách týkajících se opatření v oblasti sledování, 10. listopadu 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

situacích mohou smluvní či organizační opatření doplňovat technická opatření a posilovat celkovou úroveň ochrany údajů, například vytvořením překážek pro pokusy orgánů veřejné moci získat přístup k údajům způsobem, který není v souladu se standardy EU.

49. Ve spolupráci s dovozcem údajů můžete, pokud je to vhodné, prozkoumat následující (orientační) seznam faktorů s cílem určit, která další opatření by byla nejúčinnější pro ochranu předávaných údajů:

- formát údajů určených k předání (tj. prostý text / pseudonymizované nebo zašifrované),
- povaha údajů,
- délka a složitost pracovních toků zpracovávání údajů, počet subjektů zapojených do zpracování a vztahy mezi nimi (např. zda se předávání účastní více správců nebo jak správci, tak zpracovatelé, nebo zda jsou zapojeni zpracovatelé, kteří budou údaje od vás předávat vašemu dovozci údajů (vzhledem k příslušným ustanovením, která pro ně budou platit podle právních předpisů třetí země určení)),[53]
- možnost, že údaje mohou být dále předávány v rámci téže třetí země, nebo dokonce do jiné třetí země (např. zapojení dílčích zpracovatelů dovozce údajů[54]).

Příklady dalších opatření

50. Některé příklady technických, smluvních a organizačních opatření, která je možné zvážit, můžete nalézt v orientačních seznamech popsaných v příloze 2.

***

51. Pokud jste zavedli účinná další opatření, která v kombinaci s vámi zvoleným nástrojem pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů dosahují takové úrovně ochrany, která je nyní v zásadě rovnocenná úrovni ochrany zaručené v rámci EHP: můžete přistoupit k předávání údajů.

52. Pokud nejste schopni najít nebo provést účinná další opatření, která zajistí, aby předávané osobní údaje požívaly v zásadě rovnocenné úrovně ochrany,[55] nesmíte zahájit předávání osobních údajů do dotčené třetí země na základě nástroje pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, který používáte. Pokud již předávání údajů provádíte, máte povinnost předávání osobních údajů pozastavit nebo ukončit.[56] V souladu se zárukami obsaženými v nástroji pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, který používáte, by dovozce měl údaje, které jste již předali do dané třetí země, a jejich kopie vrátit vám nebo zničit v celém rozsahu.[57]

[53] Obecné nařízení o ochraně osobních údajů uděluje správcům a zpracovatelům různé povinnosti. Předávání může probíhat mezi správci, mezi společnými správci, od správce zpracovateli a od zpracovatelů správcům nebo mezi zpracovateli na základě povolení správce.
[54] Viz poznámka pod čarou 25.
[55] Pokud jde tento přístup nad rámec toho, co je nezbytné a přiměřené v demokratické společnosti; viz články 47 a 52 Listiny základních práv EU, čl. 23 odst. 1 obecného nařízení o ochraně osobních údajů a doporučení EDPB 02/2020 o evropských základních zárukách týkajících se opatření v oblasti sledování, 10. listopadu 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] Viz doložku 12 v příloze k rozhodnutí 87/2010 o SSD, viz (dobrovolný) dodatečný závěrečný odstavec uvedený v příloze B rozhodnutí 2004/915/ES.

Příklad: právní řád třetí země zakazuje další opatření, která jste určili (např. zakazuje použití šifrování), nebo jinak brání jejich účinnosti. Do této země nesmíte zahájit předávání osobních údajů nebo musíte do této země zastavit v současnosti probíhající předávání.

53. Pokud se rozhodnete, že budete i nadále provádět předávání bez ohledu na skutečnost, že dovozce není schopen dostát závazkům přijatým v rámci nástroje pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, měli byste uvědomit příslušný dozorový úřad v souladu s konkrétními ustanoveními vloženými do daného nástroje pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů.[58] Příslušný dozorový úřad dočasně nebo trvale zakáže předávání údajů v případech, kdy dospěje k závěru, že nelze zajistit v zásadě rovnocennou úroveň ochrany.[59]

54. Příslušný dozorový úřad může uložit jakákoliv další nápravná opatření (např. pokutu), pokud navzdory skutečnosti, že nemůžete prokázat v zásadě rovnocennou úroveň ochrany v dané třetí zemi, zahájíte předávání údajů nebo v něm budete pokračovat.

2.5 Krok 5: Procesní kroky, pokud jste určili účinná další opatření

55. Procesní kroky, které možná budete muset podniknout v případě, že jste určili účinná další opatření, která je třeba zavést, se mohou lišit v závislosti na nástroji pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, který používáte nebo zamýšlíte použít.

2.5.1 Standardní doložky o ochraně údajů („SSD“) (čl. 46 odst. 2 písm. c) a d) obecného nařízení o ochraně osobních údajů)

56. Pokud máte v úmyslu zavést další opatření doplňující SSD, není nutné, abyste žádali o povolení příslušného dozorového úřadu přidat tento druh doložek nebo dalších záruk, pokud určená další opatření nejsou v přímém nebo nepřímém rozporu s SSD a pokud jsou dostatečná k zajištění, že není znehodnocena úroveň ochrany zaručená obecným nařízením o ochraně osobních údajů.[60] Vývozce a dovozce údajů musejí zajistit, že není možné žádným způsobem vykládat další doložky jako způsob omezení práv a povinností stanovených v SSD ani za způsob snížení úrovně ochrany. Toto byste měli schopni být prokázat, včetně jednoznačnosti všech doložek, a to v souladu se zásadou odpovědnosti a vaším závazkem zajistit dostatečnou úroveň ochrany údajů. Příslušné dozorové úřady mají pravomoc tyto doplňující doložky přezkoumávat, bude-li to potřeba (například v případě stížnosti nebo šetření z vlastního podnětu).

[58] Viz Často kladené otázky EDPB k rozsudku Soudního dvora Evropské unie ve věci C-311/18 - Data Protection Commissioner v. Facebook Ireland Ltd a Maximillian Schrems, přijaté dne 23. července 2020, a zejména často kladené otázky č. 5, 6 a 9. Viz také doložku 4 písm. g) rozhodnutí Komise 2010/87/EU, jakož i doložku 5 písm. a) rozhodnutí Komise 2001/497/ES a „soubor II“ doložku II písm. c) přílohy rozhodnutí Komise 2004/915/ES.

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

[60] 109. bod odůvodnění obecného nařízení o ochraně osobních údajů uvádí: „Skutečnost, že správci a zpracovatelé mohou používat standardní doložky o ochraně údajů přijaté Komisí nebo dozorovým úřadem, by neměla správcům ani zpracovatelům bránit v tom, aby zahrnuli standardní doložky o ochraně údajů i do rozsáhlejších smluv, jako je smlouva mezi zpracovatelem a dalším zpracovatelem, nebo doplnili jiné doložky či další záruky, pokud tyto nejsou v přímém nebo nepřímém rozporu se standardními smluvními doložkami přijatými Komisí nebo dozorovým úřadem nebo pokud se nedotýkají základních práv či svobod subjektů údajů.“ Podobná ustanovení se poskytují v souborech SSD přijatých Evropskou komisí v souladu se směrnicí 95/45/ES.

57. Pokud máte v úmyslu změnit standardní doložky o ochraně údajů nebo pokud doplněná další opatření „jsou v rozporu“ přímo nebo nepřímo se standardními doložkami o ochraně údajů, má se za to, že již nepoužíváte standardní doložky o ochraně údajů (SSD)[61], a musíte požádat o povolení příslušný dozorový úřad v souladu s čl. 46 odst. 3 písm. a) obecného nařízení o ochraně osobních údajů.

2.5.2 Závazná podniková pravidla (čl. 46 odst. 2 písm. b) obecného nařízení o ochraně osobních údajů)

58. Argumentace použitá v rozsudku ve věci Schrems II platí i pro jiné nástroje pro předávání podle čl. 46 odst. 2 obecného nařízení o ochraně osobních údajů, protože všechny tyto nástroje jsou v zásadě smluvní povahy, tudíž záruky stanovené zde stranami ani jejich přijaté závazky nemohou zavazovat orgány veřejné moci třetích zemí.[62]

59. Rozsudek ve věci Schrems II je relevantní pro předávání osobních údajů na základě závazných podnikových pravidel, protože právní předpisy třetích zemí mohou mít vliv na ochranu, kterou tyto nástroje poskytují. Konkrétní dopad rozsudku Schrems II na závazná podniková pravidla se stále projednává. Sbor EDPB poskytne, jakmile to bude možné, více podrobností, zda může být nutné do závazných podnikových pravidel začlenit další závazky, v referenčních dokumentech WP256/257.[63]

60. Soudní dvůr zdůraznil, že je odpovědností vývozce údajů a dovozce údajů, aby posoudili, zda úroveň ochrany vyžadovaná právem Unie je v dotyčné třetí zemi dodržována, a stanovili, zda lze v praxi dodržet záruky poskytované standardními smluvními doložkami (SSD) a závaznými podnikovými pravidly. Pokud tomu tak není, měli byste posoudit, zda můžete pomocí dalších opatření zajistit úroveň ochrany, která je v zásadě rovnocenná úrovni ochrany poskytované v EHP, a zda právní předpisy nebo praxe dané třetí země nenaruší tato další opatření a nezabrání jejich účinnosti.

