EVROPSKÁ KOMISE

Brusel, XXX [...](2022)
XXX návrh

PROVÁDĚCÍ ROZHODNUTÍ KOMISE

společnosti XXX

podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o odpovídající úrovni ochrany osobních údajů podle rámce EU a USA pro ochranu osobních údajů.

(Text s významem pro EHP)

PROVÁDĚCÍ ROZHODNUTÍ KOMISE

společnosti XXX

podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o odpovídající úrovni ochrany osobních údajů podle rámce EU a USA pro ochranu osobních údajů.

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na 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)[1] , a zejména na čl. 45 odst. 3 uvedeného nařízení,

vzhledem k tomu, že:

1. ÚVOD

(1) Nařízení (EU) 2016/679 stanoví pravidla pro předávání osobních údajů od správců nebo zpracovatelů v Unii do třetích zemí a mezinárodním organizacím v rozsahu, v jakém tato předávání spadají do oblasti jeho působnosti. Pravidla pro mezinárodní předávání údajů jsou stanovena v kapitole V uvedeného nařízení. Přestože je tok osobních údajů do zemí mimo Evropskou unii a ze zemí mimo ni nezbytný pro rozšíření přeshraničního obchodu a mezinárodní spolupráce, nesmí být úroveň ochrany poskytovaná osobním údajům v Unii oslabena předáváním do třetích zemí[2] .

(2) Podle čl. 45 odst. 3 nařízení (EU) 2016/679 může Komise prostřednictvím prováděcího aktu rozhodnout, že třetí země, území nebo jedno či více určených odvětví v rámci třetí země zajišťují odpovídající úroveň ochrany. Za této podmínky může dojít k předání osobních údajů do třetí země, aniž by bylo nutné získat další povolení, jak je stanoveno v čl. 45 odst. 1 a 103. bodě odůvodnění nařízení (EU) 2016/679.

(3) Jak je uvedeno v čl. 45 odst. 2 nařízení (EU) 2016/679, přijetí rozhodnutí o odpovídající ochraně musí být založeno na komplexní analýze právního řádu třetí země, která zahrnuje jak pravidla platná pro dovozce údajů, tak omezení a záruky, pokud jde o přístup orgánů veřejné moci k osobním údajům. Při posuzování musí Komise určit, zda daná třetí země zaručuje úroveň ochrany "v zásadě rovnocennou" úrovni ochrany zajištěné v Unii (104. bod odůvodnění nařízení (EU) 2016/679). Zda tomu tak je, je třeba posoudit na základě

[1] L 119, 4.5.2016, s. 1 .

[2] Viz 101. bod odůvodnění nařízení (EU) 2016/679.

právních předpisů Unie, zejména nařízení (EU) 2016/679, jakož i judikatury Soudního dvora Evropské unie (dále jen "Soudní dvůr")[3] .

(4) Jak upřesnil Soudní dvůr v rozsudku ze dne 6. října 2015 ve věci C- 362/14, *Maximillian Schrems* v. *komisař pro ochranu údajů*[4] *(Schrems),* nevyžaduje to zjištění stejné úrovně ochrany. Zejména prostředky, které daná třetí země využívá k ochraně osobních údajů, se mohou lišit od prostředků používaných v Unii, pokud se v praxi ukáže, že jsou účinné pro zajištění odpovídající úrovně ochrany[5] . Norma přiměřenosti proto nevyžaduje přesnou replikaci pravidel Unie. Spíše se testuje, zda zahraniční systém jako celek poskytuje prostřednictvím obsahu práv na ochranu soukromí a jejich účinného provádění, dohledu a prosazování požadovanou úroveň ochrany[6] . Podle uvedeného rozsudku by Komise při uplatňování tohoto standardu měla dále zejména posoudit, zda právní rámec dotčené třetí země stanoví pravidla, jejichž cílem je omezit zásahy do základních práv osob, jejichž údaje jsou předávány z Unie, které by státní subjekty této země byly oprávněny provádět, pokud sledují legitimní cíle, jako je národní bezpečnost, a zda poskytuje účinnou právní ochranu proti zásahům tohoto druhu[7] . V tomto ohledu poskytuje vodítko také "Referát o přiměřenosti" Evropského sboru pro ochranu osobních údajů, který se snaží tento standard dále objasnit[8] .

(5) Platný standard s ohledem na takový zásah do základních práv na soukromí a ochranu údajů dále objasnil Soudní dvůr v rozsudku ze dne 16. července 2020 ve věci C-311/18, *komisař pro ochranu údajů v. Facebook Ireland Limited a Maximillian Schrems (Schrems II),* kterým bylo zrušeno prováděcí rozhodnutí Komise (EU) 2016/1250[9] o předchozím transatlantickém rámci pro tok údajů, štítu na ochranu soukromí mezi EU a USA (Privacy Shield). Soudní dvůr měl za to, že omezení ochrany osobních údajů vyplývající z vnitrostátního práva USA týkající se přístupu k údajům předávaným z Unie do Spojených států a jejich využívání orgány veřejné moci USA pro účely národní bezpečnosti nebyla vymezena způsobem, který by splňoval požadavky v zásadě rovnocenné požadavkům práva Unie, pokud jde o nezbytnost a přiměřenost takových zásahů do práva na ochranu údajů[10] . Soudní dvůr se rovněž domníval, že neexistuje žádný důvod k podání žaloby u orgánu, který by osobám, jejichž údaje byly předány Spojeným státům, poskytoval záruky v zásadě rovnocenné těm, které vyžaduje článek 47 Listiny o právu na účinnou právní ochranu[11] .

(6) V návaznosti na rozsudek *Schrems II zahájila* Komise jednání s vládou Spojených států s cílem přijmout nové rozhodnutí o přiměřenosti, které by splňovalo požadavky na

[3] Naposledy viz věc C-311/18, Facebook Ireland a Schrems (*Schrems II*) ECLI:EU:C:2020:559.

[4] Případ C-362/14, Maximilian Schrems v. Data . Komisař (*Schrems)*, ECLI:EU:C:2015:650, bod 73.

[5] *Schrems*, bod 74.

[6] Viz sdělení Komise Evropskému parlamentu a Radě, Výměna a ochrana osobních údajů v globalizovaném světě, COM(2017) 7 ze dne 10.1.2017, oddíl 3.1, s. 6-7.

[7] *Schrems*, bod 88-89.

[8] Evropský sbor pro ochranu osobních údajů, Adequacy Referential, WP 254 rev. 01.k dispozici na tomto odkazu: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

[9] Prováděcí rozhodnutí Komise (EU) 2016/1250 ze dne 12. července 2016 podle směrnice Evropského parlamentu a Rady 95/46/ES o přiměřenosti ochrany poskytované EU. Štít USA na ochranu soukromí (Úř. věst. L 207, 1.8.2016, s. 1).

[10] *Schrems II*, bod 185.

[11] *Schrems II*, bod 197.

požadavky čl. 45 odst. 2 nařízení (EU) 2016/679, jak je vykládá Soudní dvůr. V důsledku těchto jednání přijaly Spojené státy dne 7. října 2022 výkonný příkaz 14086 "Posílení záruk pro zpravodajské činnosti USA v oblasti signálů" (EO 14086), který je doplněn nařízením o soudu pro přezkum ochrany údajů vydaným generálním prokurátorem USA (AG Regulation)[12] . Kromě toho byl aktualizován rámec, který se vztahuje na obchodní subjekty zpracovávající údaje předávané z Unie podle tohoto rozhodnutí - "Rámec EU a USA pro ochranu soukromí údajů" (EU-U.S. DPF nebo DPF).

(7) Komise pečlivě analyzovala právní předpisy a praxi USA, včetně nařízení 14086 a nařízení AG. Na základě zjištění uvedených v 9.-192. bodě odůvodnění dospěla Komise k závěru, že Spojené státy zajišťují odpovídající úroveň ochrany osobních údajů předávaných v rámci DPF mezi EU a USA od správce nebo zpracovatele v Unii[13] certifikovaným organizacím ve Spojených státech.

(8) Toto rozhodnutí má za následek, že předávání osobních údajů od správců a zpracovatelů v Unii[14] certifikovaným organizacím ve Spojených státech může probíhat bez nutnosti získat jakékoli další povolení. Není jím dotčeno přímé uplatňování nařízení (EU) 2016/679 na tyto organizace, pokud jsou splněny podmínky týkající se územní působnosti uvedeného nařízení stanovené v jeho článku 3.

2. RÁMEC EU A USA PRO OCHRANU OSOBNÍCH ÚDAJŮ

2.1 Osobní a věcná působnost

2.1.1 Certifikované organizace

(9) Rámec EU a USA pro ochranu osobních údajů je založen na systému certifikace, kterým se organizace USA zavazují k dodržování souboru zásad ochrany osobních údajů - "Zásad rámce EU a USA pro ochranu osobních údajů", včetně doplňkových zásad (společně dále jen "zásady") - vydaných Ministerstvem obchodu USA (DoC) a obsažených v příloze I tohoto rozhodnutí[15] . Aby organizace mohla získat certifikaci podle Zásad ochrany osobních údajů EU a USA, musí podléhat vyšetřovacím a donucovacím pravomocem Federální obchodní komise (FTC) nebo Ministerstva dopravy USA (DoT)[16] . Zásady se uplatňují okamžitě po certifikaci. Jak je podrobněji vysvětleno ve 47.-51. bodě odůvodnění, organizace DPF EU a USA musí každoročně znovu osvědčit, že dodržují zásady[17] .

2.1.2 Definice osobních údajů a pojmy správce a "zástupce

[12] 28 CFR část 302.

[13] Toto rozhodnutí má význam pro EHP. Dohoda o Evropském hospodářském prostoru (Dohoda o EHP) stanoví rozšíření vnitřního trhu Evropské unie na tři státy EHP: Island, Lichtenštejnsko a Norsko. Rozhodnutí Smíšeného výboru, kterým se nařízení (EU) 2016/679 začleňuje do přílohy XI Dohody o EHP, bylo přijato Smíšeným výborem EHP dne 6. července 2018 a vstoupilo v platnost dne 20. července 2018. Na nařízení se tedy vztahuje uvedená dohoda. Pro účely tohoto rozhodnutí by se tedy odkazy na EU a členské státy EU měly chápat tak, že se vztahují i na státy EHP.

[14] Tímto rozhodnutím nejsou dotčeny požadavky nařízení (EU) 2016/679, které se vztahují na subjekty (správce a zpracovatele) v Unii předávající údaje, například na omezení účelu, minimalizaci údajů, transparentnost a bezpečnost údajů (viz také článek 44 nařízení (EU) 2016/679).

[15] V tomto ohledu viz rozsudek *Schrems*, bod 81, v němž Soudní dvůr potvrdil, že systém autocertifikace může zajistit přiměřenou úroveň ochrany.

[16] Příloha I, oddíl I.2.

[17] Příloha I, oddíl III.6.

(10) Ochrana poskytovaná v rámci DPF mezi EU a USA se vztahuje na všechny osobní údaje předávané z Unie organizacím v USA, které u DoC potvrdily dodržování zásad, s výjimkou údajů, které jsou shromažďovány za účelem zveřejnění, vysílání nebo jiných forem veřejného sdělování novinářských materiálů a informací v dříve zveřejněných materiálech šířených z mediálních archivů[18] . Takové informace proto nelze předávat na základě EU-Údajů.
DPF V USA.

(11) Zásady definují osobní údaje/osobní informace stejně jako nařízení (EU) 2016/679, tj. jako "údaje o identifikované nebo identifikovatelné fyzické osobě, které spadají do působnosti GDPR a které organizace ve Spojených státech obdržela od EU a které jsou zaznamenány v jakékoli formě"[19] . V souladu s tím se vztahují také na pseudonymizované (nebo "kódované") údaje z výzkumu (včetně případů, kdy klíč není sdílen s přijímající organizací v USA)[20] . Podobně je pojem zpracování definován jako "jakákoli operace nebo soubor operací, které jsou prováděny s osobními údaji, ať již automatizovaně, či nikoli, jako je shromažďování, zaznamenávání, uspořádávání, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, nahlížení, používání, zveřejňování nebo šíření a výmaz nebo zničení"[21] .

(12) DPF EU - USA se vztahuje na organizace v USA, které se kvalifikují jako správci (tj. jako osoba nebo organizace, která sama nebo společně s jinými určuje účely a prostředky zpracování osobních údajů)[22] nebo zpracovatelé (tj. zástupci jednající jménem správce). Zpracovatelé v USA musí být smluvně zavázáni jednat pouze na základě pokynů správce v EU a pomáhat mu při reakci na fyzické osoby uplatňující svá práva podle zásad[23] . Kromě toho musí zpracovatel v případě dílčího zpracování uzavřít s dílčím zpracovatelem smlouvu zaručující stejnou úroveň ochrany, jakou poskytují Zásady, a přijmout opatření k zajištění jejího řádného provádění[24] .

2.2 Zásady rámce ochrany osobních údajů mezi EU a USA

2.2.1 Omezení účelu a volba

(13) Osobní údaje by měly být zpracovávány zákonně a spravedlivě. Měly by být shromažďovány za určitým účelem a následně používány pouze v rozsahu, který není neslučitelný s účelem zpracování.

(14) V rámci DPF mezi EU a USA je to zajištěno prostřednictvím různých zásad. Za prvé, podle *zásady integrity údajů a omezení účelu,* podobně jako podle čl. 5 odst. 1 písm. b) nařízení (EU) 2016/679*,* nesmí organizace zpracovávat osobní údaje způsobem, který je neslučitelný s účelem, pro který byly původně shromážděny nebo následně schváleny subjektem údajů[25] .

---

18 Příloha I, oddíl III.2.
19 Příloha I, oddíl I.8.a.
20 Příloha I oddíl III.14.g.
21 Příloha I oddíl I.8.b.
22 Příloha I oddíl I.8.c.
23 Příloha I oddíl III.10.a.
24 Příloha I oddíl II.3.b.
25 Příloha I, oddíl II.5.a. Mezi slučitelné účely může patřit audit, prevence podvodů nebo jiné účely, které odpovídají očekávání rozumné osoby vzhledem ke kontextu sběru (viz příloha I, poznámka pod čarou 6).

(15) Za druhé, pokud chce organizace použít osobní údaje pro nový (změněný) účel, který je podstatně odlišný, ale stále slučitelný s původním účelem, nebo je sdělit třetí straně, musí subjektům údajů poskytnout možnost vznést námitku (opt-out) v souladu se *zásadou volby*[26] , a to prostřednictvím jasného, zřetelného a snadno dostupného mechanismu. Důležité je, že tato zásada nenahrazuje výslovný zákaz neslučitelného zpracování[27] .

2.2.2 Zpracování zvláštních kategorií osobních údajů

(16) V případě zpracování "zvláštních kategorií" údajů by měla existovat zvláštní ochranná opatření.

(17) V souladu se *zásadou volby* se zvláštní ochranná opatření vztahují na zpracování "citlivých informací", tj. osobních údajů uvádějících zdravotní stav, rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení, členství v odborech, informace o sexuálním životě jednotlivce nebo jakékoli jiné informace získané od třetí strany, které tato strana identifikuje a považuje za citlivé[28] . To znamená, že s jakýmikoliv údaji, které jsou podle práva Unie na ochranu údajů považovány za citlivé (včetně údajů o sexuální orientaci, genetických údajů a biometrických údajů), budou certifikované organizace nakládat jako s citlivými podle DPF EU a USA.

(18) Obecně platí, že organizace musí od jednotlivců získat výslovný souhlas (tj. opt-in) s použitím citlivých informací pro jiné účely, než pro které byly původně shromážděny nebo následně schváleny jednotlivcem (prostřednictvím opt-in), nebo s jejich zpřístupněním třetím stranám[29] .

---

26 Příloha I oddíl II.2.a. To neplatí, pokud organizace poskytuje osobní údaje zpracovateli, který jedná jejím jménem a podle jejích pokynů (příloha I oddíl II.2.b). V tomto případě však organizace musí mít uzavřenou smlouvu a zajistit soulad se zásadou *odpovědnosti za další předávání,* jak je podrobněji popsáno v 43. bodě odůvodnění. Kromě toho může být *zásada volby* (stejně jako *zásada oznamování)* omezena, pokud jsou osobní údaje zpracovávány v rámci hloubkové kontroly (jako součást potenciální fúze nebo převzetí) nebo auditů, a to v rozsahu a po dobu nezbytnou ke splnění zákonných požadavků nebo požadavků veřejného zájmu, nebo v rozsahu a po dobu, kdy by uplatnění těchto zásad bylo na újmu oprávněným zájmům organizace v konkrétním kontextu hloubkové kontroly nebo auditů (příloha I, oddíl III.4). Doplňková zásada 15 (příloha I, oddíl III.15.a a b) rovněž stanoví výjimku ze zásady volby (jakož i ze zásad oznamování a odpovědnosti za další předávání) pro osobní údaje z veřejně dostupných zdrojů (pokud vývozce údajů z EU neuvede, že informace podléhají omezením, která vyžadují uplatnění těchto zásad) nebo osobní údaje shromážděné z evidencí přístupných k nahlížení veřejnosti obecně (pokud nejsou kombinovány s informacemi z neveřejných evidencí a jsou dodrženy veškeré podmínky pro nahlížení). Podobně doplňková zásada 14 (příloha I, oddíl III.14.f) stanoví výjimku ze zásady *volby* (jakož i ze zásad *oznamování* a *odpovědnosti za další předávání) pro* zpracování osobních údajů farmaceutickou společností nebo společností vyrábějící zdravotnické prostředky pro činnosti sledování bezpečnosti a účinnosti výrobků, pokud dodržování těchto zásad brání dodržování regulačních požadavků.