2.5.3 Ad hoc smluvní doložky (čl. 46 odst. 3 písm. a) obecného nařízení o ochraně osobních údajů)

61. Argumentace použitá v rozsudku ve věci Schrems II platí i pro jiné nástroje pro předávání podle čl. 46 odst. 2 obecného nařízení o ochraně osobních údajů, protože všechny tyto nástroje jsou v zásadě smluvní povahy, tudíž záruky stanovené zde stranami ani jejich přijaté závazky nemohou zavazovat orgány veřejné moci třetích zemí.[64] Rozsudek ve věci Schrems II je proto relevantní pro předávání osobních údajů na základě ad hoc smluvních doložek, protože právní předpisy třetích zemí mohou mít vliv na ochranu, kterou tyto nástroje poskytují. Konkrétní dopad rozsudku Schrems II na ad hoc doložky se stále projednává. Sbor EDPB poskytne více podrobností, jakmile to bude možné.

---

[61] Viz analogicky Stanovisko EDPB 17/2020 k návrhu standardních smluvních doložek předloženému slovinským dozorovým úřadem (čl. 28 odst. 8 obecného nařízení o ochraně osobních údajů) k již přijatým SSD podle článku 28, jež obsahuje podobné ustanovení („Sbor dále připomíná, že možnost použít standardní smluvní doložky přijaté dozorovým úřadem nebrání stranám v tom, aby doplňovaly další doložky nebo další záruky za předpokladu, že tyto nebudou přímo nebo nepřímo v rozporu s přijatými standardními smluvními doložkami nebo nebudou zasahovat do základních práv nebo svobod subjektů údajů. Dále, pokud budou standardní doložky pozměněny, nebude se mít za to, že strany provedly přijaté standardní smluvní doložky“), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_cs.pdf.

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

[63] Pracovní skupina zřízená podle článku 29, Pracovní dokument, kterým se zavádí tabulka s prvky a zásadami nacházejícími se v závazných podnikových pravidlech, naposledy revidovaný a přijatý dne 6. února 2018, WP 256 rev.01; pracovní skupina zřízená podle článku 29, Pracovní dokument, kterým se zavádí tabulka s prvky a zásadami nacházejícími se v závazných podnikových pravidlech, naposledy revidovaný a přijatý dne 6. února 2018, WP 257 rev.01.

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

2.6 Krok 6: Ve vhodných intervalech provádějte opětovné hodnocení

62. Musíte průběžně monitorovat, případně i ve spolupráci s dovozci údajů, změny v třetí zemi, do které jste předali osobní údaje, které by mohly mít vliv na vaše počáteční posouzení úrovně ochrany a na rozhodnutí, která jste možná následně přijali ohledně předávání údajů. Dodržovat zásadu odpovědnosti platí stále (čl. 5 odst. 2 obecného nařízení o ochraně osobních údajů).

63. Měli byste zavést dostatečně spolehlivé mechanismy, abyste dokázali zajistit, že můžete okamžitě pozastavit nebo ukončit předávání údajů, pokud:

- dovozce porušil závazky, které na sebe vzal v rámci nástroje pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, nebo těmto závazkům není schopen dostát, nebo
- další opatření již nejsou v dané třetí zemi účinná.

3 ZÁVĚR

64. Obecné nařízení o ochraně osobních údajů stanoví pravidla pro zpracování osobních údajů EHP a tím umožňuje volný pohyb osobních údajů v rámci tohoto prostoru. Kapitola V obecného nařízení o ochraně osobních údajů upravuje předávání osobních údajů do třetích zemí a nastavuje vysokou laťku: předání nesmí znehodnotit úroveň ochrany fyzických osob zaručenou obecným nařízením o ochraně osobních údajů (článek 44 obecného nařízení o ochraně osobních údajů). V rozsudku ve věci C-311/18 (Schrems II) SDEU zdůraznil nutnost zajistit kontinuitu úrovně ochrany poskytované podle obecného nařízení o ochraně osobních údajů osobním údajům předávaným do třetí země.[65]

65. Máte-li zajistit v zásadě rovnocennou úroveň ochrany vašich údajů, musíte se v první řadě důkladně seznámit s okolnostmi vašeho předávání. Musíte rovněž zkontrolovat, že údaje, které předáváte, jsou přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou předávány a zpracovávány ve třetí zemi.

66. Také musíte určit nástroje pro předávání, které pro svá předání používáte. Pokud nástrojem pro předání není rozhodnutí o odpovídající ochraně, musíte jednotlivě případ od případu ověřit, zda právní řád či praxe dané třetí země určení neznehodnocuje v souvislosti s vašimi předáváními záruky obsažené v nástroji pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů. Pokud nástroj pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů sám o sobě nedokáže osobním údajům, které předáváte, zajistit úroveň ochrany, která je v zásadě rovnocenná, mohou tuto mezeru vyplnit další opatření.

67. Pokud nejste schopni najít nebo provést účinná další opatření, která zajistí, aby předávané osobní údaje požívaly v zásadě rovnocenné úrovně ochrany, nesmíte zahájit předávání osobních údajů do dotčené třetí země na základě vámi zvoleného nástroje pro předávání. Pokud již předávání údajů provádíte, máte povinnost okamžitě předávání osobních údajů pozastavit nebo ukončit.

68. Příslušný dozorový úřad má pravomoc pozastavit nebo ukončit předávání osobních údajů do třetí země, pokud není zaručena taková ochrana předávaných údajů, kterou vyžaduje právo EU, zejména články 45 a 46 obecného nařízení o ochraně osobních údajů a Listina základních práv.

Za Evropský sbor pro ochranu osobních údajů

předsedkyně

(Andrea Jelinek)

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

PŘÍLOHA 1: DEFINICE

- „Třetí zemí“ se rozumí jakákoliv země, která není členským státem EHP.
- „EHP“ se rozumí Evropský hospodářský prostor a zahrnuje členské státy Evropské unie a Island, Norsko a Lichtenštejnsko. Na tyto tři uvedené státy se obecného nařízení o ochraně osobních údajů vztahuje na základě dohody o EHP a zejména její přílohy XI a protokolu č. 37.
- „Obecným nařízením o ochraně osobních údajů“ se rozumí nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
- „Listinou“ se rozumí Listina základních práv Evropské unie, Úř. věst. C 326, 26.10.2012, s. 391–407.
- Zkratkou „SDEU“ se rozumí Soudní dvůr Evropské unie. Jedná se o soudní orgán Evropské unie a ve spolupráci se soudy členských států zajišťuje jednotné uplatňování a výklad práva EU.
- „Dovozcem údajů“ se rozumí správce nebo zpracovatel v rámci EHP, který předává osobní údaje správci nebo zpracovateli ve třetí zemi.
- „Vývozcem údajů“ se rozumí správce nebo zpracovatel ve třetí zemi, který přijímá osobní údaje předávané z EHP nebo k nim získává přístup.
- „Nástrojem pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů“ se rozumí vhodné záruky podle článku 46 obecného nařízení o ochraně osobních údajů, které zavedou vývozci údajů při předávání osobních údajů do třetí země v případě, že neexistuje rozhodnutí o odpovídající ochraně v souladu s čl. 45 odst. 3 obecného nařízení o ochraně osobních údajů. V čl. 46 odst. 2 a 3 obecného nařízení o ochraně osobních údajů je uveden seznam nástrojů pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, které mohou správci a zpracovatelé využít.
- Zkratkou „SSD“ se rozumí standardní doložky o ochraně údajů (či „standardní smluvní doložky“) přijaté Evropskou komisí pro předávání osobních údajů mezi správci či zpracovateli v EHP a správci či zpracovateli v zemích mimo EHP. Standardní smluvní doložky přijaté Evropskou komisí jsou podle obecného nařízení o ochraně osobních údajů jedním z nástrojů pro předávání, a to v souladu s čl. 46 odst. 2 písm. c) a čl. 46 odst. 5 obecného nařízení o ochraně osobních údajů.

PŘÍLOHA 2: PŘÍKLADY DALŠÍCH OPATŘENÍ

69. Následující opatření slouží jako příklady dalších opatření, která můžete zvážit, pokud dospějete ke kroku 4 „Přijměte další opatření“. Tento seznam není vyčerpávající. Výběr a provedení jednoho nebo několika z těchto opatření nezajistí nutně a systematicky, že vaše předání bude splňovat standard v zásadě rovnocenné ochrany, který ukládá právo EU. Měli byste vybrat ta další opatření, který mohou tuto úroveň ochrany vašim předáním účinně zaručit.

70. Jakákoliv další opatření mohou být považována za účinná ve smyslu rozsudku SDEU ve věci „Schrems II“, pokud odstraňují konkrétní nedostatky zjištěné ve vašem posouzení právní situace ve třetí zemi a v rozsahu, v jakém tyto nedostatky odstraňují. Pokud v konečném důsledku nemůžete zajistit v zásadě rovnocennou úroveň ochrany, nesmíte osobní údaje předávat.