27 To platí pro všechna předávání údajů v rámci DPF mezi EU a USA, včetně případů, kdy se jedná o údaje shromážděné v souvislosti s pracovním poměrem. I když tedy organizace s certifikací USA může v zásadě používat údaje o lidských zdrojích pro jiné účely, které nesouvisejí s pracovním poměrem (např. pro určitá marketingová sdělení), musí dodržovat zákaz neslučitelného zpracování a navíc tak může činit pouze v souladu se zásadami *oznamování* a *volby.* Zákaz, aby americká organizace podnikala jakékoli sankční kroky vůči zaměstnanci za uplatnění takové volby, včetně jakéhokoli omezení pracovních příležitostí, zajistí, že navzdory vztahu podřízenosti a přirozené závislosti nebude na zaměstnance vyvíjen nátlak, a bude tak moci uplatnit skutečně svobodnou volbu. Viz příloha I, oddíl III.9.b.(i).

28 Příloha I oddíl II bod 2.c.

29 Příloha I oddíl II.2.c.

(19) Takový souhlas nemusí být získán za omezených okolností podobných srovnatelným výjimkám stanoveným v právu Unie v oblasti ochrany údajů, např. pokud je zpracování citlivých údajů v životně důležitém zájmu osoby; je nezbytné pro určení právních nároků; nebo je nezbytné pro poskytnutí lékařské péče nebo diagnózy[30] .

2.2.3 Přesnost, minimalizace a zabezpečení dat

(20) Údaje by měly být přesné a v případě potřeby aktualizované. Měly by být rovněž přiměřené, relevantní a nepřiměřené vzhledem k účelům, pro které jsou zpracovávány, a v zásadě by neměly být uchovávány déle, než je nezbytné pro účely, pro které jsou osobní údaje zpracovávány.

(21) Podle *zásady integrity údajů a omezení účelu*[31] musí být osobní údaje omezeny na to, co je relevantní pro účel zpracování. Kromě toho musí organizace v rozsahu nezbytném pro účely zpracování přijmout přiměřené kroky k zajištění toho, aby osobní údaje byly spolehlivé pro zamýšlené použití, přesné, úplné a aktuální.

(22) Osobní informace mohou být navíc uchovávány ve formě, která identifikuje nebo činí jednotlivce identifikovatelným (a tedy ve formě osobních údajů)[32] pouze po dobu, po kterou slouží účelu (účelům), pro který byly původně shromážděny nebo následně schváleny jednotlivcem v souladu se *zásadou volby*. Tato povinnost nebrání organizacím pokračovat ve zpracovávání osobních údajů po delší dobu, ale pouze po dobu a v rozsahu, v jakém takové zpracování přiměřeně slouží jednomu z následujících konkrétních účelů podobných srovnatelným výjimkám stanoveným v právu Unie v oblasti ochrany údajů: archivace ve veřejném zájmu, žurnalistika, literatura a umění, vědecký a historický výzkum a statistická analýza[33] . Pokud jsou osobní údaje uchovávány pro jeden z těchto účelů, podléhá jejich zpracování zárukám stanoveným v Zásadách[34] .

(23) Osobní údaje by rovněž měly být zpracovávány způsobem, který zajistí jejich bezpečnost, včetně ochrany před neoprávněným nebo nezákonným zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Za tímto účelem by správci a zpracovatelé měli přijmout vhodná technická nebo organizační opatření na ochranu osobních údajů před možnými hrozbami. Tato opatření by měla být posuzována s ohledem na stav techniky, související náklady a povahu, rozsah, kontext a účely zpracování, jakož i rizika pro práva fyzických osob.

(24) V rámci DPF mezi EU a USA je to zajištěno *zásadou bezpečnosti,* která podobně jako článek 32 nařízení (EU) 2016/679 vyžaduje přijetí přiměřených a vhodných bezpečnostních opatření s ohledem na rizika spojená se zpracováním a povahu údajů[35] .

---

30 Příloha I, oddíl III.1.

31 Příloha I, oddíl II.5.

32 Viz příloha I, poznámka pod čarou č. 7, která objasňuje, že fyzická osoba je považována za "identifikovatelnou", pokud by organizace nebo třetí strana mohla tuto fyzickou osobu přiměřeně identifikovat s ohledem na prostředky identifikace, které budou pravděpodobně použity (mimo jiné s ohledem na náklady a čas potřebný k identifikaci a na dostupnou technologii v době zpracování).

33 Příloha I oddíl II.5.b.

34 *Tamtéž*.

35 Příloha I, oddíl II.4.a. Kromě toho, pokud jde o údaje o lidských zdrojích, vyžaduje DPF EU a USA, aby zaměstnavatelé zohlednili preference zaměstnanců v oblasti ochrany soukromí omezením přístupu k osobním údajům, anonymizací některých údajů nebo přidělením kódů či pseudonymů (příloha I, oddíl III.9.b.(iii)).

2.2.4 Transparentnost

(25) Subjekty údajů by měly být informovány o hlavních rysech zpracování svých osobních údajů.

(26) To je zajištěno prostřednictvím *zásady oznamování*[36] , která podobně jako požadavky na transparentnost podle nařízení (EU) 2016/679 vyžaduje, aby organizace informovaly subjekty údajů mimo jiné o (i) účasti organizace v DPF, (ii) druhu shromažďovaných údajů, (iii) účelu zpracování, (iv) druhu nebo totožnosti třetích stran, kterým mohou být osobní údaje zpřístupněny, a o účelu tohoto zpřístupnění, (v) jejich individuálních právech, (vi) jak se obrátit na organizaci a (vii) dostupných možnostech nápravy.

(27) Toto oznámení musí být poskytnuto jasným a zřetelným jazykem při první žádosti fyzických osob o poskytnutí osobních údajů nebo co nejdříve poté, v každém případě však předtím, než jsou údaje použity k jinému účelu, než pro který byly shromážděny, nebo předtím, než jsou zpřístupněny třetí straně[37] .

(28) Kromě toho musí organizace zveřejnit své zásady ochrany osobních údajů odrážející zásady (nebo je v případě údajů o lidských zdrojích snadno zpřístupnit dotčeným osobám) a poskytnout odkazy na internetové stránky DoC (s dalšími podrobnostmi o certifikaci, právech subjektů údajů a dostupných mechanismech odvolání), seznam zúčastněných organizací v rámci ochrany osobních údajů (DPF List) a internetové stránky příslušného poskytovatele alternativního řešení sporů[38] .

2.2.5 Individuální práva

(29) Subjekty údajů by měly mít určitá práva, která lze vůči správci nebo zpracovateli uplatnit, zejména právo na přístup k údajům, právo vznést námitku proti zpracování a právo na opravu a výmaz údajů.

(30) Taková práva poskytuje jednotlivcům *zásada přístupu*[39] v rámci DPF mezi EU a USA. Subjekty údajů mají zejména právo bez nutnosti zdůvodnění získat od organizace potvrzení, zda zpracovává osobní údaje, které se jich týkají; nechat si údaje sdělit; a získat informace o účelu zpracování, kategoriích zpracovávaných osobních údajů a (kategoriích) příjemců, kterým jsou údaje sdělovány[40] . Organizace jsou povinny reagovat na

---

36 Příloha I, oddíl II.1.

37 Příloha I oddíl II.1.b. Doplňková zásada 14 (příloha I oddíl III.14.b a c) stanoví zvláštní ustanovení pro zpracování osobních údajů v souvislosti se zdravotnickým výzkumem a klinickými zkouškami. Tato zásada zejména umožňuje organizacím zpracovávat údaje z klinických hodnocení i poté, co osoba od hodnocení odstoupí, pokud to bylo jasně uvedeno v oznámení poskytnutém při souhlasu s účastí. Podobně, pokud organizace DPF v EU a USA obdrží osobní údaje pro účely zdravotnického výzkumu, může je použít pouze pro novou výzkumnou činnost v souladu se zásadami *oznamování* a *volby. V takovém* případě by oznámení jednotlivci mělo v zásadě obsahovat informace o jakémkoli budoucím konkrétním využití údajů (např. související studie). Pokud není možné od počátku zahrnout všechna budoucí použití údajů (protože nové výzkumné použití může vyplynout z nových poznatků nebo vývoje v oblasti medicíny/výzkumu), musí být zahrnuto vysvětlení, že údaje mohou být použity v budoucích nepředvídaných lékařských a farmaceutických výzkumných činnostech. Pokud takové další použití není v souladu s obecnými výzkumnými účely, pro které byly údaje shromážděny, je třeba získat nový souhlas (tj. opt-in). Dále viz konkrétní omezení/výjimky ze zásady *oznamování* popsané v poznámce pod čarou č. 63.

38 Příloha I oddíl III.6.d.

39 Viz také doplňková zásada "Přístup" (příloha I, oddíl III.8).

40 Příloha I, oddíl III.8.a.(i)-(ii).

žádosti o přístup v přiměřené lhůtě.[41] . Organizace může stanovit přiměřené omezení počtu případů, kdy v daném období vyhoví žádostem o přístup od určité osoby, a může účtovat poplatek, který není nepřiměřený, např. pokud jsou žádosti zjevně nadměrné, zejména kvůli jejich opakovanému charakteru[42] .

(31) Právo na přístup lze omezit pouze za výjimečných okolností podobných těm, které jsou stanoveny v právu Unie v oblasti ochrany údajů, zejména pokud by byla porušena oprávněná práva jiných osob; pokud by zátěž nebo náklady spojené s poskytnutím přístupu byly nepřiměřené rizikům pro soukromí jednotlivce za daných okolností případu (ačkoli náklady a zátěž nejsou rozhodujícími faktory při určování, zda je poskytnutí přístupu přiměřené); v rozsahu, v jakém by zpřístupnění mohlo narušit ochranu důležitých protichůdných veřejných zájmů, jako je národní bezpečnost, veřejná bezpečnost nebo obrana; informace obsahují důvěrné obchodní informace; nebo jsou informace zpracovávány výhradně pro výzkumné nebo statistické účely[43] . Každé odepření nebo omezení práva musí být nezbytné a řádně odůvodněné, přičemž organizace nese břemeno prokázání, že tyto požadavky jsou splněny[44] . Pokud je možné oddělit informace od ostatních údajů, na které se omezení vztahuje, musí organizace chráněné informace redigovat a ostatní informace zveřejnit[45] .

(32) Kromě toho mají subjekty údajů právo na opravu nebo změnu nepřesných údajů a na výmaz údajů, které byly zpracovány v rozporu se zásadami[46] . Jak je vysvětleno ve 14. bodě odůvodnění, fyzické osoby mají navíc právo vznést námitku/odmítnout zpracování svých údajů pro podstatně odlišné (ale slučitelné) účely, než pro které byly údaje shromážděny, a právo na poskytnutí svých údajů třetím stranám. Pokud jsou osobní údaje používány pro účely přímého marketingu, mají fyzické osoby obecné právo kdykoli odmítnout zpracování[47] .

(33) Zásady se výslovně nezabývají otázkou rozhodnutí, která se týkají subjektu údajů a která jsou založena výhradně na automatizovaném zpracování osobních údajů. Pokud však jde o osobní údaje, které byly shromážděny v Unii, jakékoliv rozhodnutí založené na automatizovaném zpracování bude obvykle přijímat správce v Unii (který má přímý vztah s dotčeným subjektem údajů), a proto se na něj přímo vztahuje nařízení (EU) 2016/679[48] . To zahrnuje scénáře předávání, kdy zpracování provádí zahraniční (například americký) podnikatelský subjekt, který jedná jako zástupce (zpracovatel) jménem správce v Unii (nebo jako dílčí zpracovatel, který jedná jménem zpracovatele v Unii, jenž údaje obdržel od správce v Unii, který je shromáždil) a který na tomto základě následně přijímá rozhodnutí.

41 Příloha I, oddíl III.8.i.

42 Příloha I, oddíl III.8.f., body i) až ii) a g).

43 Příloha I, oddíl III.4; 8.b, c, e; 14.e, f a 15.d.

44 Příloha I, oddíl III.8.e.(ii). Organizace musí jednotlivce informovat o důvodech zamítnutí/omezení a poskytnout kontaktní místo pro případné další dotazy, oddíl III.8.a.(iii).

45 Příloha I, oddíl III.8.a.(i).

46 Příloha I, oddíl II.6 a III.8.a.(i).

47 Příloha I, oddíl III.8.12.

48 Naopak ve výjimečném případě, kdy má americká organizace přímý vztah se subjektem údajů v Unii, je to obvykle důsledek toho, že se na danou osobu v Unii zaměřila tím, že jí nabízí zboží nebo služby nebo sleduje její chování. V takovém případě bude americká organizace sama spadat do oblasti působnosti nařízení (EU) 2016/679 (čl. 3 odst. 2), a musí tedy přímo dodržovat právo Unie v oblasti ochrany údajů.

(34) To potvrdila i studie, kterou Komise zadala v roce 2018 v rámci druhého výročního přezkumu fungování štítu na ochranu soukromí[49] , která dospěla k závěru, že v té době neexistovaly žádné důkazy naznačující, že by organizace štítu na ochranu soukromí běžně prováděly automatizované rozhodování na základě osobních údajů předávaných v rámci štítu na ochranu soukromí.

(35) V každém případě v oblastech, kde se společnosti s největší pravděpodobností uchylují k automatizovanému zpracování osobních údajů za účelem přijímání rozhodnutí, která mají vliv na jednotlivce (např. poskytování úvěrů, nabídky hypoték, zaměstnání, bydlení a pojištění), nabízí právo USA zvláštní ochranu proti nepříznivým rozhodnutím[50] . Tyto zákony obvykle stanoví, že jednotlivci mají právo být informováni o konkrétních důvodech, na nichž je rozhodnutí založeno (např. zamítnutí úvěru), právo zpochybnit neúplné nebo nepřesné informace (a také právo spoléhat se na nezákonné faktory) a právo na nápravu. V oblasti spotřebitelských úvěrů obsahují zákon o spravedlivém úvěrovém zpravodajství (FCRA) a zákon o rovných úvěrových příležitostech (ECOA) záruky, které spotřebitelům poskytují určitou formu práva na vysvětlení a práva napadnout rozhodnutí. Tyto zákony jsou relevantní v celé řadě oblastí, včetně úvěrů, zaměstnání, bydlení a pojištění. Kromě toho některé antidiskriminační zákony, jako je hlava VII zákona o občanských právech a zákon o spravedlivém bydlení, poskytují jednotlivcům ochranu s ohledem na modely používané při automatizovaném rozhodování, které by mohly vést k diskriminaci na základě určitých charakteristik, a přiznávají jednotlivcům právo napadnout taková rozhodnutí, včetně automatizovaných. Pokud jde o informace o zdravotním stavu, zákon o přenositelnosti a odpovědnosti zdravotního pojištění (Health Insurance Portability and Accountability Act, HIPAA) vytváří určitá práva, která jsou podobná právům GDPR, pokud jde o přístup k osobním zdravotním informacím. Pokyny amerických orgánů navíc vyžadují, aby poskytovatelé zdravotní péče obdrželi informace, které jim umožní informovat jednotlivce o systémech automatizovaného rozhodování používaných ve zdravotnictví[51] .

(36) Proto tato pravidla poskytují ochranu podobnou ochraně poskytované podle práva Unie v oblasti ochrany údajů v nepravděpodobné situaci, kdy by automatizovaná rozhodnutí přijímala samotná organizace DPF EU a USA.

2.2.6 Omezení dalšího předávání

(37) Úroveň ochrany poskytovaná osobním údajům předávaným z Unie organizacím ve Spojených státech nesmí být snížena dalším předáním těchto údajů příjemci ve Spojených státech nebo jiné třetí zemi.

(38) Podle *zásady odpovědnosti při dalším předávání*[52] platí zvláštní pravidla pro tzv. další předávání, tj. předávání osobních údajů z organizace DPF EU a USA správci nebo zpracovateli, který je třetí stranou, bez ohledu na to, zda se nachází ve Spojených státech nebo ve třetí zemi mimo Spojené státy (a

[49] SWD(2018)497final, oddíl 4.1.5. Studie se zaměřila na i) rozsah, v jakém organizace štítu na ochranu soukromí v USA přijímají rozhodnutí týkající se fyzických osob na základě automatizovaného zpracování osobních údajů předávaných ze společností v EU v rámci štítu na ochranu soukromí, a ii) záruky pro fyzické osoby, které federální právo USA pro tento druh situací stanoví, a podmínky pro uplatnění těchto záruk.

[50] Viz např. zákon o rovných úvěrových příležitostech (ECOA, 15 U.S.C. 1691 a násl.), zákon o spravedlivém úvěrovém zpravodajství (FRCA, 15 USC § 1681 a násl.) nebo zákon o spravedlivém bydlení (FHA, 42 U.S.C. 3601 a násl.). Kromě toho se Spojené státy přihlásily k zásadám OECD v oblasti umělé inteligence, které mimo jiné zahrnují zásady transparentnosti, schopnosti vysvětlovat, bezpečnosti a odpovědnosti.

[51] Viz např. pokyny dostupné na adrese 2042 - Jaké osobní zdravotní informace mají jednotlivci podle HIPAA právo získat od svých poskytovatelů zdravotní péče a zdravotních plánů? | HHS.gov.

[52] Viz oddíl II.3 přílohy I a doplňková zásada "Povinné smlouvy pro další převody" (oddíl III.10 přílohy I).