71. Jako správce nebo zpracovatel již můžete být povinni provádět některá z opatření popsaných v této příloze, i pokud se na vašeho dovozce údaje vztahuje rozhodnutí o odpovídající ochraně, obdobně jako jste možná povinni je provést při zpracovávání údajů v rámci EHP.[66]

Technická opatření

72. Tento oddíl popisuje orientační příklady technických opatření, která mohou doplnit záruky obsažené v nástrojích pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů s cílem zajistit soulad s úrovní ochrany, která je požadována podle práva EU v souvislosti s předáním osobních údajů do třetí země. Tato opatření budou nutná zejména v případě, že právo této třetí země ukládá příjemci osobních údajů povinnosti, které jsou v rozporu se zárukami poskytovanými nástroji pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, a mohou tedy ohrozit smluvní záruku odpovídající úrovně ochrany před přístupem orgánů veřejné moci uvedené třetí země k těmto údajům.[67]

73. Pro větší jasnost tento oddíl uvádí nejprve technická opatření, která by mohla být potenciálně účinná v některých scénářích / případech použití s cílem zajistit v zásadě rovnocennou úroveň ochrany. Potom jsou v tomto oddíle uvedeny některé scénáře / případy použití, kdy nelze najít žádná technická opatření, která by zajistila tuto úroveň ochrany.

Scénáře, pro které je možné najít *účinná* opatření

74. Opatření uvedená níže mají zajistit, aby přístup k předávaným údajům ze strany orgánů veřejné moci ve třetích zemích nesnížil účinnost vhodných záruk obsažených v nástrojích pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů. Tato opatření se použijí, i když je přístup orgánů veřejné moci v souladu s právem země dovozce, pokud jde tento přístup nad rámec toho, co je nezbytné a přiměřené v demokratické společnosti[68]. Cílem těchto opatření je předem zabránit přístupu, který může být v rozporu s právními předpisy, tím, že se orgánům znemožní identifikace subjektů údajů, vyvozování informací o nich, určení jejich identity na základě vyloučení jiných možností

[66] Čl. 5 odst. 2 obecného nařízení o ochraně osobních údajů, článek 32 obecného nařízení o ochraně osobních údajů.
[67] C-311/18 (Schrems II), bod 135.
[68] Viz články 47 a 52 Listiny základních práv EU, čl. 23 odst. 1 obecného nařízení o ochraně osobních údajů a doporučení EDPB o evropských základních zárukách týkajících se opatření v oblasti sledování.

v jiném kontextu nebo přiřazování předaných údajů k jiným souborům údajů, které mohou být v jejich vlastnictví a které mohou obsahovat kromě jiných údajů on-line identifikátory poskytované přístroji, aplikacemi, nástroji a protokoly používanými subjekty údajů v jiných kontextech.

75. Orgány veřejné moci ve třetích zemích mohou usilovat o získání přístupu k předaným údajům

a) během přenosu prostřednictvím přístupu ke komunikačním kanálům používaným k předávání údajů do země příjemce. Tento přístup může být pasivní a v takovémto případě je potom obsah komunikace, případně po provedení procesu výběru, jednoduše zkopírován. Přístup však může být také aktivní v tom smyslu, že se orgány veřejné moci vloží do komunikačního procesu nejen tím, že si přečtou obsah, ale také tím, že jeho části zmanipulují nebo potlačí;

b) zatímco jsou tyto údaje uchovávány zamýšleným příjemcem údajů, a to buď tím, že zažádají o přístup do prostor zpracování jako takových, nebo tím, že uloží příjemci údajů povinnost najít a vytěžit údaje, o které mají orgány zájem, a tyto údaje orgánům předat.

76. Tento oddíl se zabývá scénáři, kdy jsou uplatněna opatření, která jsou účinná v obou případech. Je možné použít i různá další opatření, která mohou být za daných okolností konkrétních případů předání dostatečná, pokud právo přijímající země stanoví pouze jeden druh přístupu. Je proto nezbytné, aby vývozce údajů pečlivě analyzoval, a to i s podporou dovozce údajů, povinnosti uložené dovozci.

Například dovozci údajů v USA, na které se vztahuje hlava 50 § 1881a Sbírky zákonů USA (§ 702 zákona FISA), mají přímou povinnost poskytnout přístup k dovezeným osobním údajům, která jsou v jejich vlastnictví, správě nebo pod jejich kontrolu, nebo tyto údaje postoupit. Tato povinnost může zahrnovat i veškeré šifrovací klíče nezbytné k zajištění nečitelnosti údajů.

77. Tyto scénáře popisují zvláštní okolnosti a přijatá opatření. Jakékoliv změny scénářů mohou vést k odlišným závěrům.

78. Správci možná budou muset použít některá nebo všechna zde popsaná opatření bez ohledu na úroveň ochrany, kterou stanoví platné právní předpisy dovozci údajů, protože musejí za konkrétních okolností předání postupovat v souladu s články 25 a 32 obecného nařízení o ochraně osobních údajů. Jinými slovy, vývozci mohou být povinni provádět opatření popsaná v tomto dokumentu, i pokud se na jejich dovozce údaje vztahuje rozhodnutí o odpovídající ochraně, obdobně jako v případě, kdy správci a zpracovatelé mohou být povinni tato opatření provést při zpracovávání údajů v rámci EHP.

Případ použití 1: Uložení údajů pro účely zálohování a jiné účely, které nevyžadují přístup k nezašifrovaným údajům

79. Vývozce údajů využívá poskytovatele služeb hostingu v třetí zemi za účelem ukládání osobních údajů, např. za účelem zálohování.

Pokud

1. osobní údaje jsou před předáním zpracovány formou silného šifrování;
2. algoritmus šifrování a nastavení jeho parametrů (např. délka klíče, případně provozní mód) jsou v souladu se stavem techniky a je možné je považovat za odolné vůči kryptoanalýze prováděné orgány veřejné moci v zemi příjemce s ohledem na zdroje a technické schopnosti, které mají tyto orgány k dispozici (např. výpočetní kapacita pro útoky hrubou silou);
3. síla šifrování zohledňuje konkrétní časové období, po které je nutné zachovávat důvěrnost zašifrovaných osobních údajů;

4. algoritmus šifrování je bezchybně proveden náležitě spravovaným softwarem, u kterého byl ověřen soulad se specifikací zvoleného algoritmu, například prostřednictvím vydávání osvědčení;
5. správa klíčů je spolehlivá (jejich generování, používání, ukládání, případně přiřazení k totožnosti zamýšleného příjemce a zrušení) a
6. klíče jsou uchovávány pouze pod kontrolou vývozce údajů nebo jiných subjektů pověřených tímto úkolem, kteří mají sídlo v EHP nebo ve třetí zemi nebo na jejím území nebo jde o jedno či více konkrétních odvětví v rámci třetí země, nebo v rámci mezinárodní organizace, u které Komise v souladu s článkem 45 obecného nařízení o ochraně osobních údajů stanovila, že je zajištěna odpovídající úroveň ochrany,

pak se sbor EDPB domnívá, že provedené šifrování představuje účinné další opatření.

Případ použití 2: Předání pseudonymizovaných údajů

80. Vývozce údajů nejprve pseudonymizuje údaje, které má v držení, a pak je předá do třetí země k analýze, např. pro účely výzkumu.

Pokud

1. vývozce údajů předává osobní údaje zpracované takovým způsobem, že tyto osobní údaje již není možné přiřadit ke konkrétnímu subjektu údajů ani je není možné použít k identifikaci subjektu údajů vyloučením jiných možností ve větší skupině, a to bez použití dodatečných informací[69];
2. tyto další informace jsou spravovány výlučně pod kontrolou vývozce údajů a jsou uchovávány v některém členském státě nebo v třetí zemi, území nebo v rámci jednoho či více konkrétních odvětví v rámci třetí země nebo v rámci mezinárodní organizace, u které Komise v souladu s článkem 45 obecného nařízení o ochraně osobních údajů stanovila, že je zajištěna odpovídající úroveň ochrany;
3. zpřístupnění nebo neoprávněnému používání těchto dalších informací se zabrání prostřednictvím technických a organizačních záruk, je zajištěno, že vývozce údajů si zachová výlučnou kontrolu nad algoritmem nebo repozitářem, který umožňuje opětovnou identifikaci pomocí dalších informací, a
4. správce prostřednictvím důkladné analýzy dotčených údajů a s ohledem na veškeré informace, kterými orgány veřejné moci přijímající země mohou disponovat, stanovil, že pseudonymizované osobní údaje není možné přiřadit identifikované nebo identifikovatelné fyzické osobě, a to ani křížovým porovnáním s takovýmito informacemi,

pak se sbor EDPB domnívá, že provedená pseudonymizace představuje účinné další opatření.

81. Upozorňujeme, že v řadě situací mohou prvky fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby, její fyzická lokace nebo její interakce

[69] V souladu s čl. 4 bodem 5 obecného nařízení o ochraně osobních údajů: „‚pseudonymizací' [se rozumí] zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;".

s internetovými službami v daných časových okamžicích[70] umožňovat identifikaci dané osoby, i když není uvedeno její jméno, adresa nebo jiné prosté identifikátory.

82. To platí zvlášť v případě, kdy se údaje týkají využívání informačních služeb (datum přístupu, pořadí navštívených prvků, charakteristika použitých zařízení atd.). Tyto služby mohou, pokud jde o dovozce osobních údajů, podléhat povinnosti udělit přístup týmž orgánům veřejné moci v jejich jurisdikci, které pak budou pravděpodobně disponovat údaji o používání těchto informačních služeb ze strany osoby (osob), na kterou (které) se zaměřují.

83. Kromě toho vzhledem k tomu, že užívání některých informačních služeb je ze své podstaty veřejné, nebo vzhledem k využitelnosti těchto údajů stranami, které mají významné zdroje, budou správci muset postupovat s mimořádnou pečlivostí, protože orgány veřejné moci v jejich jurisdikcích pravděpodobně disponují údaji o využívání informačních služeb osobou, na kterou se zaměřují.

Případ použití 3: Šifrované údaje, které třetími zeměmi pouze tranzitují

84. Vývozce údaje chce předat údaje na místo určení, které se uznává na místo, jež nabízí dostatečnou ochranu v souladu s článkem 45 obecného nařízení o ochraně osobních údajů. Údaje směřují přes třetí zemi.

Pokud

1. vývozce údajů předává osobní údaje dovozci údajů v jurisdikci zajišťující dostatečnou ochranu, údaje se přepravují přes internet a mohou být zeměpisně přesměrovány přes třetí zemi, která nezajišťuje v zásadě rovnocennou úroveň ochrany;
2. použije se přepravní šifrování, u kterého je zaručeno, že použité šifrovací protokoly odpovídají stavu techniky a nabízejí účinnou ochranu před aktivními a pasivními útoky za použití zdrojů, o kterých je známo, že jsou k dispozici orgánům veřejné moci dané třetí země;
3. dešifrování je možné pouze mimo danou třetí zemi;
4. strany, které se komunikace účastní, se dohodnou na důvěryhodném certifikačním orgánu nebo infrastruktuře veřejného klíče;
5. použijí se zvláštní ochranná opatření odpovídající stavu techniky proti aktivním a pasivním útokům na údaje šifrované pro přepravu;
6. v případě, že šifrování pro přepravu nezajišťuje samo o sobě dostatečnou bezpečnost kvůli zkušenostem se slabými místy použité infrastruktury nebo softwaru, jsou osobní údaje rovněž šifrovány prostřednictvím koncového šifrování v aplikační vrstvě za pomoci metod šifrování odpovídajících stavu techniky;
7. algoritmus šifrování a nastavení jeho parametrů (např. délka klíče, případně provozní mód) jsou v souladu se stavem techniky a je možné je považovat za odolné vůči kryptoanalýze prováděné orgány veřejné moci v zemi tranzitu s ohledem na zdroje a technické schopnosti, které mají tyto orgány k dispozice (např. výpočetní kapacita pro útoky hrubou silou);
8. síla šifrování zohledňuje konkrétní časové období, po které je nutné zachovávat důvěrnost zašifrovaných osobních údajů;

[70] Čl. 4 bod 1 obecného nařízení o ochraně osobních údajů: „‚osobními údaji' [se rozumí] veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen ‚subjekt údajů'); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;".

9. algoritmus šifrování je bezchybně proveden náležitě spravovaným softwarem, u kterého byl ověřen soulad se specifikací zvoleného algoritmu, například prostřednictvím vydávání osvědčení;
10. byla vyloučena existence „zadních vrátek“ (u hardwaru či softwaru);
11. správa klíčů ze strany vývozce nebo subjektu, které tento vývozce pověřil v rámci dané jurisdikce, jež nabízí v zásadě rovnocennou úroveň ochrany, je spolehlivá (jejich generování, používání, ukládání, případě přiřazení k totožnosti zamýšleného příjemce a zrušení),

pak se sbor EDPB domnívá, že přepravní šifrování případně v kombinaci s koncovým šifrováním obsahu představuje účinné další opatření.

Případ použití 4: Chráněný příjemce

85. Vývozce údajů předává osobní údaje dovozci údajů ve třetí zemi, který je zvlášť chráněn právním řádem dané země, např. za účelem společného poskytování lékařské péče pacientovi nebo právních služeb klientovi.

Pokud

1. právní řád třetí zemí osvobozuje dovozce údajů, který sídlí v dané zemi, od přístupu k údajům v držení daného příjemce, který by mohl být v rozporu s předpisy, pro konkrétně stanovený účel, např. kvůli povinnosti zachovávat profesní tajemství, která se na dovozce údajů vztahuje;
2. toto osvobození se týká veškerých informací v držení daného dovozce údajů, které mohou být použity k obcházení ochrany výsadních informací (kryptografické klíče, hesla, jiné bezpečnostní údaje atd.);
3. dovozce údajů nevyužívá služby zpracovatele způsobem, který by orgánům veřejné moci umožnil získat přístup k údajům v době, kdy je má v držení zpracovatel, a dovozce údajů ani dále nepředává údaje jinému subjektu, který není chráněn, a to na základě nástroje pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů;
4. osobní údaje jsou šifrovány před odesláním pomocí metody, která odpovídá stavu techniky, což zaručuje, že dešifrování nebude možné bez znalosti dešifrovacího klíče (koncové šifrování), a to po celou dobu, kdy je nutné údaje chránit;
5. dešifrovací klíč je výlučně v držení chráněného dovozce údajů a je vhodně zabezpečen před neoprávněným použitím nebo zpřístupněním prostřednictvím technických a organizačních opatření, která odpovídají stavu techniky, a
6. vývozce údaje spolehlivě určil, že šifrovací klíč, který hodlá použít, odpovídá dešifrovacímu klíči v držení příjemce,

pak se sbor EDPB domnívá, že provedené přepravní šifrování představuje účinné další opatření.

Případ použití 5: Dílčí zpracování nebo zpracování více stran

86. Vývozce údajů chce, aby osobní údaje byly zpracovávány společně dvěma nebo více nezávislými zpracovateli nacházejícími se v různých jurisdikcích, aniž by jim zpřístupnil obsah údajů. Před odesláním údaje rozdělí tak, že žádná část, kterou obdrží jednotliví zpracovatelé, nestačí k celkovému nebo částečnému zrekonstruování osobních údajů. Vývozce údajů přijme výsledek zpracování od každého zpracovatele nezávisle a spojí obdržené části tak, aby dospěl ke konečnému výsledku, který mohou představovat osobní nebo agregované údaje.

Pokud

1. vývozce údajů zpracovává osobní údaje tak, že je rozdělí na dvě či více částí, z nichž žádná již nemůže být vykládána nebo přiřazena ke konkrétnímu subjektu údajů bez použití dalších informací;
2. každá z částí se odesílá samostatnému zpracovateli nacházejícímu se v jiné jurisdikci;
3. zpracovatelé mohou případně zpracovávat údaje společně, např. pomocí zabezpečené metody výpočtu více stran, tak, aby nikomu z nich nebyly odhaleny žádné informace, které nevlastnili před zahájením výpočtů;
4. algoritmus použitý pro sdílený výpočet je zabezpečen před aktivními protivníky;
5. neexistují žádné důkazy o spolupráci mezi orgány veřejné moci nacházejícími se v příslušných jurisdikcích, kde je usazen každý ze zpracovatelů, která by jim umožnila získat přístup ke všem souborům osobních údajů v držení zpracovatelů a umožnila jim rekonstruovat a využít obsah osobních údajů v nezašifrované podobě za okolností, kdy by toto využití nerespektovalo podstatu základních práv a svobod subjektů údajů. Obdobně by orgány veřejné moci kterékoliv země neměly mít pravomoc získat přístup k osobním údajům v držení zpracovatelů ve všech dotčených jurisdikcích;
6. správce prostřednictvím důkladné analýzy dotčených údajů a s ohledem na veškeré informace, kterými orgány veřejné moci přijímajících zemí mohou disponovat, stanovil, že části osobních údajů, které odesílá zpracovatelům, není možné přiřadit identifikované nebo identifikovatelné fyzické osobě, a to ani křížovým porovnáním s těmito informacemi,

pak se sbor EDPB domnívá, že provedené dílčí zpracování představuje účinné další opatření.

Scénáře, pro které není možné najít *žádná účinná* opatření

87. Opatření popsaná níže v určitých situacích nebudou účinně zajišťovat v zásadě rovnocennou úroveň ochrany údajů předávaných do třetí země. Proto je nelze považovat za další opatření.

Případ použití 6: Předání poskytovatelům cloudových služeb nebo jiným zpracovatelům, kteří vyžadují přístup k nezašifrovaným údajům

88. Vývozce údajů používá poskytovatele cloudových služeb nebo jiného zpracovatele, aby nechal zpracovat osobní údaje v souladu s pokyny vývozce ve třetí zemi.

Pokud

1. správce předává údaje poskytovateli cloudových služeb nebo jinému zpracovateli;
2. poskytovatel cloudových služeb nebo jiný zpracovatel potřebuje přístup k nezašifrovaným údajům, aby mohl provést přidělený úkol, a
3. pravomoc svěřená orgánům veřejné moci přijímající země získat přístup k předaným údajům jde nad rámec toho, co je nezbytné a přiměřené v demokratické společnosti,[71]

[71] Viz články 47 a 52 Listiny základních práv EU, čl. 23 odst. 1 obecného nařízení o ochraně osobních údajů a doporučení EDPB o evropských základních zárukách týkajících se opatření v oblasti sledování.

pak si sbor EDPB nedokáže vzhledem k současnému stavu techniky představit účinná technická opatření, která by zabránila tomuto přístupu, který představuje porušení práv subjektů údajů. Sbor EDPB nevylučuje, že díky dalšímu technologickému vývoji budou k dispozici opatření, jak dosáhnout zamýšlených obchodních záměrů bez nutnosti získat přístup k nezašifrovaným údajům.

89. V uvedených scénářích, kdy jsou nezašifrované osobní údaje technicky nezbytné k poskytování služby ze strany zpracovatele, nepředstavuje šifrování, a to ani společně s šifrováním údajů na úložišti („data at rest“), další opatření, které zaručuje v zásadě rovnocennou úroveň ochrany, pokud dovozce údajů vlastní kryptografické klíče.