Unie). Jakékoli další předání se může uskutečnit pouze (i) pro omezené a stanovené účely,
(ii) na základě smlouvy mezi organizací DPF EU a USA a třetí stranou[53] (nebo srovnatelného ujednání v rámci skupiny podniků[54]) a (iii) pouze v případě, že tato smlouva vyžaduje, aby třetí strana poskytla stejnou úroveň ochrany, jakou zaručují Zásady.

(39) Tato povinnost poskytovat stejnou úroveň ochrany, jakou zaručují zásady, ve spojení se *zásadou integrity údajů a omezení účelu* znamená zejména to, že třetí strana může zpracovávat osobní údaje, které jí byly předány, pouze pro účely, které nejsou neslučitelné s účely, pro které byly shromážděny nebo následně schváleny jednotlivcem (v souladu se *zásadou volby)*.

(40) *Zásadu odpovědnosti za další předávání* je třeba chápat rovněž ve spojení se *zásadou oznamování* a v případě dalšího předávání správci, který je třetí stranou[55] , se *zásadou volby,* podle níž musí být subjekty údajů informovány (mimo jiné) o typu/identitě jakéhokoli příjemce, účelu dalšího předávání a nabízené volbě a mohou vznést námitku (opt out) nebo v případě citlivých údajů musí dát "výslovný souhlas" (opt in) s dalším předáváním.

(41) Povinnost zajistit stejnou úroveň ochrany, jakou vyžadují Zásady, se vztahuje na všechny třetí strany, které se podílejí na zpracování takto předaných údajů, bez ohledu na jejich umístění (v USA nebo v jiné třetí zemi), jakož i v případě, že původní třetí strana-příjemce sama předá tyto údaje jiné třetí straně-příjemci, například pro účely dílčího zpracování.

(42) Ve všech případech musí být ve smlouvě s příjemcem, který je třetí stranou, stanoveno, že příjemce oznámí organizaci DPF EU a USA, pokud zjistí, že již nemůže splnit svůj závazek. Pokud k takovému zjištění dojde, musí být zpracování třetí stranou ukončeno nebo musí být přijata jiná přiměřená a vhodná opatření k nápravě situace[56] .

(43) Další ochrana se uplatňuje v případě dalšího předávání údajů zástupci třetí strany (tj. zpracovateli). V takovém případě musí americká organizace zajistit, aby zprostředkovatel jednal pouze na základě jejích pokynů, a přijmout přiměřená a vhodná opatření, aby i) zajistila, že

[53] Jako výjimku z této obecné zásady může organizace dále předávat osobní údaje malého počtu zaměstnanců, aniž by s příjemcem uzavřela smlouvu, a to pro příležitostné provozní potřeby související se zaměstnáním, např. pro rezervaci letu, hotelového pokoje nebo pojištění. I v tomto případě však musí organizace dodržovat zásady *oznamování* a *volby* (viz příloha I oddíl III.9.e).

[54] Viz doplňková zásada "Povinné smlouvy pro další převody" (příloha I, oddíl III.10.b). Tato zásada sice umožňuje předávání založené i na mimosmluvních nástrojích (např. na vnitroskupinových programech shody a kontroly), ale text jasně stanoví, že tyto nástroje musí vždy "zajišťovat kontinuitu ochrany osobních údajů podle těchto zásad". Navíc vzhledem k tomu, že certifikovaná americká organizace bude i nadále odpovědná za dodržování Zásad, bude mít silnou motivaci používat nástroje, které jsou v praxi skutečně účinné.

[55] Fyzické osoby nemají právo na odmítnutí, pokud jsou osobní údaje předávány třetí straně, která jedná jako zástupce a plní úkoly jménem a podle pokynů organizace USA. To však vyžaduje uzavření smlouvy se zástupcem a americká organizace ponese odpovědnost za zaručení ochrany poskytované podle zásad tím, že bude vykonávat své příkazní pravomoci.

[56] Situace se liší podle toho, zda je třetí strana správcem nebo zpracovatelem (agentem). V prvním případě musí smlouva s třetí stranou stanovit, že třetí strana ukončí zpracování nebo přijme jiná přiměřená a vhodná opatření k nápravě situace. V druhém případě je na EU americká organizace DPF - jako ten, kdo kontroluje zpracování, podle jehož pokynů agent pracuje - přijmout tato opatření. Viz oddíl II.3 přílohy I.

účinně zpracovává předané osobní údaje způsobem, který je v souladu s povinnostmi organizace podle Zásad, a ii) na základě upozornění zastavit a napravit neoprávněné zpracování[57] . DoC může po organizaci požadovat, aby poskytla shrnutí nebo reprezentativní kopii ustanovení smlouvy o ochraně osobních údajů[58] . Pokud v řetězci (dílčích) zpracování vzniknou problémy s dodržováním předpisů, organizace jednající jako správce osobních údajů bude v zásadě čelit odpovědnosti, jak je uvedeno v *zásadě regresu, vymáhání a odpovědnosti, s* výjimkou případů, kdy prokáže, že není odpovědná za událost, která vedla ke vzniku škody[59] .

2.2.7 Odpovědnost

(44) Podle zásady odpovědnosti musí subjekty, které zpracovávají údaje, zavést vhodná technická a organizační opatření, aby účinně plnily své povinnosti v oblasti ochrany údajů, a musí být schopny toto plnění prokázat, zejména příslušnému dozorovému úřadu.

(45) Jakmile se organizace dobrovolně rozhodne certifikovat[60] v rámci DPF EU a USA, je její účinné dodržování zásad povinné a vymahatelné. Podle *zásady odvolání, prosazování a odpovědnosti*[61] musí organizace DPF EU-SA poskytnout účinné mechanismy k zajištění dodržování zásad. Organizace musí rovněž přijmout opatření k ověření[62] , zda jejich zásady ochrany osobních údajů odpovídají Zásadám a zda jsou skutečně dodržovány. To lze provést buď prostřednictvím systému sebehodnocení, který musí zahrnovat interní postupy zajišťující, že zaměstnanci absolvují školení o provádění zásad ochrany soukromí organizace a že dodržování zásad je pravidelně objektivně přezkoumáváno, nebo prostřednictvím externích kontrol dodržování zásad, jejichž metody mohou zahrnovat audit, namátkové kontroly nebo použití technologických nástrojů.

(46) Kromě toho musí organizace uchovávat záznamy o provádění svých postupů v oblasti DPF v EU a USA a na požádání je zpřístupnit v souvislosti s vyšetřováním nebo stížností na nedodržování předpisů nezávislému orgánu pro řešení sporů nebo příslušnému donucovacímu orgánu[63] .

2.3 Správa, dohled a prosazování

(47) DoC bude spravovat a monitorovat DPF EU a USA. Rámec stanoví mechanismy dohledu a vymáhání, aby bylo možné ověřit a zajistit, že organizace DPF EU a USA dodržují zásady a že případné nedodržení zásad bude řešeno. Tyto mechanismy jsou uvedeny v Zásadách (příloha I) a v závazcích přijatých DoC (příloha III), FTC (příloha IV) a DoT (příloha V).

2.3.1 (Opětovná) certifikace

(48) Aby organizace získaly certifikaci v rámci DPF EU a USA (nebo ji každoročně obnovovaly), musí veřejně deklarovat svůj závazek dodržovat zásady, učinit

---

57 Příloha I oddíl II.3.b.
58 *Tamtéž*.
59 Příloha I oddíl II.7.d.
60 Viz také doplňková zásada "Vlastní certifikace" (příloha I, oddíl III.6).
61 Viz také doplňková zásada "Řešení sporů a prosazování" (příloha I, oddíl III.11).
62 Viz také doplňková zásada "Ověřování" (příloha I, oddíl III.7).
63 Příloha I, oddíl III.7.

své zásady ochrany osobních údajů k dispozici a plně je uplatňovat[64] . V rámci jejich (opětovného)
)v žádosti o certifikaci musí organizace předložit DoC mimo jiné informace o názvu příslušné organizace, popis účelu, pro který bude organizace zpracovávat osobní údaje, osobní údaje, na které se bude certifikace vztahovat, jakož i zvolenou metodu ověření, příslušný nezávislý mechanismus odvolání a statutární orgán, který má pravomoc vymáhat dodržování zásad[65] .

(49) Organizace mohou získávat osobní údaje na základě DPF EU - USA ode dne, kdy je DoC zařadí na seznam DPF. Aby byla zajištěna právní jistota a zabránilo se "falešným tvrzením", nesmí organizace, které certifikují poprvé, veřejně odkazovat na své dodržování zásad dříve, než DoC rozhodne, že předložení certifikace organizace je úplné, a zařadí organizaci na seznam DPF[66] . Aby se tyto organizace mohly i nadále spoléhat na DPF EU a USA při přijímání osobních údajů z Unie, musí každoročně znovu potvrdit svou účast v rámci. Pokud organizace z jakéhokoli důvodu opustí seznam DPF EU a USA, musí odstranit všechna prohlášení, která naznačují, že se organizace nadále účastní rámce[67] .

(50) Jak se odráží v závazcích uvedených v příloze III, DoC bude ověřovat, zda organizace splňují všechny požadavky na certifikaci a zda zavedly (veřejnou) politiku ochrany osobních údajů obsahující informace požadované podle *zásady oznamování*[68] . Na základě zkušeností s procesem (re)certifikace v rámci štítu na ochranu soukromí bude DoC provádět řadu kontrol, mimo jiné ověří, zda zásady ochrany soukromí organizací obsahují hypertextový odkaz na správný formulář stížnosti na internetových stránkách příslušného mechanismu pro řešení sporů, a pokud je do žádosti o certifikaci zahrnuto několik subjektů a dceřiných společností jedné organizace, zda zásady ochrany soukromí každého z těchto subjektů splňují požadavky na certifikaci a jsou snadno dostupné subjektům údajů[69] . Kromě toho bude DoC v případě potřeby provádět křížové kontroly s FTC a DoT, aby ověřil, zda organizace podléhají orgánu dohledu uvedenému v jejich žádostech o (opětovnou) certifikaci, a bude spolupracovat se subjekty alternativního řešení sporů, aby ověřil, zda jsou organizace registrovány pro nezávislý mechanismus řešení sporů uvedený v jejich žádostech o (opětovnou) certifikaci[70] .

(51) DoC informuje organizace, že pro dokončení (re)certifikace musí vyřešit všechny problémy zjištěné během přezkumu. V případě, že organizace nereaguje ve lhůtě stanovené DoC (například pokud jde o re-certifikaci, očekává se, že proces bude dokončen do 45 dnů)[71] nebo jinak nedokončí svou certifikaci, bude podání považováno za opuštěné. V takovém případě

---

64 Příloha I oddíl I. 2.

65 Příloha I oddíl III.6.b a příloha III, viz oddíl "Ověření požadavků na vlastní certifikaci".

66 Příloha I, poznámka pod čarou 12.

67 Příloha I oddíl III.6.h.

68 Příloha I, oddíl III.6.a a poznámka pod čarou 12, jakož i příloha III, viz oddíl "Ověřit požadavky na vlastní certifikaci".

69 Příloha III, oddíl "Ověřit požadavky na vlastní certifikaci.

70 Podobně bude DoC spolupracovat s třetí stranou, která bude sloužit jako správce finančních prostředků vybraných prostřednictvím poplatku za panel DPA (viz 71. bod odůvodnění), aby ověřila, zda organizace, které si zvolí DPA jako svůj nezávislý mechanismus pro regresní úhradu, zaplatily poplatek za příslušný rok. Viz příloha III, oddíl "Požadavky na ověření vlastní certifikace".

71 Příloha III, poznámka pod čarou 2.

v případě jakéhokoli nepravdivého prohlášení o účasti nebo souladu s DPF mezi EU a USA může být předmětem donucovacích opatření ze strany FTC nebo DoT[72] .

(52) Aby bylo zajištěno řádné uplatňování DPF EU a USA, musí být zainteresované strany, jako jsou subjekty údajů, vývozci údajů a vnitrostátní orgány pro ochranu údajů, schopny identifikovat organizace, které zásady dodržují. V zájmu zajištění takové transparentnosti na "vstupním bodě" se DoC zavázal vést a zpřístupnit veřejnosti seznam organizací, které osvědčily, že dodržují zásady, a spadají do pravomoci alespoň jednoho z donucovacích orgánů uvedených v přílohách IV a V tohoto rozhodnutí[73] . DoC bude seznam aktualizovat na základě každoročního předložení opětovného osvědčení organizace a vždy, když organizace odstoupí nebo je vyřazena z DPF EU a USA. Aby byla zaručena transparentnost i v "bodě odchodu", bude DoC vést a zpřístupňovat veřejnosti záznamy o organizacích, které byly ze seznamu vyškrtnuty, přičemž v každém případě uvede důvod takového vyškrtnutí[74] . V neposlední řadě poskytne odkaz na internetové stránky FTC na stránkách EU.
U.S. DPF, který bude uvádět donucovací opatření FTC podle rámce[75] .

2.3.2 Kontrola dodržování předpisů

(53) DoC bude průběžně monitorovat účinné dodržování zásad organizacemi EU a USA v oblasti DPF prostřednictvím různých mechanismů[76] . Zejména bude provádět "namátkové kontroly" náhodně vybraných organizací, jakož i ad hoc namátkové kontroly konkrétních organizací, pokud budou zjištěny potenciální problémy s dodržováním zásad (např. nahlášené DoC třetími stranami), s cílem ověřit, zda (i) jsou k dispozici kontaktní místa pro vyřizování stížností a žádostí subjektů údajů a zda na ně reagují;
(ii) zásady ochrany osobních údajů organizace jsou snadno dostupné jak na jejích internetových stránkách, tak prostřednictvím hypertextového odkazu na internetových stránkách DoC; iii) zásady ochrany osobních údajů organizace jsou nadále v souladu s požadavky na certifikaci a iv) pro řešení stížností je k dispozici zvolený nezávislý mechanismus řešení sporů organizace[77] .

(54) Pokud existují věrohodné důkazy o tom, že organizace neplní své závazky vyplývající z DPF EU a USA (včetně případů, kdy DoC obdrží stížnosti nebo organizace uspokojivě neodpovídá na dotazy DoC), DoC bude požadovat, aby organizace vyplnila a předložila podrobný dotazník[78] . Organizace, která na dotazník uspokojivě a včas neodpoví, bude postoupena příslušnému orgánu (FTC nebo DoT) k případnému vymáhání práva[79] . V rámci monitorování dodržování předpisů v rámci štítu na ~~ochranu soukromí DoC~~

[72] Viz příloha III, oddíl "Požadavky na ověření vlastní certifikace".

[73] Informace o správě seznamu DPF lze nalézt v příloze III (viz úvod v části "Správa a dohled nad rámcovým programem ochrany osobních údajů ze strany ministerstva obchodu") a v příloze I (oddíl I.3, oddíl I.4, oddíl III.6.d a oddíl III.11.g).

[74] Příloha III, viz úvod v části "Správa rámcového programu ochrany osobních údajů a dohled nad ním ze strany ministerstva obchodu".

[75] Viz příloha III, oddíl "Přizpůsobení webové stránky rámce ochrany osobních údajů cílovým skupinám".

[76] Viz příloha III, oddíl "Provádění pravidelných přezkumů a hodnocení souladu rámcového programu ochrany osobních údajů z moci úřední".

[77] V rámci svých monitorovacích činností může DoC používat různé nástroje, včetně kontroly nefunkčních odkazů na zásady ochrany osobních údajů nebo aktivního sledování zpráv, které poskytují věrohodné důkazy o nedodržování zásad.

[78] Viz příloha III, oddíl "Provádění pravidelných přezkumů a hodnocení souladu rámcového programu ochrany osobních údajů z moci úřední".

[79] Viz příloha III, oddíl "Provádění pravidelných přezkumů a hodnocení souladu rámcového programu ochrany osobních údajů z moci úřední".

pravidelně prováděla namátkové kontroly uvedené v 53. bodě odůvodnění a průběžně sledovala veřejné zprávy, což jí umožnilo identifikovat, řešit a vyřešit problémy s dodržováním předpisů[80] . Organizace, které trvale nedodržují zásady, budou vyřazeny ze seznamu DPF a musí vrátit nebo vymazat osobní údaje získané na základě rámce[81] .

(55) V ostatních případech odstranění, jako je dobrovolné odstoupení od účasti nebo neprovedení recertifikace, musí organizace údaje buď vymazat nebo vrátit, nebo si je může ponechat, pokud každoročně potvrdí DoC svůj závazek pokračovat v uplatňování zásad nebo zajistí odpovídající ochranu osobních údajů jiným povoleným způsobem (např. použitím smlouvy, která plně odráží požadavky příslušných standardních smluvních doložek schválených Komisí)[82] . V tomto případě musí organizace rovněž určit kontaktní místo v rámci organizace pro všechny otázky týkající se DPF EU a USA.