Případ použití 7: Vzdálený přístup k údajům pro obchodní účely

90. Vývozce údajů zpřístupňuje osobní údaje subjektům ve třetí zemi za účelem použití pro společné obchodní účely. Typickou takovouto situaci mohou představovat správce či zpracovatel usazený na území některého členského státu předávající osobní údaje správci nebo zpracovateli v třetí zemi, která patří do téže skupiny podniků, nebo skupina podniků zapojená do společné hospodářské činnosti. Dovozce údajů může například použít údaje, jichž je příjemcem, k poskytování personalistických služeb vývozci údajů, k čemuž potřebuje personalistické údaje, nebo k telefonické nebo e-mailové komunikaci se zákazníky vývozce údajů, kteří žijí v Evropské unii.

Pokud

1. vývozce údajů předává osobní údaje dovozci údajů ve třetí zemi tím, že je zpřístupňuje v rámci společně používaného informačního systému způsobem, který umožňuje dovozci přímý přístup k údajům podle své volby nebo jejich přímým, individuálním nebo hromadným předáním prostřednictvím použití komunikační služby;
2. dovozce používá nezašifrované údaje pro své vlastní účely;
3. pravomoc svěřená orgánům veřejné moci přijímající země získat přístup k předaným údajům jde nad rámec toho, co je nezbytné a přiměřené v demokratické společnosti,

pak si sbor EDPB nedokáže představit účinná technická opatření, která by zabránila tomuto přístupu, který představuje porušení práv subjektů údajů.

91. V uvedených scénářích, kdy jsou nezašifrované osobní údaje technicky nezbytné k poskytování služby ze strany zpracovatele, nepředstavuje šifrování, a to ani společně s šifrováním údajů na úložišti („data at rest“), další opatření, které zaručuje v zásadě rovnocennou úroveň ochrany, pokud dovozce údajů vlastní kryptografické klíče.

Dodatečná smluvní opatření

92. Tato opatření budou obecně sestávat z jednostranných, dvoustranných nebo vícestranných[72] smluvních závazků.[73] Pokud se použije nástroj pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, bude ve většině případů již obsahovat řadu (většinou smluvních) závazků jak pro vývozce, tak pro dovozce údaje, které mají sloužit jako záruky pro osobní údaje.[74]

93. V některých situacích mohou tato opatření doplňovat a posilovat záruky, které mohou poskytovat nástroj pro předávání a příslušné právní předpisy třetí země, pokud s ohledem na okolnosti daného předání nesplňují veškeré požadované podmínky k zajištění úrovně ochrany, která je v zásadě rovnocenná úrovni zaručované v EU. Vzhledem k povaze smluvních opatření, která obecně nejsou závazná pro orgány dané třetí země, pokud nejsou stranou smlouvy[75], měla by tato opatření být kombinována s jinými technickými a organizačními opatřeními za účelem zajištění požadované úrovně ochrany údajů. Výběr a provedení jednoho nebo několika z těchto opatření nezajistí nutně a systematicky, že vaše předání bude splňovat standard v zásadě rovnocenné ochrany, který ukládá právo EU.

94. Podle toho, jaká smluvní opatření jsou již obsažena v nástroji pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů, který používáte, mohou být dodatečná smluvní opatření rovněž užitečná tím, že umožní vývozcům údajů usazeným v EHP, aby vzali na vědomí nové změny, které mají vliv na ochranu údajů předaných do třetích zemí.

95. Jak již bylo řečeno, smluvní opatření nebudou schopna vyloučit uplatnění právních předpisů třetí země, které nesplňují standardy EDPB týkající se evropských základních záruk v těch případech, kdy právní předpis ukládá dovozcům povinnost vyhovět příkazům zpřístupnit údaje, které obdrží od orgánů veřejné moci.[76]

96. Některé příklady těchto případných smluvních opatření jsou uvedeny níže a jsou roztříděny podle své povahy:

Stanovení smluvní povinnosti používat zvláštní technická opatření

97. ***V závislosti na konkrétních okolnostech předání je možné, že ve smlouvě bude nutné stanovit, že aby mohlo dojít k předání, musí být zavedena zvláštní technická opatření (viz výše doporučená technická opatření).***

[72] Například v rámci závazných podnikových pravidel, která by v každém případě měla upravovat některá z opatření uvedených níže.

[73] Budou mít soukromou povahu a nebudou považovány za mezinárodní dohody podle mezinárodního práva veřejného. Z toho vyplývá, že za obvyklých okolností nebudou závazné pro orgán veřejné moci třetí země jakožto subjekty, které nejsou stranou smlouvy uzavřené mezi soukromými subjekty ve třetích zemích, jak zdůraznil Soudní dvůr v rozsudku ve věci C-311/18 (Schrems II), bod 125.

[74] Viz rozsudek ve věci C-311/18 (Schrems II), bod 137, ve kterém Soudní dvůr v konečném důsledku uznal, že SSD obsahují *„účinné mechanismy, které v praxi umožní zajistit dodržování úrovně ochrany vyžadované unijním právem a v případě, že by došlo k porušení takových doložek nebo k nemožnosti je dodržet, dočasně nebo trvale zakázat předávání osobních údajů na jejich základě“*, viz také bod 148).

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

[76] Rozsudek SDEU ve věci C-311/18 (Schrems II), bod 132.

98. ***Podmínky účinnosti:***

- Tato doložka by mohla být účinná v těch situacích, kdy vývozce zjistil nutnost technických opatření. Následně musí být zakotvena v právní podobě, aby bylo zajištěno, že se dovozce, bude-li to zapotřebí, rovněž zavazuje zavést nezbytná technická opatření.

Závazky v oblasti transparentnosti:

99. ***Vývozce by mohl doplnit do příloh smlouvy informace, které poskytne dovozce na základě vynaložení veškerého úsilí a jež se týkají přístupu k údajům ze strany orgánů veřejné moci v zemi určení, mimo jiné i v oblasti zpravodajských služeb, pokud je daný právní předpis v souladu s evropskými základními zárukami sboru EDPB. To může vývozci údajů pomoci splnit své závazky zdokumentovat své posouzení úrovně ochrany v dané třetí zemi.***

100. Dovozce by mohl být například povinen:

(1) uvést právní a správní předpisy v zemi určení, které se vztahují na dovozce a jeho (další) zpracovatele a které by umožnily přístup orgánům veřejné moci k osobním údajům, jež se předávají, zejména pak v oblasti zpravodajských služeb, prosazování práva a správního a regulačního dohledu v souvislosti s předávanými údaji;
(2) pokud neexistují právní předpisy upravující přístup orgánů veřejné moci k údajům, poskytnout informace a statistiky na základě zkušenosti daného dovozce či zpráv z různých zdrojů (např. partneři, veřejně dostupné zdroje, vnitrostátní judikatura a rozhodnutí od orgánů dohledu) o přístupu orgánů veřejné moci k osobním údajům v situacích, které jsou podobné dané situaci předávání údajů (tj. v konkrétní regulační oblasti; s ohledem na druh subjektů, k nimž dovozce údajů patří, ...);
(3) uvést, jaká (případná) opatření se přijímají za účelem zabránění přístupu k předávaným údajům;
(4) poskytnout dostatečně podrobné informace o všech žádostech o přístup k osobním údajům ze strany orgánů veřejné moci, které dovozce obdržel za dané časové období[77], zejména v oblastech uvedených v bodě 1 výše, a obsahující informace o obdržených žádostech, požadovaných údajích, dožadujícím orgánu a právním základu pro zpřístupnění a o tom, do jaké míry dovozce zpřístupnil požadované údaje;[78]
(5) upřesnit, zda a v jakém rozsahu brání právní předpisy dovozci, aby poskytl informace uvedené v bodech (1)–(5) výše.

101. Tyto informace by mohly být poskytnuty formou strukturovaných dotazníků, které by dovozce vyplnil a podepsal, a stvrzeny smluvním závazkem dovozce oznámit v rámci stanovené lhůty veškeré případné změny těchto informací, jak je běžná praxe v případě postupů v oblasti náležité pečlivosti.

[77] Délka období by měla záviset na riziku pro práva a svobody subjektů údajů, jejichž údaje jsou předmětem dotčeného předávání – např. dvanáct měsíců před ukončením používání nástroje na vývoz údajů s vývozcem údajů.
[78] Vyhovění této povinnosti samo o sobě neznamená zajištění vhodné úrovně ochrany. Zároveň pokud skutečně dojde k jakémukoliv nevhodnému zpřístupnění, bude zapotřebí provedení dalších opatření.

102. ***Podmínky účinnosti:***

- Dovozce musí být schopen poskytnout vývozci tyto druhy informací podle svého nejlepšího vědomí a po vynaložení veškerého úsilí na jejich získání.[79]
- Tento závazek uložený dovozci je jedním z prostředků, jak zajistit, že dovozce získá a bude si udržovat povědomí o rizicích spojených s předáváním údajů do dané třetí země. Tím umožní vývozci, aby se zdržel uzavření smlouvy, nebo pokud se změní informace po uzavření smlouvy, aby dostál své povinnosti dočasně zastavit předávání a/nebo odstoupit od smlouvy, pokud právní řád dané třetí země, záruky obsažené v nástroji pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů a veškeré další záruky, které mohl přijmout, již nemohou zaručit úroveň ochrany, která je v zásadě rovnocenná úrovni v EU. Tento závazek však nemůže odůvodnit ani zpřístupnění osobních údajů ze strany dovozce, ani vzbudit očekávání, že již nebudou předloženy žádné další žádosti o přístup.

***

103. ***Vývozce by mohl rovněž doplnit doložky, podle kterých by dovozce osvědčil, že 1) nevytváří záměrně „zadní vrátka" ani podobné programování, které by mohlo být použito k přístupu do systému a/nebo k osobním údajům; 2) záměrně nevytvořil ani nezměnil své obchodní procesy způsobem, který usnadňuje přístup k osobních údajům nebo k systémům, a 3) že vnitrostátní právo nebo vládní politika neukládá dovozci povinnost vytvářet nebo spravovat „zadní vrátka" nebo usnadňovat přístup k osobním údajům nebo systémům nebo povinnost dovozce vlastnit a předat šifrovací klíč.[80]***

104. ***Podmínky účinnosti:***

- Existence právních předpisů nebo vládních politik, které brání dovozcům zpřístupňovat tyto informace, může způsobit, že tato doložka nebude účinná. Dovozce tudíž nebude schopen uzavřít smlouvu nebo bude muset vývozci oznámit, že není schopen nadále plnit své smluvní závazky.[81]
- Smlouva musí obsahovat postihy a/nebo možnost, aby vývozce smlouvu v krátké lhůtě vypověděl v případech, kdy ho dovozce neinformoval o existenci „zadních vrátek" nebo podobného programování nebo o zmanipulovaných obchodních postupech nebo jakýchkoliv požadavků na provedení čehokoliv z výše uvedeného nebo pokud okamžitě neinformuje vývozce, jakmile se o jejich existenci dozví.

***

105. ***Vývozce by mohl posílit své pravomoci provádět přezkoumání[82] nebo kontroly v zařízeních dovozce na zpracování údajů na místě a/nebo na dálku s cílem ověřit, zda byly údaje zpřístupněny orgánům veřejné moci a za jakých podmínek (přístup nepřekračující to, co je nezbytné a přiměřené v demokratické společnosti), například stanovením krátké lhůty a mechanismů zajišťujících rychlý zásah kontrolních orgánů a posilujících autonomii vývozce při výběru kontrolních orgánů.***

[79] Viz bod 32.5 výše.
[80] Tato doložka je důležitá pro zaručení odpovídající úrovně ochrany předávaných osobních údajů a obvykle by měla být povinná.
[81] Viz bod 32.5 výše.
[82] Viz například doložku 5 písm. f) mezi správci a zpracovateli uvedenou v rozhodnutí 2010/87/EU, přezkoumání je rovněž možné stanovit prostřednictvím kodexu chování nebo osvědčení.

106. ***Podmínky účinnosti:***

- Rozsah přezkoumání, má-li být účinný, by měl z právního a technického hlediska zahrnovat veškeré zpracování osobních údajů předaných do třetí země ze strany zpracovatelů nebo dílčích zpracovatelů dovozce.
- Záznamy o přístupu nebo podobné záznamové stopy by měly být odolné vůči manipulacím, aby auditoři mohli nalézt důkazy o zpřístupnění. Záznamy o přístupu nebo podobné záznamové stopy by rovněž měly rozlišovat mezi přístupy v rámci řádných obchodních činností a přístupy z důvodu průkazů nebo žádostí o přístup.

***

107. ***Pokud se mělo na základě původního posouzení za to, že právo a praxe v dané třetí zemi dovozce poskytuje úroveň ochrany v zásadě rovnocennou úrovni poskytované v EU, pokud jde o údaje předávané vývozcem, vývozce by stále mohl posílit závazek dovozce údaje okamžitě informovat vývozce údajů o své neschopnosti dostát smluvním závazkům, a tudíž i požadovanému standardu „v zásadě rovnocenné úrovně ochrany údajů“.***[83]

108. Tato neschopnost dostát závazkům může mít za následek změny v právních předpisech a praxi dané třetí země.[84] Doložky mohou stanovit zvláštní a přísné časové lhůty a postup pro rychlé pozastavení předávání údajů a/nebo vypovězení smlouvy a povinnost dovozce vrátit nebo smazat požadované údaje. Díky tomu, že bude mít vývozce přehled o obdržených žádostech, jejich rozsahu a o účinnosti přijatých protiopatření, by měl mít dostatečné informace k výkonu své povinnosti předávání pozastavit nebo ukončit a/nebo odstoupit od smlouvy.

109. ***Podmínky účinnosti:***

- K oznámení musí dojít před poskytnutím přístupu k údajům. V opačné případě v okamžiku, kdy vývozce oznámení obdrží, již mohlo dojít k porušení práv fyzických osob, pokud je žádost založena na právních předpisech dané třetí země, které jdou nad rámec toho, co dovoluje úroveň ochrany údajů poskytovaná podle práva EU. Oznámení však stále může být užitečné pro zabránění budoucích porušení předpisů a k tomu, aby vývozci umožnilo splnit svou povinnost pozastavit předávání osobních údajů do třetí země a/nebo vypovědět smlouvu.
- Dovozce údajů musí sledovat veškeré právní nebo politické změny, které mohou mít za následek to, že nebude schopen dostát svým povinnostem, a okamžitě informovat vývozce údajů o veškerých takovýchto změnách a vývoji, a to, je-li to možné, ještě před jejich zavedením, aby vývozci údajů umožnil údaje získat zpět od dovozce údajů.
- Doložky by měly stanovit rychlý mechanismus, jehož prostřednictvím vývozce údajů oprávní dovozce údajů, aby okamžitě zabezpečil nebo vrátil údaje vývozci údajů, a pokud to není možné, aby je vymazal nebo bezpečně zašifroval bez toho, aby musel nutně čekat na pokyny vývozce, pokud budou splněny zvláštní podmínky, které mají být dohodnuty vývozcem a

[83] Doložka 5 písm. a) a písm. d) bod i) rozhodnutí 2010/87/EU o SSD.

[84] Viz C-311/18 (Schrems II), bod 139, ve které Soudní dvůr uvádí, že *„Tatáž doložka 5 sice v písm. d) bodě i) umožňuje příjemci předávaných osobních údajů v případě, že mu to zakazují právní předpisy, jako například v případě, kdy je tak zakázáno trestním právem, aby byla zajištěna důvěrnost vyšetřování v rámci výkonu práva, neoznámit správci usazenému v Unii právně závazný požadavek na zveřejnění osobních údajů ze strany donucovacího orgánu, tento příjemce je nicméně podle doložky 5 písm. a) přílohy rozhodnutí o SSD povinen správce informovat o tom, že již nemůže zajistit dodržování standardních doložek o ochraně osobních údajů.“.*

dovozcem údajů. Dovozce by měl tento mechanismus provádět od počátku předávání údajů a pravidelně jej ověřovat, aby zajistil, že je možné jej uplatnit v krátké lhůtě.

- Jiné doložky by mohly vývozci umožnit sledovat, zda dovozce plní tyto povinnosti, a to prostřednictvím přezkoumání, kontrol a jiných ověřovacích opatření a vynucovat je pokutami ukládanými dovozci a/nebo možností, že vývozce pozastaví předávání a/nebo okamžitě vypoví smlouvu.

***

110. ***Pokud to umožňuje vnitrostátní právo ve třetí zemi, měla by smlouva posilovat povinnosti dovozce v oblasti transparentnosti tím, že stanoví metodu „Warrant Canary“, podle které se dovozce zavazuje, že bude pravidelně zveřejňovat (nejméně každých 24 hodin) kryptograficky podepsanou zprávu informující vývozce, že k danému datu a času neobdržel žádný příkaz ke zpřístupnění osobních údajů či podobné příkazy. Pokud nebude k dispozici aktuální verze tohoto oznámení, bude to pro vývozce znamenat, že dovozce mohl obdržet takovýto příkaz.***

111. ***Podmínky účinnosti:***

- Právní předpisy třetí země musí umožňovat dovozci údajů, aby vydával tuto formu pasivního oznámení vývozci.
- Vývozce údajů musí automaticky sledovat oznámení zaslaná pomocí této metody.
- Dovozce údajů musí zajistit, že jeho soukromý klíč pro podepisování oznámení podle metody Warrant Canary je uchováván v bezpečí a že podle právních předpisů třetí země nemůže být nucen vydávat falešná oznámení. Proto může být užitečné, pokud je zapotřebí několik podpisů od různých osob a/nebo pokud je toto oznámení vydáváno osobou sídlící mimo jurisdikci dané třetí země.

Povinnosti přijmout zvláštní opatření

112. ***Dovozce údajů se může zavázat, že bude přezkoumávat v souladu s právním řádem země určení zákonnost veškerých příkazů ke zpřístupnění údajů, zejména pak to, zda je dožadující orgán veřejné moci skutečně oprávněn k jejich vydání, a že napadne příkaz, pokud po pečlivém přezkoumání dospěje k závěru, že podle práva země určení existují důvody k tomuto napadení. V případě, že dovozce údajů napadne příkaz, měl by požádat o předběžná opatření s cílem pozastavit účinky příkazu, dokud soud nerozhodne ve věci samé. Dovozce by měl mít povinnost nezpřístupňovat vyžádané osobní údaje, dokud k tomu nebude povinován na základě platných procesních pravidel. Dovozce údajů se rovněž zavazuje, že při odpovědi na příkaz poskytne minimální množství informací, které je přípustné, a to na základě rozumného výkladu příkazu.***

113. ***Podmínky účinnosti:***

- Právní řád třetí země musí zajistit účinné právní cesty, jak napadnout příkazy ke zpřístupňování údajů.
- Tato doložka vždy zajistí velmi omezenou dodatečnou ochranu, protože příkaz ke zpřístupnění údajů může být podle právního řádu třetí země zákonný, ale současně tento právní řád nemusí odpovídat standardům EU. Toto smluvní opatření bude nezbytně muset být doplňkem k jiným dalším opatřením.