2.3.3 Identifikace a řešení nepravdivých tvrzení o účasti

(56) DoC bude monitorovat případná nepravdivá tvrzení o účasti v DPF EU a USA nebo nesprávné používání certifikační značky DPF EU a USA, a to jak z moci úřední, tak na základě stížností (např. obdržených od orgánů pro ochranu údajů)[83] . DoC bude zejména průběžně ověřovat, zda organizace, které (i) odstoupí z účasti v EU-U.S. DPF, (ii) nedokončí roční recertifikaci (tj. buď zahájí, ale nedokončí roční recertifikační proces včas, nebo roční recertifikační proces vůbec nezahájí), (iii) budou odstraněny jako účastníci, zejména pro "trvalé neplnění", nebo (iv) nedokončí počáteční certifikaci (tj.tj. zahájily, ale nedokončily proces počáteční certifikace včas), odstranit ze všech příslušných zveřejněných zásad ochrany osobních údajů odkazy na Rámec pro ochranu osobních údajů mezi EU a USA, které naznačují, že se organizace aktivně účastní Rámce[84] . DoC bude rovněž provádět internetové vyhledávání s cílem identifikovat odkazy na rámec EU a USA pro ochranu soukromí v zásadách ochrany soukromí organizací, včetně identifikace nepravdivých tvrzení organizací, které se nikdy neúčastnily rámce EU a USA pro ochranu soukromí[85] .

(57) Pokud DoC zjistí, že odkazy na DPF EU a USA nebyly odstraněny nebo jsou používány nesprávně, informuje organizaci o možném postoupení případu FTC/DoT[86] . Pokud organizace nereaguje dostatečně staticky, předá DoC záležitost příslušné agentuře k případnému vymáhání práva[87] . Jakékoli

---

80 Během druhého ročního přezkumu štítu na ochranu soukromí informovala DoC, že provedla namátkové kontroly u 100 organizací a v 21 případech zaslala dotazníky o dodržování předpisů (poté byly zjištěné problémy odstraněny), viz pracovní dokument Komise (2018) 497 final, s. 9. Podobně úřad DoC během třetího výročního přezkumu štítu na ochranu soukromí informoval, že na základě monitorování veřejných zpráv zjistil tři incidenty a zahájil praxi provádění namátkových kontrol u 30 společností každý měsíc, což vedlo k následným kontrolám s dotazníky o dodržování předpisů ve 28 % případů (po nichž byly zjištěné problémy okamžitě napraveny nebo ve třech případech vyřešeny po zaslání varovného dopisu), viz pracovní dokument Komise (2019) 495 final, s. 8.

81 Příloha I oddíl III.11.g. Trvalý nesoulad vzniká zejména tehdy, pokud organizace odmítne vyhovět konečnému rozhodnutí samoregulačního orgánu pro ochranu soukromí, nezávislého orgánu pro řešení sporů nebo orgánu pro vymáhání práva.

82 Příloha I oddíl III.6.f.

83 Příloha III, oddíl "Vyhledávání a řešení nepravdivých tvrzení o účasti".

84 *Tamtéž.*

85 *Tamtéž.*

86 *Tamtéž.*

87 V rámci štítu na ochranu soukromí oznámilo ministerstvo vnitra během třetího výročního přezkumu rámce, že zjistilo 669 případů falešných žádostí o účast (mezi říjnem 2018 a říjnem 2019), z nichž většina byla

zkreslování informací, které organizace poskytuje veřejnosti ohledně dodržování zásad formou zavádějících prohlášení nebo praktik, je předmětem donucovacích opatření ze strany FTC, DoT nebo jiných příslušných donucovacích orgánů USA. Zkreslená prohlášení vůči DoT jsou vymahatelná podle zákona o nepravdivých prohlášeních (18 U.S.C. § 1001).

2.3.4 Vymáhání práva

(58) Aby byla v praxi zaručena odpovídající úroveň ochrany údajů, měl by být zřízen nezávislý dozorový úřad, který by byl pověřen monitorováním a vymáháním dodržování pravidel ochrany údajů.

(59) Organizace DPF mezi EU a USA musí podléhat jurisdikci příslušných amerických orgánů - FTC a DoT - které mají nezbytné vyšetřovací a donucovací pravomoci k účinnému zajištění dodržování zásad[88] .

(60) FTC je nezávislý orgán složený z pěti komisařů, kteří jsou jmenováni prezidentem s doporučením a souhlasem Senátu[89] . Komisaři jsou jmenováni na sedmileté funkční období a mohou být odvoláni prezidentem pouze z důvodu neefektivity, zanedbání povinností nebo nesprávného výkonu funkce. FTC může mít nejvýše tři komisaře z téže politické strany a komisaři nesmějí po dobu svého jmenování vykonávat žádnou jinou činnost, povolání nebo zaměstnání.

(61) FTC může vyšetřovat dodržování zásad, jakož i nepravdivá tvrzení o dodržování zásad nebo účasti v DPF EU a USA ze strany organizací, které již nejsou na seznamu DPF nebo nikdy necertifikovaly[90] . FTC může vymáhat dodržování předpisů tím, že bude žádat o vydání správních nebo federálních soudních příkazů (včetně "souhlasných příkazů" dosažených prostřednictvím narovnání)[91] o předběžné nebo trvalé soudní příkazy nebo jiná nápravná opatření a bude systematicky sledovat dodržování těchto příkazů[92] . Pokud organizace takové příkazy nedodrží, může FTC požadovat občanskoprávní sankce a další nápravná opatření, včetně náhrady škody způsobené protiprávním jednáním. Každý souhlasný příkaz vydaný organizaci DPF EU a USA bude obsahovat ustanovení o podávání vlastních zpráv[93] , přičemž organizace budou povinny zveřejnit všechny příslušné části týkající se DPF EU a USA v jakékoli zprávě o dodržování předpisů nebo hodnotící zprávě předložené FTC. A konečně, FTC bude vést online seznam organizací, na které se vztahují příkazy FTC nebo soudu v případech DPF EU a USA[94] .

---

které byly vyřešeny po varovném dopise DoC, přičemž 143 případů bylo postoupeno FTC (viz 61. bod odůvodnění níže). Viz dokument Komise SWD (2019) 495 final, s. 10.

88 Organizace DPF EU a USA musí veřejně prohlásit svůj závazek dodržovat zásady, zveřejnit své zásady ochrany osobních údajů v souladu s těmito zásadami a plně je uplatňovat. Nedodržení těchto zásad je vymahatelné podle § 5 zákona FTC, který zakazuje nekalé a klamavé jednání v obchodě nebo při ovlivňování obchodu (15 U.S.C. §45), a § 41712 zákona U.S.C., který zakazuje dopravci nebo zprostředkovateli prodeje letenek používat nekalé nebo klamavé praktiky v letecké dopravě nebo při prodeji letecké dopravy.

89 15 U.S.C. § 41.

90 Příloha IV.

91 Podle informací FTC nemá pravomoc provádět kontroly na místě v oblasti ochrany soukromí. Má však pravomoc přimět organizace k předložení dokumentů a poskytnutí svědeckých výpovědí (viz § 20 zákona o FTC) a v případě nedodržení těchto příkazů může využít soudní systém k jejich vymáhání.

92 Viz příloha IV, oddíl "Vyhledávání a monitorování příkazů".

93 FTC nebo soudní příkazy mohou vyžadovat, aby společnosti zavedly programy ochrany soukromí a pravidelně předkládaly FTC zprávy o dodržování těchto programů nebo jejich hodnocení nezávislými třetími stranami.

94 Příloha IV, oddíl "Vyhledávání a monitorování příkazů".

(62) Pokud jde o štít na ochranu soukromí, FTC podnikla donucovací kroky přibližně ve 22 případech, a to jak v souvislosti s porušením konkrétních požadavků rámce (např. nepotvrzení DoC, že organizace pokračuje v uplatňování ochrany štítu na ochranu soukromí i poté, co rámec opustila, neověření prostřednictvím sebehodnocení nebo externí kontroly dodržování požadavků, že organizace dodržuje rámec)[95] , tak v souvislosti s nepravdivými tvrzeními o účasti v rámci (např.organizace, které nedokončily kroky nezbytné k získání certifikace nebo nechaly svou certifikaci zaniknout, ale nepravdivě uvedly, že se nadále účastní rámce)[96] . Tato donucovací opatření mimo jiné vyplynula z proaktivního využívání správních předvolání k získání materiálů od některých účastníků štítu na ochranu soukromí za účelem kontroly, zda nedochází k podstatnému porušování povinností štítu na ochranu soukromí[97] .

(63) DoT má výlučnou pravomoc regulovat postupy leteckých společností v oblasti ochrany soukromí a sdílí pravomoc s FTC, pokud jde o postupy zprostředkovatelů prodeje letenek při ochraně soukromí v letecké dopravě. Úředníci DoT se nejprve snaží dosáhnout urovnání, a pokud to není možné, mohou zahájit řízení o vymáhání práva zahrnující důkazní řízení před správním soudcem DoT, který je oprávněn vydávat příkazy k zastavení činnosti a občanskoprávní sankce[98] . Správní soudci požívají několika ochranných opatření podle zákona o správním řízení (Administrative Procedure Act - APA), která zajišťují jejich nezávislost a nestrannost. Například mohou být odvoláni pouze z dobrého důvodu; jsou přidělováni k případům na základě rotace; nesmějí vykonávat povinnosti neslučitelné s jejich povinnostmi a odpovědností jako správních soudců; nepodléhají dohledu vyšetřovacího týmu orgánu, u kterého jsou zaměstnáni (v tomto případě ministerstva dopravy); a musí vykonávat svou funkci rozhodování/vykonávání nestranně[99] . DoT se zavázal, že bude monitorovat příkazy k výkonu rozhodnutí a zajistí, aby příkazy vyplývající z nařízení EU
Případy americké společnosti DPF jsou k dispozici na jejích internetových stránkách[100] .

2.4 Náprava

(64) Aby byla zajištěna odpovídající ochrana a zejména prosazování práv jednotlivce, měla by být subjektu údajů poskytnuta účinná správní a soudní náprava.

(65) *Zásada odvolání, vymáhání a odpovědnosti v* rámci DPF EU a USA vyžaduje, aby organizace poskytly fyzickým osobám, které jsou postiženy nedodržováním předpisů, odvolání, a tedy možnost, aby subjekty údajů v Unii podávaly stížnosti týkající se nedodržování předpisů ze strany organizací v rámci DPF EU a USA a aby tyto stížnosti byly vyřešeny, v případě potřeby rozhodnutím, které zajistí účinnou nápravu[101] . Organizace musí v rámci své certifikace splnit požadavky této zásady tím, že zajistí účinné a snadno dostupné nezávislé mechanismy opravných prostředků, a to tak, že

---

95 Komise SWD (2019) 495 final, s. 11.

96 Viz případy uvedené na webových stránkách FTC, které jsou k dispozici na adrese https://www.ftc.gov/business-guidance/privacy- security/privacy-shield. Viz také SWD Komise (2017) 344 final, s. 17; SWD Komise (2018) 497 final, s. 12 a SWD Komise (2019) 495 final, s. 11.

97 Viz např. Připravené poznámky předsedy Josepha Simonse na druhém výročním hodnocení štítu na ochranu soukromí (ftc.gov).

98 Viz příloha V, oddíl "Postupy vymáhání".

99 Viz 5 U.S.C. §§ 3105, 7521(a), 554(d) a 556(b)(3).

100 Příloha V, viz oddíl "Monitorování a vydávání veřejných příkazů k výkonu rozhodnutí týkajících se porušování DPF mezi EU a USA".

101 Příloha I, oddíl II.7.

v němž mohou být stížnosti a spory každého jednotlivce prošetřeny a urychleně vyřešeny bez jakýchkoli nákladů pro jednotlivce[102] .

(66) Organizace si mohou zvolit nezávislé mechanismy odvolání buď v Unii, nebo ve Spojených státech. Jak je podrobněji vysvětleno v 71. bodě odůvodnění, zahrnuje to možnost dobrovolně se zavázat ke spolupráci s orgány EU pro ochranu údajů. Pokud organizace zpracovávají údaje o lidských zdrojích, je takový závazek ke spolupráci s orgány EU pro ochranu údajů povinný. Mezi další alternativy patří nezávislé alternativní řešení sporů nebo programy ochrany soukromí vytvořené soukromým sektorem, které zahrnují zásady do svých pravidel. Ty musí zahrnovat účinné mechanismy prosazování v souladu s požadavky *Zásady odvolatelnosti, prosazování a odpovědnosti*.

(67) V důsledku toho poskytuje směrnice o ochraně osobních údajů mezi EU a USA subjektům údajů řadu možností, jak vymáhat svá práva, podávat stížnosti na nedodržování předpisů ze strany organizací EU a USA a jak dosáhnout vyřešení svých stížností, v případě potřeby prostřednictvím rozhodnutí o účinné nápravě. Fyzické osoby mohou podat stížnost přímo organizaci, nezávislému orgánu pro řešení sporů určenému organizací, vnitrostátním orgánům pro ochranu údajů, DoC nebo FTC. V případech, kdy jejich stížnosti nebyly vyřešeny žádným z těchto mechanismů odvolání nebo vymáhání, mají fyzické osoby rovněž právo dovolávat se závazného rozhodčího řízení (příloha I přílohy I tohoto rozhodnutí). S výjimkou rozhodčího soudu, který vyžaduje vyčerpání některých opravných prostředků před jeho uplatněním, mohou jednotlivci využít některý z opravných prostředků nebo všechny mechanismy podle svého výběru a nejsou povinni zvolit jeden mechanismus místo druhého nebo dodržet určitou posloupnost.

(68) Zaprvé, subjekty údajů v Unii mohou případy nedodržování zásad řešit prostřednictvím **přímých kontaktů s organizacemi EU a USA pro ochranu osobních údajů**[103] . Pro usnadnění řešení musí organizace zavést účinný mechanismus nápravy pro řešení takových stížností. Politika ochrany osobních údajů organizace proto musí jasně informovat fyzické osoby o kontaktním místě, ať už v rámci organizace, nebo mimo ni, které bude vyřizovat stížnosti (včetně jakékoli příslušné instituce v Unii, která může reagovat na dotazy nebo stížnosti), a také o určeném nezávislém orgánu pro řešení sporů (viz 69. bod odůvodnění). Po obdržení stížnosti jednotlivce, a to přímo od jednotlivce nebo prostřednictvím orgánu pro ochranu údajů po postoupení orgánem pro ochranu údajů, musí organizace poskytnout subjektu údajů v Unii odpověď ve lhůtě 45 dnů[104] . Stejně tak jsou organizace povinny neprodleně reagovat na dotazy a jiné žádosti o informace od DoC nebo od orgánu pro ochranu údajů[105] (pokud se organizace zavázala spolupracovat s orgánem pro ochranu údajů) týkající se dodržování zásad.

(69) Za druhé, jednotlivci mohou podat stížnost také přímo **nezávislému orgánu pro řešení sporů** (buď ve Spojených státech, nebo v Unii), který organizace určila k prošetření a vyřešení individuálních stížností (pokud nejsou zjevně neopodstatněné nebo neopodstatněné) a k bezplatnému poskytnutí odpovídajícího opravného prostředku jednotlivci[106] . Sankce a nápravná opatření uložená takovým orgánem musí být dostatečně přísná, aby zajistila, že organizace budou dodržovat zásady, a měla by umožnit, aby organizace zvrátila nebo napravila účinky nedodržení zásad.

---

102 Příloha I, oddíl III.11.

103 Příloha I, oddíl III.11.d.(i).

104 Příloha I, oddíl III.11.d.(i).

105 Jedná se o zpracovatelský orgán určený skupinou orgánů pro ochranu údajů stanovenou v doplňkové zásadě "Úloha orgánů pro ochranu údajů" (příloha I, oddíl III.5).

106 Příloha I oddíl III.11.d.

dodržování předpisů a v závislosti na okolnostech ukončení dalšího zpracování dotčených osobních údajů a/nebo jejich výmaz, jakož i zveřejnění zjištění o nedodržení předpisů[107] . Nezávislé orgány pro řešení sporů určené organizací jsou povinny na svých veřejných internetových stránkách uvádět příslušné informace týkající se rámce pro řešení sporů mezi EU a USA a služeb, které v jeho rámci poskytují[108] . Každoročně musí zveřejnit výroční zprávu obsahující souhrnné statistiky týkající se těchto služeb[109] .

(70) V rámci svých postupů kontroly dodržování předpisů může DoC ověřit, zda jsou organizace DPF EU a USA skutečně registrovány u nezávislých mechanismů pro regresní řízení, o nichž tvrdí, že jsou u nich registrovány[110] . Jak organizace, tak odpovědné nezávislé mechanismy pro regresy jsou povinny neprodleně reagovat na dotazy a žádosti DoC o informace týkající se DPF EU a USA. DoC bude spolupracovat s nezávislými mechanismy pro zjednávání nápravy, aby ověřil, zda na svých internetových stránkách uvádějí informace o zásadách a službách, které poskytují v rámci DPF EU a USA, a zda zveřejňují výroční zprávy[111] .

(71) V případech, kdy organizace nedodrží rozhodnutí orgánu pro řešení sporů nebo samoregulačního orgánu, musí tento orgán oznámit toto nedodržení DoC a FTC (nebo jinému orgánu USA příslušnému k vyšetřování nedodržení ze strany organizace), případně příslušnému soudu[112] . Pokud se organizace odmítne podřídit konečnému rozhodnutí jakéhokoli samoregulačního orgánu, nezávislého orgánu pro řešení sporů v oblasti ochrany soukromí nebo vládního orgánu, nebo pokud takový orgán zjistí, že organizace často nedodržuje zásady, může to být považováno za trvalé nedodržování zásad, což má za následek, že DoC po předchozím 30denním upozornění a možnosti odpovědět organizaci, která nedodržela zásady, vyškrtne organizaci ze seznamu DPF[113] . Pokud organizace po vyškrtnutí ze seznamu nadále uplatňuje nárok na certifikaci DPF mezi EU a USA, DoC ji postoupí FTC nebo jinému donucovacímu orgánu[114] .