- Napadení příkazů musí mít podle práva třetí země odkladný účinek. V opačném případě by orgány veřejné moci měly stále přístup k osobním údajům fyzických osob a veškeré následné kroky ve prospěch dané fyzické osoby by měly omezený účinek v podobě možnosti, aby tato osoba požadovala náhradu škod v důsledku nepříznivých dopadů, které vznikly kvůli zpřístupnění údajů.
- Dovozce bude muset být schopen zdokumentovat a prokázat vývozci opatření, která přijal, v rámci vynakládání veškerého úsilí, aby dostál tomuto závazku.

***

114. ***V téže situaci, která je popsána výše, by se dovozce mohl zavázat, že informuje dožadující orgán veřejné moci o tom, že příkaz není slučitelný se zárukami obsaženými v nástroji pro předávání podle článku 46 obecného nařízení o ochraně osobních údajů[85], a o vzniklém střetu povinností na straně dovozce. Dovozce by pak současně a co nejdříve uvědomil vývozce a/nebo příslušný dozorový úřad z EHP, pokud je to možné podle právního řádu třetí země.***

115. ***Podmínky účinnosti:***

- Tyto informace o ochraně, kterou poskytuje právo EU, a o střetu povinností by měly mít v právním řádu třetí země určitý právní účinek, například soudní nebo správní přezkum příkazu nebo žádosti o přístup, nutnost soudního příkazu a/nebo dočasné pozastavení účinnosti příkazu s cílem doplnit určitou ochranu údajů.
- Právní systém země nesmí bránit dovozci, aby uvědomil vývozce nebo aspoň příslušný dozorový úřad z EHP o obdrženém příkazu nebo žádosti o přístup.
- Dovozce bude muset být schopen zdokumentovat a prokázat vývozci opatření, která přijal, v rámci vynakládání veškerého úsilí, aby dostál tomuto závazku.

Posílení postavení subjektů údajů za účelem výkonu jejich práv

116. ***Smlouva by mohla stanovit, aby přístup k osobním údajům předaným formou prostého textu při běžném výkonu obchodní činnosti (včetně podpůrných případů) byl umožněn pouze s výslovným nebo konkludentním souhlasem vývozce a/nebo subjektu údajů.***

117. ***Podmínky účinnosti:***

- Tato doložka by mohla být účinná v situacích, kdy dovozci obdrželi od orgánů veřejné moci žádosti o dobrovolnou spolupráci, na rozdíl například od přístupu k údajům ze strany orgánů veřejné moci, ke kterému dojde bez vědomí či proti vůli dovozce údajů.
- V některých situacích nebude subjekt údajů schopen ohradit se proti přístupu nebo udělit souhlas, který by splňoval veškeré podmínky stanovené podle práva EU (byl svobodný, konkrétní, informovaný a jednoznačný) (např. v případě zaměstnanců)[86].

[85] Například SSD stanoví, že zpracování údajů, včetně jejich předávání, bylo a bude i nadále prováděno v souladu s *„právem rozhodným pro ochranu údajů“.* Toto právo je definováno jako *„právní předpisy ochraňující základní práva a svobody jednotlivců, a zejména jejich právo na soukromí ve vztahu ke zpracování osobních údajů, které se vztahují na správce údajů v členském státě, ve kterém je usazen vývozce údajů“.* SDEU potvrzuje, že mezi tyto předpisy přitom patří ustanovení obecného nařízení o ochraně osobních údajů ve spojení s Listinou základních práv EU, viz rozsudek SDEU ve věci C-311/18 (Schrems II), bod 138.
[86] Čl. 4 bod 11 obecného nařízení o ochraně osobních údajů.

- Vnitrostátní právní předpisy nebo politiky, které nutí dovozce, aby nezveřejňoval, že obdržel příkaz o přístupu k údajů, mohou mít za následek, že tato doložka bude neúčinná, ledaže ji doplní technické metody, které budou vyžadovat zásah subjektu údajů nebo vývozce, který umožní, aby byly údaje přístupné ve formě prostého textu. Tato technická opatření s cílem omezit přístup si je možné představit zvláště tehdy, pokud se přístup uděluje pouze v některých podpůrných případech či v případech poskytování služeb, ale údaje jako takové jsou uloženy v EHP.

***

118. ***Smlouva by mohla dovozci a/nebo vývozci uložit povinnost, okamžitě žádost nebo příkaz obdržený od orgánů veřejné moci třetí země oznámit subjektu údajů nebo mu oznámit, že dovozce není schopen dostát smluvním závazkům, s cílem umožnit subjektu údajů požádat o informace a o účinnou ochranu (např. podáním stížnosti u svého příslušného dozorového úřadu a/nebo soudního orgánu a prokázáním své aktivní legitimace u soudů třetí země).***

119. ***Podmínky účinnosti:***

- Toto oznámení by mohlo upozornit subjekt údajů na možné přístupy k jeho údajům ze strany orgánů veřejné moci třetí země. Tím by mohlo umožnit subjektu údajů žádat o další informace od vývozců nebo podat stížnost u svého příslušného dozorového úřadu. Tato doložka by rovněž mohla být řešením pro některé obtíže, jimž může fyzická osoba čelit při prokazování své aktivní legitimace *(locus standi)* u soudů třetí země, pokud jde o možnost napadnout přístup orgánů veřejné moci k údajům této osoby.
- Vnitrostátní právní předpisy a politiky mohou zabránit tomu, aby dovozce informoval subjekt údajů. Vývozce a dovozce by se přesto mohli zavázat, že informují subjekt údajů, jakmile budou omezení týkající se zpřístupnění údajů zrušena, a vynaložit veškeré úsilí o získání zrušení zákazu informovat subjekt údajů. Vývozce nebo příslušný dozorový úřad by přinejmenším mohli informovat subjekt údajů o pozastavení nebo zákazu předávání jeho osobních údajů kvůli neschopnosti dovozce údajů jednat v souladu s jeho smluvními závazky v důsledku obdržení žádosti o přístup.

***

120. ***Smlouva by mohla vývozce a dovozce zavazovat, aby byli nápomocni subjektu údajů při vykonávání jeho práv v jurisdikci třetí země prostřednictvím ad hoc mechanismů právní ochrany a právního poradenství.***

121. ***Podmínky účinnosti:***

- Vnitrostátní právní předpisy a politiky mohou stanovit podmínky, které mohou znehodnotit účinnost stanovených ad hoc mechanismů právní ochrany.
- Právní poradenství by mohlo být pro subjekt údajů užitečné zejména vzhledem k tomu, jak složité a nákladné může být pro subjekt údajů porozumět právnímu systému třetí země a provádět právní kroky ze zahraničí, případně též v cizím jazyce. Tato doložka však bude vždy nabízet jen omezenou dodatečnou ochranu, protože poskytování pomoci a právního poradenství subjektu údajů nemůže samo o sobě být opravným prostředkem pro selhání právního řádu třetí země, pokud jde o zajištění úrovně ochrany v zásadě rovnocenné úrovni

zaručené v EU. Toto smluvní opatření bude nezbytně muset být doplňkem k jiným dalším opatřením.

Toto další opatření by bylo účinné pouze tehdy, pokud by právo třetí země stanovilo opravný prostředek u vnitrostátních soudů a pokud by existoval ad hoc mechanismus právní ochrany. V každém případě by se však nejednalo o účinné další opatření proti opatřením za účelem sledování, pokud neexistuje žádný mechanismus právní ochrany.

Organizační opatření

122. K dalším organizačním opatřením mohou patřit interní politiky, organizační metody nebo normy, které by mohli správci a zpracovatelé uplatňovat u sebe a ukládat jejich zavedení dovozcům údajů ve třetích zemích. Mohou přispět k zajištění soudržnosti v ochraně osobních údajů během celého cyklu zpracování. Organizační opatření mohou rovněž zvýšit povědomí vývozců o riziku a pokusech získat přístup k údajům ve třetích zemích a jejich schopnost na tyto situace reagovat. Výběr a provedení jednoho nebo několika z těchto opatření nezajistí nutně a systematicky, že vaše předání bude splňovat standard v zásadě rovnocenné ochrany, který ukládá právo EU. V závislosti na konkrétních okolnostech předání a provedeného posouzení právních předpisů třetí země jsou organizační opatření nezbytná jako doplnění smluvních a/nebo technických opatření s cílem zajistit úroveň ochrany osobních údajů, která je v zásadě rovnocenná úrovni zaručené v EU.