(72) Zatřetí, fyzické osoby mohou své stížnosti podávat také **vnitrostátnímu orgánu pro ochranu údajů v** Unii. Organizace jsou povinny spolupracovat při vyšetřování a řešení stížnosti orgánem pro ochranu údajů buď v případě, že se týká zpracování údajů o lidských zdrojích shromážděných v souvislosti s pracovněprávním vztahem, nebo pokud se příslušná organizace dobrovolně podrobila dohledu ze strany orgánů pro ochranu údajů[115] . Organizace musí zejména reagovat na dotazy, vyhovět doporučením orgánu pro ochranu údajů, včetně nápravných nebo kompenzačních opatření, a poskytnout orgánu pro ochranu údajů písemné potvrzení, že taková opatření byla přijata[116] .

---

107 Příloha I, oddíl II.7 a III.11.e.

108 Příloha I, oddíl III.11.d.(ii).

109 Výroční zpráva musí obsahovat: (1) celkový počet stížností týkajících se DPF mezi EU a USA, které byly přijaty během vykazovaného roku; (2) druhy přijatých stížností; (3) opatření pro kvalitu řešení sporů, jako je doba potřebná k vyřízení stížností; a (4) výsledky přijatých stížností, zejména počet a druhy nápravných opatření nebo uložených sankcí.

110 Příloha I, oddíl "Ověření požadavků na vlastní certifikaci".

111 Viz příloha III, oddíl "Usnadnění spolupráce s orgány alternativního řešení sporů, které poskytují služby související se zásadami". Viz také příloha I, oddíl III.11.d.(ii)-(iii).

112 Viz příloha I oddíl III.11.e.

113 Viz příloha I oddíl III.11.g, zejména body ii) a iii).

114 Viz příloha III, oddíl "Vyhledávání a řešení nepravdivých tvrzení o účasti".

115 Příloha I oddíl II.7.b.

116 Příloha I, oddíl III.5.

(73) Pro usnadnění spolupráce v zájmu účinného vyřizování stížností zřídily jak DoC, tak FTC zvláštní kontaktní místo, které je odpovědné za přímý kontakt s orgány pro ochranu údajů[117] . Tato kontaktní místa pomáhají s dotazy orgánů pro ochranu údajů týkajícími se dodržování zásad ze strany organizace.

(74) Poradenství poskytované úřadem pro ochranu údajů[118] je vydáváno poté, co obě strany sporu měly přiměřenou příležitost se k němu vyjádřit a předložit případné důkazy. Panel může vydat radu tak rychle, jak to umožňuje požadavek na řádný proces, a to zpravidla do 60 dnů od obdržení stížnosti[119] . Pokud organizace nevyhoví do 25 dnů od doručení rady a nenabídne uspokojivé vysvětlení prodlení, může panel oznámit svůj záměr buď předložit věc FTC (nebo jinému příslušnému donucovacímu orgánu USA), nebo dojít k závěru, že závazek ke spolupráci byl vážně porušen. V prvním případě to může vést k donucovacímu opatření na základě oddílu 5 zákona o FTC (nebo podobného zákona)[120] . Ve druhé alternativě bude komise informovat DoC, který bude odmítnutí organizace vyhovět doporučení komise pro ochranu údajů považovat za trvalé nedodržování předpisů, které povede k vyřazení organizace ze seznamu DPF.

(75) Pokud orgán pro ochranu údajů, jemuž byla stížnost adresována, nepřijal žádná opatření k vyřízení stížnosti nebo je přijal nedostatečně, má stěžovatel možnost napadnout taková (ne)opatření u vnitrostátních soudů příslušného členského státu EU.

(76) Jednotlivci mohou podávat stížnosti orgánům pro ochranu údajů i v případě, že panel pro ochranu údajů nebyl určen jako orgán pro řešení sporů organizace. V těchto případech může orgán pro ochranu údajů tyto stížnosti postoupit buď DoC, nebo FTC. S cílem usnadnit a rozšířit spolupráci v záležitostech týkajících se individuálních stížností a nedodržování zásad organizacemi DPF EU a USA zřídí DoC zvláštní kontaktní místo, které bude působit jako styčný bod a bude nápomocno při dotazech DPA týkajících se dodržování zásad ze strany organizace[121] . Podobně se FTC zavázala zřídit specializované kontaktní místo[122] .

(77) Za čtvrté, **DoC** se zavázala přijímat, přezkoumávat a vyvíjet maximální úsilí při řešení stížností na nedodržování zásad ze strany organizace[123] . Za tímto účelem DoC stanoví zvláštní postupy pro orgány odpovědné za ochranu údajů, které stížnosti předávají vyhrazenému kontaktnímu místu, sledují je a navazují s organizacemi, aby usnadnily jejich řešení[124] . V zájmu urychlení vyřizování jednotlivých stížností je kontaktní místo ve spojení přímo s příslušným orgánem pro ochranu údajů v otázkách dodržování zásad a zejména jej informuje o stavu stížností ve lhůtě nejvýše 90 dnů od postoupení[125] . To umožňuje subjektům údajů podávat stížnosti na nesoulad s právními předpisy

117 Příloha III (viz oddíl "Usnadnění spolupráce s orgány pro ochranu údajů") a příloha IV (viz oddíly "Prioritizace postoupení a vyšetřování" a "Spolupráce při prosazování práva s orgány pro ochranu údajů v EU").

118 Jednací řád neformálního panelu orgánů pro ochranu údajů by měly stanovit orgány pro ochranu údajů na základě své kompetence organizovat svou práci a vzájemně spolupracovat.

119 Příloha I, oddíl III.5.c.(i).

120 Příloha I, oddíl III.5.c.(ii).

121 Viz příloha III, oddíl "Usnadnění spolupráce s orgány pro ochranu údajů".

122 Viz příloha IV, oddíly "Prioritizace postoupení a vyšetřování" a "Spolupráce při prosazování práva s orgány EU pro ochranu údajů".

123 Příloha III, viz např. oddíl "Usnadnění spolupráce s orgány pro ochranu údajů".

124 Příloha I oddíl II.7.e a příloha III oddíl "Usnadnění spolupráce s orgány pro ochranu údajů".

125 *Tamtéž.*

organizacemi EU a USA v rámci DPF přímo jejich národním orgánům pro ochranu údajů a nechat je předat DoC jako americkému orgánu spravujícímu DPF EU a USA.

(78) Pokud DoC na základě ověření z moci úřední, stížností nebo jiných informací dospěje k závěru, že organizace trvale nedodržuje zásady, může takovou organizaci vyškrtnout ze seznamu DPF[126] . Odmítnutí vyhovět konečnému rozhodnutí jakéhokoli samoregulačního orgánu pro ochranu soukromí, nezávislého orgánu pro řešení sporů nebo vládního orgánu, včetně orgánu pro ochranu údajů, bude považováno za trvalé nedodržování[127] .

(79) Za páté, organizace DPF mezi EU a USA musí podléhat jurisdikci amerických orgánů, zejména **FTC**[128] , které mají nezbytné vyšetřovací a donucovací pravomoci k účinnému zajištění dodržování zásad. FTC přednostně posuzuje oznámení o nedodržování Zásad, která obdrží od nezávislých orgánů pro řešení sporů nebo samoregulačních orgánů, DoC a DPA (jednajících z vlastního podnětu nebo na základě stížností), aby určila, zda byl porušen § 5 zákona o FTC[129] . FTC se zavázala vytvořit standardizovaný postup postoupení, určit v agentuře kontaktní místo pro postoupení DPA a vyměňovat si informace o postoupeních. Kromě toho může přijímat stížnosti přímo od jednotlivců a provádět šetření DPF EU a USA z vlastní iniciativy, zejména v rámci širšího šetření otázek ochrany soukromí.

(80) Za šesté, jako "poslední možnost" v případě, že žádná z ostatních dostupných možností nápravy uspokojivě nevyřešila stížnost jednotlivce, může subjekt údajů v Unii využít **závazného rozhodčího řízení**, **které** vede "Rámcový panel pro ochranu soukromí EU a USA" (Panel DPF EU a USA)[130] . Organizace musí jednotlivce informovat o možnosti dovolávat se závazného rozhodčího řízení a jsou povinny reagovat, jakmile jednotlivec tuto možnost využije, a to doručením oznámení dotčené organizaci[131] .

(81) Tento rozhodčí senát pro ochranu údajů mezi EU a USA se skládá z nejméně deseti rozhodců, které určí DoC a Komise na základě jejich nezávislosti, bezúhonnosti a zkušeností s právem USA v oblasti ochrany soukromí a ochrany údajů v Unii. Pro každý jednotlivý spor vyberou strany z této skupiny jednoho nebo tři rozhodce[132] .

(82) Ministerstvo spravedlnosti vybralo Mezinárodní centrum pro řešení sporů (ICDR), mezinárodní divizi Americké arbitrážní asociace (AAA), aby spravovala rozhodčí řízení. Řízení před rozhodčím tribunálem DPF EU a USA se bude řídit souborem dohodnutých rozhodčích pravidel a kodexem chování jmenovaných rozhodců. Webové stránky ICDR- AAA poskytují jednotlivcům jasné a stručné informace o rozhodčím mechanismu a postupu podání rozhodčí žaloby.

(83) Pravidla rozhodčího řízení dohodnutá mezi DoC a Komisí doplňují DPF mezi EU a USA, který obsahuje několik prvků, jež zlepšují přístupnost tohoto rozhodčího řízení.

---

126 Příloha I oddíl III.11.g.

127 Příloha I oddíl III.11.g.

128 Organizace DPF EU a USA musí veřejně prohlásit svůj závazek dodržovat zásady, zveřejnit své zásady ochrany osobních údajů v souladu s těmito zásadami a plně je uplatňovat. Nedodržení těchto zásad je vymahatelné podle oddílu 5 zákona FTC, který zakazuje nekalé a klamavé jednání v obchodě nebo při ovlivňování obchodu.

129 Viz také podobné závazky přijaté ministerstvem dopravy, příloha V.

130 Viz příloha I, příloha I "Vzor rozhodčího řízení".

131 Viz příloha I, oddíl II.1.a.(xi) a II.7.c.

132 Počet rozhodců v rozhodčím senátu musí být dohodnut mezi stranami.

mechanismus pro subjekty údajů v Unii: (i) při přípravě žaloby před rozhodčím senátem může subjektu údajů pomáhat jeho vnitrostátní orgán pro ochranu údajů; ii) rozhodčí řízení se bude konat ve Spojených státech, ale subjekty údajů z Unie se mohou rozhodnout, že se ho zúčastní prostřednictvím videokonference nebo telefonické konference, která bude pro danou osobu bezplatná; (iii) ačkoli jazykem používaným v rozhodčím řízení bude zpravidla angličtina, tlumočení na rozhodčím jednání a překlad budou v zásadě poskytovány na základě odůvodněné žádosti a bez nákladů pro subjekt údajů; iv) konečně, ačkoli každá strana musí nést své vlastní náklady na právní zastoupení, pokud je před rozhodčím senátem zastoupena advokátem, bude DoC udržovat fond, do něhož budou každoročně přispívat EU a USA.USA, které mají pokrýt náklady rozhodčího řízení až do maximální výše, kterou určí orgány USA po konzultaci s Komisí[133] .

(84) Komise pro DPF EU a USA je oprávněna uložit individuální nepeněžní spravedlivou úlevu[134] , která je nezbytná k nápravě nedodržení zásad. Ačkoli panel při svém rozhodování bere v úvahu další nápravná opatření, která již byla získána prostřednictvím jiných mechanismů DPF EU a USA, jednotlivci se stále mohou obrátit na rozhodčí řízení, pokud považují tato jiná nápravná opatření za nedostatečná. To umožňuje subjektům údajů v Unii dovolávat se rozhodčího řízení ve všech případech, kdy opatření nebo nečinnost organizací DPF EU a USA, nezávislých mechanismů pro odvolání nebo příslušných orgánů USA (například FTC) uspokojivě nevyřešily jejich stížnosti. Rozhodčího řízení se nelze dovolávat, pokud má orgán pro ochranu údajů zákonnou pravomoc řešit spornou stížnost ve vztahu k organizaci DPF EU-U.S., a to v případech, kdy je organizace buď povinna spolupracovat a dodržovat doporučení orgánů pro ochranu údajů, pokud jde o zpracování údajů o lidských zdrojích shromážděných v souvislosti se zaměstnáním, nebo se k tomu dobrovolně zavázala. Jednotlivci mohou vymáhat rozhodnutí rozhodčího soudu v rámci amerických soudů podle federálního zákona o arbitráži, čímž je zajištěn právní prostředek nápravy v případě, že organizace nedodrží zákon.

(85) Za sedmé, pokud organizace nedodrží svůj závazek dodržovat zásady a zveřejněnou politiku ochrany soukromí, jsou podle amerického práva k dispozici **další možnosti soudní nápravy,** včetně získání náhrady škody. Například jednotlivci mohou za určitých podmínek dosáhnout soudní nápravy (včetně náhrady škody) podle státních spotřebitelských zákonů v případech podvodného zkreslení, nekalého nebo klamavého jednání nebo praktik[135] , a podle deliktního práva (zejména podle deliktů narušení soukromí[136] , přivlastnění jména nebo podobizny[137] a zveřejnění soukromých skutečností[138]).

---

133 Příloha I oddílu G.6.

134 Jednotlivci nemohou v rozhodčím řízení uplatňovat nárok na náhradu škody, ale odvolání se na rozhodčí řízení neznamená, že by byla vyloučena možnost domáhat se náhrady škody u běžných soudů v USA.

135 Viz např. státní zákony na ochranu spotřebitele v Kalifornii (Cal. Civ. Code §§ 1750 - 1785 (West) Consumers Legal Remedies Act); District of Columbia (D.C. Code §§ 28-3901); Florida (Fla. Stat. §§ 501.201 - 501.213, Deceptive and Unfair Trade Practices Act); Illinois (815 Ill. Comp. Stat. 505/1 - 505/12, Consumer Fraud and Deceptive Business Practices Act); Pensylvánie (73 Pa. Stat. Ann. §§ 201-1 - 201-9.3 (West) Unfair Trade Practices and Consumer Protection Law).

136 Tj. v případě úmyslného zásahu do soukromých záležitostí nebo zájmů jednotlivce způsobem, který by byl pro rozumnou osobu vysoce urážlivý (Restatement (2nd) of Torts, § 652(b)).

137 Tento delikt se běžně uplatňuje v případě přivlastnění a použití jména nebo podobizny fyzické osoby k propagaci podniku nebo výrobku nebo k podobnému komerčnímu účelu (viz Restatement (2nd) of Torts, § 652C).

138 Tj. když jsou zveřejněny informace týkající se soukromého života jednotlivce, pokud je to pro rozumnou osobu vysoce urážlivé a informace nejsou legitimním zájmem veřejnosti (Restatement (2nd)

of Torts, § 652D).

3. PŘÍSTUP K OSOBNÍM ÚDAJŮM PŘEDÁVANÝM Z EVROPSKÉ UNIE A JEJICH POUŽÍVÁNÍ ORGÁNY VEŘEJNÉ MOCI VE SPOJENÝCH STÁTECH AMERICKÝCH

(86) Komise rovněž posoudila omezení a záruky, včetně mechanismů dohledu a individuální nápravy, které jsou k dispozici v právu Spojených států, pokud jde o shromažďování a následné využívání osobních údajů předávaných správcům a zpracovatelům v USA orgány veřejné moci ve veřejném zájmu, zejména pro účely vymáhání trestního práva a národní bezpečnosti (přístup vlády)[139] . Při posuzování toho, zda podmínky, za nichž vláda přistupuje k údajům předávaným do Spojených států podle tohoto rozhodnutí, splňují test "zásadní rovnocennosti" podle čl. 45 odst. 1 nařízení (EU) 2016/679, jak jej vykládá Soudní dvůr s ohledem na Listinu základních práv, vzala Komise v úvahu několik kritérií.

(87) Každé omezení práva na ochranu osobních údajů musí být zejména stanoveno zákonem a právní základ, který umožňuje zásah do takového práva, musí sám vymezovat rozsah omezení výkonu dotčeného práva[140] . Kromě toho, aby byl splněn požadavek proporcionality, podle něhož se odchylky a omezení ochrany osobních údajů musí uplatňovat pouze v míře, která je v demokratické společnosti nezbytně nutná k dosažení konkrétních cílů obecného zájmu rovnocenných cílům uznaným Unií, musí tento právní základ stanovit jasná a přesná pravidla upravující rozsah a uplatňování dotyčných opatření a stanovit minimální záruky, aby osoby, jejichž údaje byly předány, měly dostatečné záruky účinné ochrany svých osobních údajů před rizikem zneužití[141] . Tato pravidla a záruky musí být navíc právně závazné a vymahatelné pro fyzické osoby[142] . Subjekty údajů musí mít zejména možnost podat žalobu k nezávislému a nestrannému soudu, aby získaly přístup ke svým osobním údajům nebo aby dosáhly opravy či výmazu těchto údajů[143] .

3.1 Přístup a použití orgány veřejné moci USA pro účely vymáhání trestního práva.

(88) Pokud jde o zásahy do osobních údajů předávaných v rámci DPF mezi EU a USA pro účely vymáhání trestního práva, ukládá právo Spojených států řadu omezení přístupu k osobním údajům a jejich používání a stanoví mechanismy dohledu a nápravy, které jsou v souladu s požadavky uvedenými v 87. bodě odůvodnění tohoto rozhodnutí. Podmínky, za nichž lze k takovému přístupu přistupovat, a záruky použitelné na využívání těchto pravomocí jsou podrobně posouzeny v následujících oddílech. V tomto ohledu vláda Spojených států (prostřednictvím ministerstva spravedlnosti, DoJ) také

139 To je důležité i s ohledem na oddíl I.5 přílohy I.

140 Viz *Schrems II*, body 174-175 a citovaná judikatura. Pokud jde o přístup orgánů veřejné moci členských států, viz také rozsudek *Privacy International,* C-623/17, ECLI:EU:C:2020:790, bod 65, a rozsudek *La Quadrature du Net a další,* C-511/18, C-512/18 a C-520/18, ECLI:EU:C:2020:791, bod 175.

141 Viz *Schrems II*, body 176 a 181, jakož i citovaná judikatura. Pokud jde o přístup orgánů veřejné moci členských států, viz také rozsudek *Privacy International*, bod 68, a rozsudek *La Quadrature du Net a další*, bod 132.

142 Viz Schrems II, body 181-182.

143 Viz *Schrems I*, bod 95 a *Schrems II*, bod 194. V tomto ohledu SDEU zejména zdůraznil, že soulad s článkem 47 Listiny základních práv, který zaručuje právo na účinný opravný prostředek před nezávislým a nestranným soudem, "přispívá k požadované úrovni ochrany v Evropské unii [a] musí být stanoven Komisí před přijetím rozhodnutí o přiměřenosti podle čl. 45 odst. 1 nařízení (EU) 2016/679" (*Schrems II*, bod 186).

poskytla ujištění o platných omezeních a zárukách (příloha VI tohoto rozhodnutí).

3.1.1 Právní základy, omezení a záruky

3.1.1.1 Omezení a záruky, pokud jde o shromažďování osobních údajů pro účely vymáhání trestního práva

(89) K osobním údajům zpracovávaným certifikovanými organizacemi USA, které by byly předávány z Unie na základě DPF mezi EU a USA, mohou mít přístup pro účely vymáhání trestního práva federální státní zástupci a federální vyšetřovací agenti USA na základě různých postupů, jak je podrobněji vysvětleno v 90.-95. bodě odůvodnění. Tyto postupy se použijí stejným způsobem, pokud jsou informace získávány od jakékoli organizace USA, bez ohledu na státní příslušnost nebo místo pobytu dotčených subjektů údajů[144] . Podle prohlášení vlády USA se stejná nebo vyšší ochrana vztahuje na vyšetřování orgánů činných v trestním řízení na úrovni státu (s ohledem na vyšetřování prováděná podle státních zákonů)[145] .

(90) Za prvé, na žádost federálního policisty nebo vládního zmocněnce může soudce vydat příkaz k prohlídce nebo zabavení (včetně elektronicky uložených informací)[146] . Takový příkaz může být vydán pouze tehdy, pokud existuje "pravděpodobný důvod[147] ", že na místě uvedeném v příkazu budou pravděpodobně nalezeny "zabavitelné věci" (důkazy o trestném činu, nezákonně držené věci nebo majetek určený nebo určený k použití nebo použitý při spáchání trestného činu). V příkazu musí být identifikován majetek nebo předmět, který má být zajištěn, a určen soudce, kterému musí být příkaz vrácen. Osoba, která je předmětem prohlídky nebo jejíž majetek je předmětem prohlídky, může navrhnout, aby byly vyloučeny důkazy získané nebo získané z nezákonné prohlídky, pokud jsou tyto důkazy předloženy proti této osobě během trestního řízení[148] . Pokud je držitel údajů (např. společnost) povinen zpřístupnit údaje na základě příkazu, může zejména napadnout požadavek na zpřístupnění jako nepřiměřeně zatěžující[149] .

(91) Za druhé, předvolání může vydat velká porota (vyšetřovací orgán soudu jmenovaný soudcem nebo soudcem) v souvislosti s vyšetřováním určitých závažných případů.

---

144 Viz příloha VI. Viz např. v souvislosti se zákonem o odposlechu, zákonem o uchovávaných komunikacích a zákonem o elektronickém registru (podrobněji zmíněno v bodech odůvodnění 92-95), *Suzlon Energy Ltd v. Microsoft Corp., 671 F.3d 726, 729* (9th Cir. 2011).

145 Příloha VI, poznámka pod čarou 2. Zejména ochrana podle státního práva musí být přinejmenším stejná jako ochrana podle zákona o ochraně osobních údajů.
Ústava USA.

146 Federální pravidla trestního řízení, 41. V rozsudku z roku 2018 Nejvyšší soud potvrdil, že příkaz k prohlídce nebo výjimka z příkazu k prohlídce je nutná i pro přístup orgánů činných v trestním řízení k historickým záznamům o poloze mobilních sítí, které poskytují komplexní přehled o pohybu uživatele, a že uživatel může mít ve vztahu k těmto informacím přiměřené očekávání soukromí (*Timothy Ivory Carpenter v. Spojené státy americké,* č. 16-402, 585 U.S. (2018)). V důsledku toho nelze takové údaje obecně získat od mobilní společnosti na základě soudního příkazu na základě důvodného podezření, že informace jsou relevantní a podstatné pro probíhající trestní vyšetřování, ale vyžaduje prokázání existence pravděpodobného důvodu při použití soudního příkazu.

147 Podle Nejvyššího soudu je "pravděpodobný důvod" "praktickým, netechnickým" standardem, který se opírá o "faktické a praktické úvahy každodenního života, na jejichž základě jednají rozumní a obezřetní lidé [...]" (*Illinois v. Gates*, 462 U.S. 213, 232 (1983)). Pokud jde o příkazy k prohlídce, pravděpodobný důvod existuje, pokud existuje přiměřená pravděpodobnost, že prohlídka povede k nalezení důkazů o trestném činu (id).

148 *Mapp v. Ohio*, 367 U.S. 643 (1961).

149 Viz *In re Application of United States*, 610 F.2d 1148, 1157 (3. obvod 1979) (rozhodl, že "řádný proces vyžaduje slyšení v otázce zatížení před tím, než donutí telefonní společnost poskytnout" pomoc s příkazem k prohlídce) a *In re Application of United States*, 616 F.2d 1122 (9. obvod 1980).

trestných činů[150] , obvykle na žádost federálního státního zástupce, aby od někoho požadoval předložení nebo zpřístupnění obchodních záznamů, elektronicky uložených informací nebo jiných hmotných věcí. Kromě toho různé zákony povolují používat správní předvolání k předložení nebo zpřístupnění obchodních záznamů, elektronicky uložených informací nebo jiných hmotných věcí při vyšetřováních týkajících se podvodů ve zdravotnictví, zneužívání dětí, ochrany tajných služeb, případů kontrolovaných látek a vyšetřování generálního inspektora[151] . V obou případech musí být informace relevantní pro vyšetřování a předvolání nesmí být nepřiměřené, tj. nepřiměřeně široké, neúnosné nebo zatěžující (a příjemce předvolání je může z těchto důvodů napadnout)[152] .

(92) Za třetí, přístup ke komunikačním údajům umožňuje orgánům činným v trestním řízení několik právních základů. Soud může vydat příkaz, kterým povolí shromažďování informací o vytáčení, směrování, adresování a signalizaci telefonního čísla nebo e-mailu v reálném čase, které nejsou obsahem (pomocí záznamníku nebo sledovacího zařízení), pokud zjistí, že orgán osvědčil, že informace, které budou pravděpodobně získány, jsou důležité pro probíhající trestní vyšetřování[153] . V příkazu musí být mimo jiné uvedena totožnost podezřelého, je-li známa, atributy komunikace, na kterou se příkaz vztahuje, a prohlášení o trestném činu, k němuž se shromažďované informace vztahují. Použití záznamníku nebo sledovacího zařízení může být povoleno maximálně na dobu šedesáti dnů, kterou lze prodloužit pouze novým soudním příkazem.

(93) Kromě toho lze pro účely vymáhání trestního práva získat přístup k informacím o účastnících, provozním údajům a uloženému obsahu komunikací, které mají poskytovatelé internetových služeb, telefonní společnosti a další poskytovatelé služeb třetích stran, na základě zákona o uložených komunikacích[154] . K získání uloženého obsahu elektronických komunikací musí orgány činné v trestním řízení v zásadě získat soudní příkaz na základě pravděpodobného důvodu domnívat se, že daný účet obsahuje důkazy o trestném činu[155] . V případě registračních informací o účastnících, IP adres a souvisejících časových razítek a fakturačních informací mohou orgány činné v trestním řízení použít soudní obsílku. Pro většinu ostatních uložených informací, které nejsou obsahem, jako jsou hlavičky e-mailů bez předmětu, musí orgán činný v trestním řízení získat soudní příkaz, který bude vydán, pokud se soudce přesvědčí, že existují oprávněné důvody domnívat se, že požadované informace jsou relevantní a podstatné pro probíhající trestní vyšetřování.

---

[150] Pátý dodatek Ústavy USA vyžaduje obžalobu velkou porotou pro jakýkoli "hrdelní nebo jinak neblaze proslulý zločin". Grantová porota se skládá z 16 až 23 členů a rozhoduje o tom, zda existuje pravděpodobný důvod domnívat se, že byl spáchán trestný čin. K dosažení tohoto závěru jsou velké porotě svěřeny vyšetřovací pravomoci, které jí umožňují vydávat soudní obsílky.

[151] Viz příloha VI.

[152] Federální pravidla trestního řízení, 17.

[153] 18 U.S.C. §3123.

[154] 18 U.S.C. §§ 2701-2713.

[155] 18 U.S.C. §§ 2701(a)-(b)(1)(A). Pokud je dotčený účastník nebo zákazník informován (buď předem, nebo za určitých okolností prostřednictvím opožděného oznámení), lze informace o obsahu uchovávané déle než 180 dní získat také na základě správního předvolání nebo předvolání před velkou porotu (18 U.S.C. §§ 2701(b)(1)(B)) nebo soudního příkazu (pokud existují oprávněné důvody se domnívat, že informace jsou relevantní a podstatné pro probíhající trestní vyšetřování (18 U.S.C. §§ 2701(d)). V souladu s rozhodnutím federálního odvolacího soudu však vládní vyšetřovatelé zpravidla získávají povolení k prohlídce od soudců, aby mohli shromáždit obsah soukromé komunikace nebo uložené údaje od poskytovatele komerčních komunikačních služeb. *Spojené státy v. Warshak,* 631 F.3d 266 (6th Cir. 2010).

(94) Poskytovatelé, kteří obdrží žádosti podle zákona o uložených komunikacích, mohou dobrovolně informovat zákazníka nebo účastníka, jehož informace jsou požadovány, s výjimkou případů, kdy příslušný orgán činný v trestním řízení získá ochranný příkaz zakazující takové oznámení[156] . Takový ochranný příkaz je soudní příkaz, který vyžaduje, aby poskytovatel služeb elektronických komunikací nebo služeb dálkové výpočetní techniky, jemuž je určen příkaz, předvolání nebo soudní příkaz, neoznamoval existenci příkazu, předvolání nebo soudního příkazu žádné jiné osobě, a to po dobu, kterou soud považuje za vhodnou. Ochranné příkazy se vydávají, pokud soud zjistí, že existuje důvod se domnívat, že by oznámení vážně ohrozilo vyšetřování nebo nepřiměřeně zdrželo soudní řízení, např. proto, že by vedlo k ohrožení života nebo fyzické bezpečnosti osoby, útěku před trestním stíháním, zastrašování potenciálních svědků atd. Memorandum náměstka generálního prokurátora (které je závazné pro všechny státní zástupce a agenty ministerstva spravedlnosti) vyžaduje, aby státní zástupci podrobně rozhodli o potřebě ochranného příkazu a předložili soudu odůvodnění, jak jsou v konkrétním případě splněna zákonná kritéria pro získání ochranného příkazu[157] . Memorandum rovněž vyžaduje, aby žádosti o vydání ochranného příkazu obecně nesměly směřovat k odložení oznámení o více než jeden rok. Pokud by za výjimečných okolností mohly být nezbytné příkazy na delší dobu, lze o ně žádat pouze s písemným souhlasem nadřízeného orgánu určeného státním zástupcem nebo příslušným náměstkem generálního státního zástupce. Kromě toho musí státní zástupce při ukončení vyšetřování neprodleně posoudit, zda existuje důvod pro zachování jakýchkoli nevyřízených ochranných příkazů, a pokud tomu tak není, ukončit platnost ochranného příkazu a zajistit, aby o tom byl poskytovatel služeb informován[158] .

(95) Orgány činné v trestním řízení mohou rovněž v reálném čase zachycovat odposlech, ústní nebo elektronickou komunikaci na základě soudního příkazu, v němž soudce mimo jiné konstatuje, že existuje pravděpodobný důvod se domnívat, že odposlech nebo elektronický odposlech přinese důkazy o federálním trestném činu nebo o místě pobytu uprchlíka, který se skrývá před trestním stíháním[159] .

(96) Další ochranu poskytují různé politiky a pokyny ministerstva spravedlnosti, včetně pokynů generálního prokurátora pro vnitrostátní operace FBI (AGG-DOM), které mimo jiné vyžadují, aby FBI používala co nejméně rušivé vyšetřovací metody s ohledem na dopad na soukromí a občanské svobody[160] .

---

156 18 U.S.C. § 2705(b).

157 Viz memorandum vydané náměstkem generálního prokurátora Rodem Rosensteinem dne 19. října 2017 o přísnější politice týkající se žádostí o ochranné příkazy (nebo příkazy k nezveřejnění informací), které je k dispozici na adrese https://www.justice.gov/criminal-ccips/page/file/1005791/download.

158 Memorandum vydané náměstkyní generálního prokurátora Lisou Moncao dne 27. května 2022 o doplňující politice týkající se žádostí o ochranné příkazy podle § 2705 písm. b) zákona o soudní ochraně (18 U.S.C.).

159 18 U.S.C. §§ 2510-2522.

160 Pokyny generálního prokurátora pro vnitrostátní operace Federálního úřadu pro vyšetřování (FBI) (září 2008), dostupné na http://www.justice.gov/archive/opa/docs/guidelines.pdf. Další pravidla a zásady, které stanoví omezení vyšetřovacích činností federálních státních zástupců, jsou uvedeny v Příručce pro státní zástupce Spojených států (United States Attorneys' Manual, USAM), která je k dispozici na adrese http://www.justice.gov/usam/united-states- attorneys-manual. K odchýlení se od těchto pokynů je třeba získat předchozí souhlas ředitele FBI, zástupce ředitele nebo výkonného zástupce ředitele určeného ředitelem, ledaže takový souhlas nelze získat z důvodu bezprostředního nebo závažného ohrožení bezpečnosti osob nebo majetku nebo národní bezpečnosti (v takovém případě je třeba co nejdříve informovat ředitele nebo jinou pověřenou osobu). V případě nedodržení pokynů musí FBI o této skutečnosti informovat ministerstvo spravedlnosti, které následně informuje generálního prokurátora a náměstka generálního prokurátora.

3.1.1.2 Další využití shromážděných informací

(97) Pokud jde o další využití údajů shromážděných federálními orgány činnými v trestním řízení, různé zákony, pokyny a normy ukládají zvláštní záruky.

(98) V souladu s pravomocí stanovenou Clinger-Cohenovým zákonem (P.L. 104-106, Division E) a zákonem o počítačové bezpečnosti z roku 1987 (P.L. 100-235) vydal Úřad pro řízení a rozpočet (OMB) oběžník č. A-130, aby stanovil obecné závazné pokyny, které se vztahují na všechny federální úřady (včetně orgánů činných v trestním řízení) při nakládání s informacemi umožňujícími identifikaci osob[161] . Oběžník zejména požaduje, aby všechny federální úřady "omezily vytváření, shromažďování, používání, zpracovávání, uchovávání, udržování, šíření a zveřejňování informací umožňujících identifikaci osob na ty, které jsou zákonem povolené, relevantní a přiměřeně považované za nezbytné pro řádný výkon oprávněných funkcí úřadu"[162] . Kromě toho musí federální agentury v přiměřeném rozsahu zajistit, aby informace umožňující identifikaci osob byly přesné, relevantní, včasné a úplné a omezené na minimum nezbytné pro řádný výkon funkcí agentury. Obecněji řečeno, federální agentury musí zavést komplexní program ochrany soukromí, aby zajistily soulad s platnými požadavky na ochranu soukromí, vypracovat a vyhodnocovat politiky ochrany soukromí a řídit rizika pro ochranu soukromí; udržovat postupy pro odhalování, dokumentování a hlášení incidentů týkajících se dodržování ochrany soukromí; vypracovat programy zvyšování povědomí o ochraně soukromí a školení pro zaměstnance a dodavatele; a zavést zásady a postupy, které zajistí, že zaměstnanci budou zodpovědní za dodržování požadavků a politik ochrany soukromí[163] .

(99) Kromě toho zákon o elektronické veřejné správě[164] vyžaduje, aby všechny federální úřady (včetně orgánů činných v trestním řízení) zavedly takovou ochranu bezpečnosti informací, která odpovídá riziku a rozsahu škody, jež by vznikla v důsledku neoprávněného přístupu, použití, zveřejnění, narušení, změny nebo zničení; aby měly vedoucího pracovníka pro informace, který zajistí dodržování požadavků na bezpečnost informací, a aby každoročně prováděly nezávislé hodnocení (např. generálním inspektorem, viz bod odůvodnění 105) svého programu a postupů v oblasti bezpečnosti informací[165] . Podobně zákon o federálních záznamech (Federal Records Act, FRA)[166] a doplňující předpisy[167] vyžadují, aby informace uchovávané federálními agenturami podléhaly bezpečnostním opatřením zajišťujícím fyzickou integritu informací a jejich ochranu před neoprávněným přístupem.