123. Posouzení nejvhodnějších opatření musí být provedeno jednotlivě případ od případu a je třeba mít na paměti, že se správci a zpracovatelé musejí řídit zásadou odpovědnosti. Níže sbor EDPB uvádí některé příklady organizačních opatření, která vývozci mohou provést, ačkoliv jde pouze o orientační výčet a vhodná mohou být i jiná opatření:

Interní politiky upravující předávání, zejména v rámci skupin podniků

124. ***Přijetí odpovídajících interních politik s jasným rozdělením povinností pro předávání údajů, kanály pro oznamování a stálými operačními postupy pro případy utajených či úředních žádostí o přístup k údajům předložených orgány veřejné moci. Zejména v případě předání v rámci skupin podniků mohou tyto politiky zahrnovat kromě jiného jmenování zvláštního týmu, který by měl sídlit v rámci EHP a který budou tvořit odborníci na IT, ochranu údajů a právní předpisy na ochranu soukromí, a to za účelem vyřizování žádostí, které se týkají osobních údajů předaných z EU; oznámení vyššímu právnímu vedení a vedení společnosti a vývozci údajů po přijetí těchto žádostí; procesních kroků k napadení nepřiměřených nebo nezákonných žádostí a poskytnutí transparentních informací subjektům údajů.***

125. Vypracování zvláštních postupů v oblasti odborné přípravy pro pracovníky pověřené vyřizováním žádostí o přístup k osobním údajům ze strany orgánů veřejné moci, které by měly být pravidelně aktualizovány, aby odrážely aktuální vývoj v oblasti právních předpisů a judikatury ve třetí zemi nebo v EHP. Postupy v oblasti odborné přípravy by měly zahrnovat požadavky práva EU, pokud jde o přístup k osobním údajům ze strany orgánů veřejné moci, zejména ty, které vyplývají z čl. 52 odst. 1 Listiny základních práv. Povědomí pracovníků je třeba zvýšit zejména prostřednictvím posouzení praktických příkladů žádostí orgánů veřejné moci o přístup k údajům a uplatněním standardu vyplývajícího z čl. 52 odst. 1 Listiny základních práv na tyto praktické příklady. Tato odborná příprava by měla zohlednit zvláštní situaci dovozce údajů, např. právní a správní předpisy ve třetí zemi, jimiž se dovozce údajů řídí, a měla by být, je-li to možné, vypracována ve spolupráci s dovozcem údajů.

126. ***Podmínky účinnosti:***

- Tyto politiky je možné zavést pouze v případech, kdy žádost orgánů veřejné moci ve třetí zemi je slučitelná v právem EU.[87] Pokud žádost slučitelná není, nebudou tyto politiky postačovat k zajištění rovnocenné úrovně ochrany osobních údajů a – jak bylo řečeno výše – předání je třeba zastavit nebo je třeba zavést vhodná další opatření s cílem zabránit přístupu.

Opatření k zajištění transparentnosti a odpovědnosti

127. ***Dokumentovat a zaznamenávat žádosti o přístup obdržené od orgánů veřejné moci a poskytnuté odpovědi spolu s právním odůvodněním a zúčastněnými subjekty (např. zda byl uvědomen vývozce a jeho odpověď, posouzení týmu pověřeného vyřizováním takovýchto žádostí atd.). Tyto záznamy by měly být k dispozici vývozci údajů, který by je pak měl případně poskytnout dotčeným subjektům údajů.***

128. ***Podmínky účinnosti:***

- Vnitrostátní právní předpisy ve třetí zemi mohou zabránit zpřístupnění žádostí nebo významných informací o nich, a tudíž tento postup učinit neúčinným. Dovozce údajů by měl informovat vývozce o tom, že není schopen tyto dokumenty a záznamy poskytnout, čímž nabídne vývozci možnost pozastavit předávání, pokud by tato neschopnost vedla ke snížení úrovně ochrany.

***

129. ***Pravidelné zveřejňování zpráv nebo shrnutí k zajištění transparentnosti týkajících se žádostí vlády o přístup k údajům a druh poskytnuté odpovědi, pokud místní právní řád toto zveřejnění umožňuje.***

130. ***Podmínky účinnosti:***

- Poskytované informace by měly být relevantní, jednoznačné a co nejpodrobnější. Vnitrostátní právní předpisy ve třetí zemi mohou zabránit zpřístupnění podrobných informací. V těchto případech by měl dovozce údajů vynaložit veškeré úsilí ke zveřejnění statistických informací nebo podobného druhu agregovaných informací.

Organizační metody a opatření na minimalizaci údajů

131. ***V souvislosti s předáváním údajů mohou být také užitečné již existující organizační povinnosti v rámci zásady odpovědnosti, např. přijetí přísných a granulárních politik a osvědčených postupů týkajících se přístupu k údajům a zachovávání důvěrnosti, a to na základě přísného dodržování zásady, že k údajům má přístup jen osoba, která jej nutně potřebuje, tento přístup je sledován v rámci pravidelných přezkoumání a vynucován disciplinárními opatřeními. V této souvislosti je třeba zvážit minimalizaci údajů s cílem omezit expozici osobních údajů vůči neoprávněnému přístupu. Například v některých případech nemusí být nutné předávat některé údaje (jako v případě vzdáleného přístupu k údajům v EHP, např. v podpůrných případech, kdy se poskytne omezený přístup namísto plného***

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

přístupu; nebo když poskytování služby vyžaduje předání pouze omezeného souboru údajů, a nikoliv celé databáze).

132. ***Podmínky účinnosti:***

- Za účelem sledování a prosazování souladu s opatřeními na minimalizaci údajů i v souvislosti s předáváním by měly být zavedeny pravidelná přezkoumání a silná disciplinární opatření.
- Vývozce údajů před předáním provede posouzení osobních údajů, které má v držení, aby určil ty soubory údajů, které nejsou nezbytné pro účely předání, a tudíž nebudou sdíleny s dovozcem údajů.
- Opatření za účelem minimalizace údajů by měla být doprovázena technickými opatřeními s cílem zajistit, aby nedošlo k neoprávněnému přístupu k údajům. Například zavedením zabezpečených mechanismů výpočtů prováděných více stranami a šířením zašifrovaných souborů údajů mezi jednotlivými důvěryhodnými subjekty je možné již od návrhu zabránit tomu, aby každý jednostranný přístup vedl ke zpřístupnění identifikovatelných údajů.

***

133. ***Vypracování osvědčených postupů, jak vhodně a včas zapojit pověřence pro ochranu osobních údajů (pokud existuje) a poskytnout mu přístup k informacím a také jak zapojit útvar interního auditu ve věcech týkajících se mezinárodních předávání osobních údajů.***

134. ***Podmínky účinnosti:***

- Pověřenec pro ochranu osobních údajů, pokud existuje, a právní tým a tým interního auditu musí před předáním disponovat všemi relevantními informacemi a musí být konzultováni ohledně nezbytnosti předání a případných dodatečných záruk.
- K relevantním informacím by mělo patřit například posouzení nezbytnosti předání zvláštních osobních údajů, přehled o příslušných právních předpisech třetí země a zárukách, které se dovozce zavázal provést.

Přijetí standardů a osvědčených postupů

135. ***Přijetí přísných politik v oblasti zabezpečení a ochrany údajů založených na osvědčeních EU nebo na kodexech chování nebo na mezinárodních normách (např. normy ISO) a na osvědčených postupech (např. od agentury ENISA) s náležitým zohledněním stavu techniky, a to v souladu s rizikem pro kategorie zpracovávaných údajů a pravděpodobnost pokusů o přístup k těmto údajům ze strany orgánů veřejné moci.***

Jiné

136. ***Přijetí a pravidelný přezkum interních politik za účelem posouzení vhodnosti prováděných vzájemně se doplňujících opatření a určení a provádění dalších nebo alternativních řešení, je-li to nezbytné, s cílem zajistit, že je zachována úroveň ochrany předávaných osobních údajů, která je rovnocenná úrovni zaručené v EU.***

***

137. ***Závazky dovozce údajů, že se nebude podílet na žádném dalším předávání osobních údajů v rámci téže nebo jiných třetích zemí nebo že pozastaví probíhající předávání, pokud nebude moci být zaručena úroveň ochrany osobních údajů, která je v zásadě rovnocenná úrovni zajišťované v rámci EU.[88]***

PŘÍLOHA 3: PŘÍPADNÉ ZDROJE PRO POSUZOVÁNÍ TŘETÍ ZEMĚ

138. Váš dovozce údajů by měl být schopen vám poskytnout relevantní zdroje a informace týkající se dané třetí země, ve které je usazen, a právních předpisů, které se na něho vztahují. Můžete také využít několik zdrojů informací, například ty, které jsou uvedeny níže v orientačním výčtu:

- judikatura Soudního dvora Evropské unie (SDEU) nebo Evropského soudu pro lidská práva (ESLP)[89], jak je uvedeno v doporučeních o evropských základních zárukách,[90]
- rozhodnutí o odpovídající ochraně v zemi určení, pokud předání vychází z jiného právního základu,[91]
- usnesení a zprávy mezivládních organizací, jako je Rada Evropy[92], jiných regionálních subjektů[93] a orgánů a agentur OSN (např. Rady pro lidská práva OSN[94], Výboru pro lidská práva[95]),
- vnitrostátní judikatura nebo rozhodnutí vydaná nezávislými soudními či správními orgány třetích zemí příslušnými k rozhodování ve věcech ochrany údajů,
- zprávy akademických institucí a organizací občanské společnosti (např. nevládních organizací a oborových sdružení).

[88] C-311/18 (Schrems II), body 135 a 137.
[89] Viz informativní přehled o judikatuře ESLP týkající se hromadného sledování: 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; viz rozhodnutí o odpovídající ochraně na adrese 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] Viz například zprávy o jednotlivých zemích Meziamerické komise pro lidská práva, https://www.oas.org/en/iachr/reports/country.asp.
[94] Viz https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx.
[95] Viz: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5.