(100) Na základě federálních zákonných pravomocí, včetně federálního zákona o modernizaci bezpečnosti informací z roku 2014, vypracovaly OMB a Národní institut pro standardy a technologie (NIST) normy, které jsou pro federální úřady (včetně orgánů činných v trestním řízení) závazné a které dále specifikují minimální požadavky na bezpečnost informací, které musí být zavedeny, včetně kontroly přístupu, zajištění informovanosti a školení, plánování pro případ mimořádných událostí, reakce na incidenty, nástrojů pro audit a odpovědnost, zajištění integrity systému a informací,

---

161 Tj. "informace, které lze použít k rozlišení nebo vysledování identity jednotlivce, a to buď samostatně, nebo v kombinaci s jinými informacemi, které jsou spojeny nebo je lze spojit s konkrétní osobou", viz oběžník OMB č. A-130, s. 33 (definice "informací umožňujících identifikaci osob").

162 Oběžník OMB č. A-130, Řízení informací jako strategického zdroje, Dodatek II, Odpovědnosti za řízení informací umožňujících osobní identifikaci, 81 Fed. Reg. 49 689 (28. července 2016), s. 17.

163 Příloha II, § 5 písm. a) až h).

164 44 U.S.C. kapitola 36.

165 44 U.S.C. §§ 3544-3545.

166 FAC, 44 U.S.C. § 3105.
167 36 C.F.R. §§ 1228.150 a následující, 1228.228 a dodatek A.

provádění posouzení rizik v oblasti ochrany soukromí a bezpečnosti atd.[168] . Kromě toho musí všechny federální úřady (včetně orgánů činných v trestním řízení) v souladu s pokyny OMB udržovat a provádět plán pro řešení případů narušení bezpečnosti údajů, a to i pokud jde o reakci na taková narušení a posuzování rizik poškození[169] .

(101) Pokud jde o uchovávání údajů, FRA[170] vyžaduje, aby federální orgány USA (včetně orgánů činných v trestním řízení) stanovily doby uchovávání svých záznamů (po jejichž uplynutí musí být tyto záznamy zlikvidovány), které musí schválit Národní správa archivů a záznamů[171] . Délka těchto dob uchovávání je stanovena s ohledem na různé faktory, jako je typ vyšetřování, zda jsou důkazy stále relevantní pro vyšetřování atd. Pokud jde o FBI, AGG-DOM stanoví, že FBI musí mít takový plán uchovávání záznamů zaveden a udržovat systém, který může rychle vyhledat stav a podklady pro vyšetřování.

(102) Oběžník OMB č. A-130 obsahuje také určité požadavky na šíření informací umožňujících osobní identifikaci. Zejména při sdílení informací umožňujících identifikaci osob s jinými subjekty musí federální agentury USA případně stanovit podmínky (včetně zavedení konkrétních kontrol zabezpečení a ochrany soukromí), které upravují zpracování informací prostřednictvím písemných dohod (včetně smluv, dohod o používání údajů, dohod o výměně informací a memorand o porozumění)[172] . Pokud jde o důvody, na jejichž základě mohou být informace šířeny, AGG-DOM například stanoví, že FBI může informace šířit např. jiným agenturám USA, pokud souvisejí s jejich povinnostmi; zahraničním agenturám, pokud informace souvisejí s jejich povinnostmi a šíření je zejména nezbytné k ochraně bezpečnosti osob nebo majetku nebo k ochraně před trestným činem či ohrožením národní bezpečnosti nebo k jejich předcházení.

3.1.2 Dohled

(103) Činnost federálních orgánů činných v trestním řízení podléhá dohledu různých orgánů.

(104) Zaprvé, v rámci různých útvarů s odpovědností za prosazování trestního práva existují úředníci pro ochranu soukromí a občanských svobod[173] . Zatímco konkrétní pravomoci těchto

---

168 Viz např. oběžník OMB č. A-130; NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations (10. prosince 2020); a NIST Federal Information Processing Standards 200: Minimum Security Requirements for Federal Information and Information Systems.

169 Memorandum 17-12, "Příprava na narušení osobních údajů a reakce na ně", dostupné na adrese https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17- 12_0.pdf a v oběžníku OMB č. A-130. Například postupy pro reakci na narušení bezpečnosti údajů ministerstva spravedlnosti, *viz* https://www.justice.gov/file/4336/download.

170 FRA, 44 U.S.C. §§3101 a následující.

171 Národní správa archivů a záznamů má pravomoc posuzovat postupy správy záznamů agentur a může rozhodnout, zda je další uchovávání určitých záznamů oprávněné (44 U.S.C. §§ 2904(c), 2906).

172 Oběžník OMB č. A-130, příloha I, § 3 písm. d).

173 Viz 42 U.S.C. § 2000ee-1. Patří sem například Ministerstvo spravedlnosti, Ministerstvo vnitřní bezpečnosti a FBI. Na DHS je navíc za zachování a posílení ochrany soukromí a podporu transparentnosti v rámci ministerstva odpovědný hlavní úředník pro ochranu soukromí (6 U.S.C. 142, § 222). Všechny systémy, technologie, formuláře a programy DHS, které shromažďují osobní údaje nebo mají dopad na soukromí, podléhají dohledu hlavního úředníka pro ochranu soukromí, který má přístup ke všem záznamům, zprávám, auditům, přezkumům, dokumentům, dokumentům, doporučením a dalším materiálům, jež jsou k dispozici pro

úředníci se mohou poněkud lišit v závislosti na schvalovacím zákoně, obvykle zahrnují dohled nad postupy, které mají zajistit, aby příslušné oddělení/agentura náležitě zohledňovaly otázky soukromí a občanských svobod a zavedly odpovídající postupy pro řešení stížností osob, které se domnívají, že bylo porušeno jejich soukromí nebo občanské svobody. Vedoucí jednotlivých útvarů nebo agentur musí zajistit, aby úředníci pro ochranu soukromí a občanských svobod měli k dispozici materiály a zdroje pro plnění svých úkolů, aby měli přístup ke všem materiálům a pracovníkům nezbytným pro výkon svých funkcí a aby byli informováni o navrhovaných změnách politiky a aby s nimi byly konzultovány[174] . Úředníci pro ochranu soukromí a občanských svobod pravidelně podávají zprávy Kongresu, včetně počtu a povahy stížností, které oddělení/agentura obdržela, a shrnutí vyřízení těchto stížností, provedených přezkumů a šetření a dopadu činností, které úředník provedl[175] .

(105) Na činnost ministerstva spravedlnosti, včetně FBI, navíc dohlíží nezávislý generální inspektor[176] . Generální inspektoři jsou ze zákona nezávislí[177] a odpovídají za provádění nezávislých vyšetřování, auditů a inspekcí programů a činností ministerstva. Mají přístup ke všem záznamům, zprávám, auditům, revizím, dokumentům, spisům, doporučením nebo jiným relevantním materiálům, v případě potřeby na základě předvolání, a mohou podávat svědectví[178] . Generální inspektoři sice vydávají nezávazná doporučení k nápravným opatřením, ale jejich zprávy, včetně zpráv o následných opatřeních (nebo jejich nedostatku)[179] , jsou zpravidla zveřejňovány a zasílány Kongresu, který na jejich základě může vykonávat svou funkci dohledu (viz 106. bod odůvodnění)[180] .

(106) Činnosti v oblasti vymáhání trestního práva podléhají dohledu zvláštních výborů Kongresu USA (justiční výbory Sněmovny reprezentantů a Senátu). Na adrese

---

~~oddělení, a v případě potřeby na základě předvolání. Úředník pro ochranu soukromí musí každoročně~~ podávat Kongresu zprávu o činnostech ministerstva, které mají vliv na ochranu soukromí, včetně stížností na porušování ochrany soukromí.

174 42 U.S.C. § 2000ee-1(d).

175 Viz 42 U.S.C. §§ 2000ee-1 (f)(1)-(2). Například ze zprávy vedoucího Úřadu pro ochranu soukromí a občanských svobod ministerstva spravedlnosti a Úřadu pro ochranu soukromí a občanských svobod za období od října 2020 do března 2021 vyplývá, že bylo provedeno 389 přezkumů ochrany soukromí, včetně přezkumů informačních systémů a dalších programů (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

176 Podobně byl zákonem o vnitřní bezpečnosti z roku 2002 zřízen Úřad generálního inspektora ministerstva vnitřní bezpečnosti.

177 Generální inspektoři mají jisté funkční období a mohou být odvoláni pouze prezidentem, který musí Kongresu písemně sdělit důvody takového odvolání.

178 Viz § 6 zákona o generálním inspektorovi z roku 1978.

179 V tomto ohledu viz například přehled, který vypracoval Úřad generálního inspektora DoJ, o svých doporučeních a o tom, do jaké míry byla provedena prostřednictvím následných opatření oddělení a agentury, https://oig.justice.gov/sites/default/files/reports/22-043.pdf.

180 Viz zákon o generálním inspektorovi z roku 1978, §§ 4(5), 5. Například Úřad generálního inspektora v rámci Ministerstva spravedlnosti nedávno zveřejnil svou pololetní zprávu pro Kongres (1. října 2021 - 31. března 2022, https://oig.justice.gov/node/23596), která obsahuje přehled jeho auditů, hodnocení, inspekcí, zvláštních přezkumů a vyšetřování programů a operací ministerstva spravedlnosti. Mezi tyto činnosti patřilo i vyšetřování bývalého dodavatele týkající se nezákonného zveřejnění elektronického sledování (odposlechu osoby) v rámci probíhajícího vyšetřování, které vedlo k odsouzení dodavatele. Úřad generálního inspektora rovněž provedl šetření programů a postupů ministerstva spravedlnosti v oblasti bezpečnosti informací, které zahrnuje testování účinnosti politik, postupů a praktik v oblasti bezpečnosti informací u reprezentativní podskupiny systémů ministerstva spravedlnosti.

Soudní výbory provádějí pravidelný dohled různými způsoby, zejména prostřednictvím slyšení, vyšetřování, přezkumů a zpráv[181] .

3.1.3 Náprava

(107) Jak již bylo uvedeno, orgány činné v trestním řízení musí ve většině případů získat předchozí soudní povolení ke shromažďování osobních údajů. Ačkoli se to nevyžaduje v případě správních předvolání, jsou tato předvolání omezena na specifické situace a budou podléhat nezávislému soudnímu přezkumu přinejmenším v případech, kdy vláda usiluje o jejich vymáhání u soudu. Zejména příjemci správních předvolání je mohou napadnout u soudu z důvodu jejich nepřiměřenosti, tj. přílišného rozsahu, tísnivosti nebo zatížení[182] .

(108) Kromě toho právo USA poskytuje jednotlivcům řadu možností soudní nápravy proti orgánům veřejné moci nebo jejich úředníkům, pokud tyto orgány zpracovávají osobní údaje. Tyto prostředky, mezi něž patří zejména zákon APA, zákon o svobodě informací (FOIA) a zákon o ochraně soukromí v elektronických komunikacích (ECPA), jsou otevřeny všem jednotlivcům bez ohledu na jejich státní příslušnost, a to za splnění příslušných podmínek.

(109) Obecně platí, že podle ustanovení o soudním přezkumu podle APA[183] , "každá osoba, která utrpěla právní újmu v důsledku činnosti agentury nebo která byla činností agentury nepříznivě dotčena nebo poškozena", je oprávněna požádat o soudní přezkum[184] . To zahrnuje možnost požádat soud, aby "považoval za nezákonné a zrušil opatření agentury, zjištění a závěry, které byly shledány [...] svévolné, rozmarné, zneužití pravomoci nebo jinak nejsou v souladu se zákonem"[185] .

(110) Konkrétněji, hlava II zákona o ochraně soukromí v elektronických komunikacích (ECPA)[186] stanoví systém zákonných práv na ochranu soukromí a jako taková upravuje přístup orgánů činných v trestním řízení k obsahu odposlechů, ústních nebo elektronických sdělení uložených poskytovateli služeb třetích stran[187] . Kriminalizuje nezákonný (tj. soudem nepovolený nebo jinak přípustný) přístup k takovým komunikacím a poskytuje postiženému jednotlivci možnost podat občanskoprávní žalobu u federálního soudu USA na náhradu skutečné a sankční škody, jakož i na spravedlivou nebo deklaratorní úhradu proti vládnímu úředníkovi, který se úmyslně dopustil takového nezákonného jednání, nebo proti Spojeným státům.

(111) Rovněž podle zákona o svobodě informací (Freedom of Information Act - FOIA)[188] , 5 U.S.C. § 552 má každá osoba právo získat přístup k záznamům federálního úřadu a po vyčerpání správních opravných prostředků se tohoto práva domáhat u soudu, s výjimkou případů, kdy je takovýto

[181] Výbory například pořádají tematická slyšení (viz n a p ř . nedávné slyšení ve Sněmovně reprezentantů pro soudnictví). výboru na "digitální dragnets", https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983), stejně jako pravidelná slyšení o dohledu, např. nad FBI a DoJ, viz https://www.judiciary.senate.gov/meetings/08/04/2022/oversight- of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 a https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899.

[182] Viz příloha VI.

[183] 5 U.S.C. § 702.

[184] Obecně platí, že soudnímu přezkumu podléhá pouze "konečné" opatření agentury - nikoli "předběžné, procesní nebo mezitímní" opatření agentury. Viz 5 U.S.C. § 704.

[185] 5 U.S.C. § 706 ODST. 2 PÍSM. A).

[186] 18 U.S.C. §§ 2701-2712.

[187] ECPA chrání komunikace, které mají v držení dvě definované třídy poskytovatelů síťových služeb, a to poskytovatele: (i) služeb elektronické komunikace, například telefonování nebo e-mailu; (ii) služeb vzdálené výpočetní techniky, jako jsou služby ukládání nebo zpracování dat.

188 5 U.S.C. § 552.

záznamy jsou chráněny před zveřejněním na základě výjimky nebo zvláštní výjimky pro vymáhání práva[189] .

(112) Kromě toho několik dalších zákonů poskytuje jednotlivcům právo podat žalobu proti amerického orgánu veřejné moci nebo úředníka v souvislosti se zpracováním jejich osobních údajů, jako je zákon o odposlechu[190] , zákon o počítačových podvodech a zneužití[191] , zákon o federálních nárocích z deliktů[192] , zákon o právu na finanční soukromí[193] a zákon o spravedlivém úvěrovém zpravodajství[194] .

3.2 Přístup a použití orgány veřejné moci USA pro účely národní bezpečnosti

(113) Právní předpisy Spojených států obsahují různá omezení a záruky, pokud jde o přístup k osobním údajům a jejich používání pro účely národní bezpečnosti, a stanoví mechanismy dohledu a nápravy, které jsou v souladu s požadavky uvedenými v článku 2.

---

189 Tyto výjimky jsou však zarámovány. Například podle 5 U.S.C. § 552 písm. b) odst. 7 jsou práva FOIA vyloučena v případě "záznamů nebo informací shromážděných pro účely vymáhání práva, avšak pouze v rozsahu, v němž by předložení takových záznamů nebo informací (A) mohlo důvodně narušit řízení o vymáhání práva, (B) zbavilo osobu práva na spravedlivý proces nebo nestranné rozhodování", (C) by mohlo důvodně očekávat, že by představovalo neoprávněný zásah do soukromí, (D) by mohlo důvodně očekávat, že by odhalilo totožnost důvěrného zdroje, včetně státní, místní nebo zahraniční agentury nebo orgánu nebo jakékoli soukromé instituce, která poskytla informace na důvěrném základě, a v případě záznamu nebo informací shromážděných orgánem činným v trestním řízení v průběhu vyšetřování trestného činu nebo agenturou provádějící zákonné zpravodajské vyšetřování v oblasti národní bezpečnosti informace poskytnuté důvěrným zdrojem, E) by odhalil techniky a postupy vyšetřování nebo stíhání v oblasti prosazování práva nebo by odhalil pokyny pro vyšetřování nebo stíhání v oblasti prosazování práva, pokud by se dalo důvodně očekávat, že takové odhalení by znamenalo riziko obcházení zákona, nebo F) by mohl důvodně ohrozit život nebo fyzickou bezpečnost jakékoli osoby." Rovněž "[v] každém případě, kdy je podána žádost, která zahrnuje přístup k záznamům [jejichž předložení by mohlo důvodně očekávat narušení řízení o vymáhání práva] a - A) vyšetřování nebo řízení se týká možného porušení trestního práva; a (B) existuje důvod se domnívat, že (i) subjekt vyšetřování nebo řízení neví o jeho průběhu a (ii) lze důvodně očekávat, že zveřejnění existence záznamů by mohlo narušit řízení o vymáhání práva, může agentura pouze po dobu, kdy tato okolnost trvá, zacházet se záznamy, jako by nepodléhaly požadavkům tohoto oddílu." (5 U.S.C. § 552 c) odst. 1).

190 18 U.S.C. §§ 2510 a následující. Podle zákona o odposlechu (18 U.S.C. § 2520) může osoba, jejíž odposlech, ústní nebo elektronická komunikace byla zachycena, prozrazena nebo úmyslně použita, podat občanskoprávní žalobu pro porušení zákona o odposlechu, a to za určitých okolností i proti jednotlivým vládním úředníkům nebo Spojeným státům. Pokud jde o shromažďování informací, které nejsou obsahem (např. IP adresa, e-mailová adresa pro odeslání/odeslání), viz také kapitola Pen Registers and Trap and Trace Devices v hlavě 18 (18 U.S.C. §§ 3121-3127 a pro občanskoprávní řízení § 2707).

191 18 U.S.C. § 1030. Podle zákona o počítačových podvodech a zneužití počítačů může osoba podat žalobu proti kterékoli osobě v souvislosti s úmyslným neoprávněným přístupem (nebo překročením oprávněného přístupu) za účelem získání informací z finanční instituce, počítačového systému vlády USA nebo jiného určeného počítače, za určitých okolností i proti jednotlivému vládnímu úředníkovi.

192 28 U.S.C. §§ 2671 a následující. Podle federálního zákona o deliktních nárocích může osoba za určitých okolností podat žalobu proti Spojeným státům v souvislosti s "nedbalým nebo protiprávním jednáním nebo opomenutím jakéhokoli zaměstnance vlády při výkonu jeho funkce nebo zaměstnání".

193 12 U.S.C. §§ 3401 a následující. Podle zákona o právu na finanční soukromí může osoba za určitých okolností podat žalobu proti Spojeným státům v souvislosti se získáním nebo zveřejněním chráněných finančních záznamů v rozporu s tímto zákonem. Přístup vlády k chráněným finančním záznamům je obecně zakázán, pokud vláda nepodá žádost na základě zákonného předvolání nebo příkazu k prohlídce nebo, s výhradou omezení, formální písemné žádosti a pokud osoba, jejíž informace jsou požadovány, neobdrží oznámení o takové žádosti.

194 15 U.S.C. §§ 1681-1681x. Podle zákona Fair Credit Reporting Act může osoba podat žalobu proti kterékoli osobě, která nedodržuje požadavky (zejména nutnost zákonného oprávnění) týkající se shromažďování, šíření a používání zpráv o úvěrech spotřebitelů, nebo za určitých okolností proti vládnímu orgánu.

87. bod odůvodnění tohoto rozhodnutí. Podmínky, za nichž lze takový přístup uskutečnit, a záruky použitelné pro využití těchto pravomocí jsou podrobně posouzeny v následujících oddílech.

3.2.1 Právní základy, omezení a záruky

3.2.1.1 Platný právní rámec

(114) Osobní údaje předávané z Unie do organizací DPF EU a USA mohou být shromažďovány americkými orgány pro účely národní bezpečnosti na základě různých právních nástrojů a za zvláštních podmínek a záruk.

(115) Zpravodajské služby USA mohou žádat o přístup k osobním údajům, které byly předány organizacím nacházejícím se ve Spojených státech pro účely národní bezpečnosti, pouze na základě zákonného oprávnění, konkrétně na základě zákona o dohledu nad zahraničním zpravodajstvím (FISA) nebo zákonných ustanovení, která povolují přístup prostřednictvím dopisů národní bezpečnosti (NSL)[195] .

(116) FISA obsahuje několik právních základů, které lze použít ke shromažďování (a následnému zpracování) osobních údajů subjektů údajů Unie předávaných v rámci DPF mezi EU a USA (§ 105 FISA[196] , § 302 FISA[197] , § 402 FISA[198] , § 501 FISA[199] a § 702 FISA[200]), jak je podrobněji popsáno ve 135. až 145. bodě odůvodnění.

(117) Zpravodajské služby USA mají rovněž možnost shromažďovat osobní údaje mimo Spojené státy, což může zahrnovat osobní údaje při přepravě mezi Unií a Spojenými státy. Shromažďování údajů mimo Spojené státy se zakládá na výkonném nařízení č. 12333 (EO 12333)[201] , které vydal prezident[202] .

(118) Shromažďování zpravodajských informací o signálech je formou shromažďování zpravodajských informací, která je pro toto zjištění přiměřenosti nejrelevantnější, neboť se týká shromažďování elektronické komunikace a údajů z informačních systémů. Takové shromažďování mohou zpravodajské agentury USA provádět jak na území Spojených států (na základě zákona FISA), tak při přepravě údajů do Spojených států (na základě nařízení 12333).

(119) Dne 7. října 2022 vydal americký prezident výnos č. 14086 o posílení záruk pro signálové zpravodajství Spojených států, kterým se stanoví omezení a záruky pro ~~všechny americké~~ zpravodajské služby.

195 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; a 18 U.S.C. § 2709. Viz 146. bod odůvodnění.

196 50 U.S.C. § 1804, který se týká tradičního individualizovaného elektronického sledování.

197 50 U.S.C. § 1822, který se týká fyzických prohlídek pro účely zahraničního zpravodajství.

198 50 U.S.C. § 1842 s § 1841 odst. 2 a § 3127 hlavy 18, který se týká instalace registračních per nebo sledovacích zařízení.

199 50 U.S.C. § 1861, který umožňuje FBI předložit "žádost o vydání příkazu, kterým se běžnému dopravci, veřejnému ubytovacímu zařízení, fyzickému úložišti nebo půjčovně vozidel povoluje vydat záznamy, které má v držení, pro účely vyšetřování s cílem shromáždit zahraniční zpravodajské informace nebo vyšetřování týkající se mezinárodního terorismu".

200 50 U.S. Code § 1881a, který umožňuje složkám zpravodajské komunity USA získat přístup k informacím, včetně obsahu internetové komunikace, od amerických společností, které se zaměřují na určité neamerické osoby mimo Spojené státy, a to za zákonem vynucené pomoci poskytovatelů elektronických komunikací.

201 EO 12333: United States Intelligence Activities, Federal Register Vol. 40, No 235 (8. prosince 1981 ve znění z 30. července 2008). EO 12333 obecněji definuje cíle, směry, povinnosti a odpovědnosti zpravodajských činností USA (včetně úlohy různých složek zpravodajského společenství) a stanoví obecné parametry pro provádění zpravodajských činností.

202 Podle článku II Ústavy USA spadá zajištění národní bezpečnosti, zejména shromažďování zahraničních zpravodajských informací, do pravomoci prezidenta jako vrchního velitele ozbrojených sil.

zpravodajské činnosti v oblasti signálů. Tento EO do značné míry nahrazuje PPD-28[203] posiluje podmínky, omezení a záruky, které se vztahují na všechny činnosti signálového zpravodajství bez ohledu na to, kde se odehrávají[204] , a zavádí nový mechanismus nápravy, jehož prostřednictvím se mohou jednotlivci těchto záruk dovolávat a vymáhat je[205] (podrobněji viz 168.-186. bod odůvodnění). Tímto způsobem implementuje do práva USA výsledek jednání, která proběhla mezi EU a USA po zrušení rozhodnutí Komise o přiměřenosti štítu na ochranu soukromí Soudním dvorem (viz 6. bod odůvodnění). Jedná se proto o obzvláště důležitý prvek právního rámce posuzovaného v tomto rozhodnutí.

(120) Požadavky stanovené v tomto nařízení prezidenta jsou závazné pro celou zpravodajskou komunitu. Musí být dále prováděny prostřednictvím politik a postupů agentur, které je promítnou do konkrétních pokynů pro každodenní činnost. V tomto ohledu EO 14086 poskytuje zpravodajským agenturám USA maximálně jeden rok na aktualizaci jejich stávajících politik a postupů (tj. do 7. října 2023), aby je uvedly do souladu s požadavky EO. Tyto aktualizované politiky a postupy musí být vypracovány po konzultaci s generálním prokurátorem, úředníkem pro ochranu občanských svobod ředitele Národního zpravodajství (ODNI CLPO) a Radou pro dohled nad ochranou soukromí a občanských svobod (PCLOB) - nezávislým dohledovým orgánem oprávněným přezkoumávat politiky výkonné moci a jejich provádění s cílem chránit soukromí a občanské svobody (viz 159. bod odůvodnění, pokud jde o úlohu a postavení PCLOB) - a musí být zveřejněny[206] . Jakmile budou aktualizované politiky a postupy zavedeny, provede navíc PCLOB přezkum, aby zajistil jejich soulad s EO. Do 180 dnů od dokončení takového přezkumu ze strany PCLOB musí každá zpravodajská agentura pečlivě zvážit a provést nebo jinak řešit všechna doporučení PCLOB. Dne [XXX] vláda USA informovala Evropskou komisi, že tyto politiky a postupy byly aktualizovány.

3.2.1.2 Omezení a záruky, pokud jde o shromažďování osobních údajů pro účely národní bezpečnosti

(121) EO 14086 stanoví řadu nadměrných požadavků, které se vztahují na všechny činnosti v oblasti signálového zpravodajství (shromažďování, používání, šíření osobních údajů atd.).

(122) Zaprvé, tyto činnosti musí být založeny na zákoně nebo prezidentském povolení a prováděny v souladu s právem USA, včetně ústavy[207] .

---

203 EO 14086 nahrazuje předchozí prezidentskou směrnici, Presidential Policy Directive 28 (PPD 28), s výjimkou jejího oddílu 3 a doplňující přílohy (která vyžaduje, aby zpravodajské agentury každoročně přezkoumávaly své priority a požadavky v oblasti signálového zpravodajství s ohledem na přínosy aktivit v oblasti signálového zpravodajství pro národní zájmy USA, jakož i na rizika, která tyto aktivity představují) a oddílu 6 (který obsahuje obecná ustanovení), viz Memorandum o národní bezpečnosti týkající se Částečné zrušení . prezidenta politiky . Směrnice 28, k dispozici na adrese na adrese https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security- memorandum-on-partial-revocation-of-presidential-policy-directive-28/.

204 Viz § 5 písm. f) EO 14086, který vysvětluje, že EO má stejnou oblast působnosti jako PPD-28, který se podle poznámky pod čarou č. 3 vztahoval na činnosti signálového zpravodajství prováděné za účelem shromažďování komunikací nebo informací o komunikacích, s výjimkou činností signálového zpravodajství prováděných za účelem testování nebo rozvoje schopností signálového zpravodajství.

205 V tomto ohledu viz např. oddíl 5 písm. h) EO 14086, který objasňuje, že záruky v EO vytvářejí právní nárok a jednotlivci je mohou vymáhat prostřednictvím mechanismu nápravy.

206 Viz oddíl 2 písm. c) bod iv) písm. c) EO 14086.

207 Oddíl 2 písm. a) bod i) EO 14086.

(123) Za druhé, musí být zavedena vhodná ochranná opatření, která zajistí, aby soukromí a občanské svobody byly nedílnou součástí plánování takových činností[208] .

(124) Konkrétně lze jakoukoli činnost v oblasti signálového zpravodajství provádět pouze "po zjištění na základě přiměřeného posouzení všech relevantních faktorů, že tyto činnosti jsou nezbytné k dosažení potvrzené zpravodajské priority" (pokud jde o pojem "potvrzená zpravodajská priorita", viz 129. bod odůvodnění)[209] .

(125) Kromě toho mohou být tyto činnosti prováděny pouze "v rozsahu a způsobem, který je přiměřený potvrzené zpravodajské prioritě, pro kterou byly povoleny"[210] . Jinými slovy, musí být dosaženo náležité rovnováhy "mezi významem sledované zpravodajské priority a dopadem na soukromí a občanské svobody dotčených osob bez ohledu na jejich státní příslušnost nebo místo jejich pobytu"[211] .

(126) Aby bylo zajištěno dodržování těchto obecných požadavků, které odrážejí zásady zákonnosti, nezbytnosti a přiměřenosti, podléhají činnosti signálového zpravodajství dohledu (podrobněji viz 154.-166. bod odůvodnění)[212] .

(127) Tyto zastřešující požadavky jsou v souvislosti se shromažďováním zpravodajských informací o signálech dále odůvodněny řadou podmínek a omezení, které zajišťují, že zásahy do práv jednotlivců jsou omezeny na míru nezbytnou a přiměřenou k dosažení legitimního cíle.

(128) Zaprvé, EO omezuje důvody, na jejichž základě lze shromažďovat údaje v rámci zpravodajských činností, a to dvěma způsoby. Na jedné straně EO stanoví legitimní cíle, které lze sbíráním signálů sledovat, např. pochopení nebo posouzení schopností, záměrů nebo činností zahraničních organizací, včetně mezinárodních teroristických organizací, které představují současnou nebo potenciální hrozbu pro národní bezpečnost Spojených států; ochrana před zahraničními vojenskými schopnostmi a činnostmi; pochopení nebo posouzení nadnárodních hrozeb, které mají dopad na globální bezpečnost, jako jsou klimatické a jiné ekologické změny, rizika pro veřejné zdraví a humanitární hrozby[213] . Na druhou stranu EO uvádí určité cíle, které nesmí být nikdy sledovány prostřednictvím činností signálového zpravodajství, např. za účelem zatížení kritiky, disentu nebo svobodného vyjadřování myšlenek či politických názorů jednotlivci nebo tiskem; za účelem znevýhodnění osob na základě jejich etnického původu, rasy, pohlaví, genderové identity, sexuální orientace nebo náboženství; nebo za účelem poskytnutí konkurenční výhody americkým společnostem[214] .

---

208 Oddíl 2 písm. a) bod ii) EO 14086.

209 Oddíl 2 písm. a) bod ii) část A EO 14086. To nevyžaduje, aby signální zpravodajství bylo vždy jediným prostředkem k prosazování aspektů potvrzené zpravodajské priority. Shromažďování signálového zpravodajství lze například využít k zajištění alternativních cest k ověření (např. k potvrzení informací získaných z jiných zpravodajských zdrojů) nebo k udržení spolehlivého přístupu ke stejným informacím (oddíl 2 písm. c) bod i) část A EO 14086).

210 Oddíl 2(a)(ii)(B) EO 14086.

211 Oddíl 2(a)(ii)(B) EO 14086.

212 Oddíl 2 písm. a) bod iii) ve spojení s oddílem 2 písm. d) EO 14086.

213 Oddíl 2 písm. b) bod i) EO 14086. V případě, že se objeví nové požadavky na národní bezpečnost, například nové hrozby pro národní bezpečnost, může prezident tento seznam aktualizovat. Takové aktualizace musí být v zásadě zveřejněny, pokud prezident nerozhodne, že by to samo o sobě představovalo riziko pro národní bezpečnost Spojených států (oddíl 2 písm. b) bod i) písm. b) EO 14086).

214 Oddíl 2 písm. b) bod ii) EO 14086.

(129) Kromě toho se zpravodajské agentury nemohou opírat o legitimní cíle stanovené v EO 14086, aby ospravedlnily shromažďování signálového zpravodajství, ale musí je pro operativní účely dále zdůvodnit do konkrétnějších priorit, pro které lze signálové zpravodajství shromažďovat. Jinými slovy, skutečné shromažďování může probíhat pouze za účelem dosažení konkrétnější priority. Tyto priority se stanovují prostřednictvím zvláštního procesu, jehož cílem je zajistit soulad s platnými právními požadavky, včetně požadavků týkajících se soukromí a občanských svobod. Konkrétněji řečeno, zpravodajské priority nejprve vypracovává ředitel národního zpravodajství (prostřednictvím tzv. rámce národních zpravodajských priorit) a předkládá je prezidentovi ke schválení[215] . Předtím, než ředitel navrhne prezidentovi zpravodajské priority, musí v souladu s EO 14086 získat pro každou prioritu posouzení od pracovníka ředitele Národního zpravodajství pro ochranu občanských svobod (ODNI CLPO), zda 1) podporuje jeden nebo více legitimních cílů uvedených v EO; (2) nebyla navržena a ani se nepředpokládá, že by vedla ke sběru signálů pro zakázané cíle uvedené v EO; a (3) byla stanovena po náležitém zvážení ochrany soukromí a občanských svobod všech osob bez ohledu na jejich státní příslušnost nebo místo jejich případného pobytu[216] . V případě, že ředitel nesouhlasí s posouzením CLPO, musí být obě stanoviska předložena prezidentovi[217] .

(130) Tento proces proto zejména zajišťuje, aby se hledisko ochrany soukromí zohledňovalo již v počáteční fázi, kdy se stanovují zpravodajské priority.

(131) Za druhé, jakmile je stanovena zpravodajská priorita, rozhoduje se o tom, zda a v jakém rozsahu lze pro její prosazení shromažďovat signální zpravodajské informace, podle řady požadavků. Tyto požadavky operacionalizují zastřešující standardy nezbytnosti a přiměřenosti stanovené v oddíle 2 písm. a) EO.

(132) Zejména lze shromažďovat zpravodajské informace o signálech pouze "po zjištění, že na základě přiměřeného posouzení všech relevantních faktorů je shromažďování nezbytné k dosažení konkrétní zpravodajské priority"[218] . Při určování, zda je konkrétní činnost sběru signálů nezbytná k dosažení schválené zpravodajské priority, musí zpravodajské agentury USA zvážit dostupnost, proveditelnost a vhodnost jiných, méně invazivních zdrojů a metod, včetně zdrojů diplomatických a veřejných[219] . Pokud jsou tyto alternativní, méně rušivé zdroje a metody k dispozici, musí být upřednostněny[220] .

(133) Pokud je při uplatňování těchto kritérií shromažďování zpravodajských informací o signálech považováno za nezbytné, musí být "co nejvíce přizpůsobeno" a nesmí "nepřiměřeně ovlivňovat soukromí a občanské svobody"[221] . Aby se zajistilo, že soukromí a občanské svobody nebudou nepřiměřeně dotčeny - tj. aby se dosáhlo náležité rovnováhy mezi potřebami národní bezpečnosti a ochranou soukromí a občanských svobod -, je třeba, aby se všechny

---

215 Článek 102A zákona o národní bezpečnosti a čl. 2 písm. b) bod iii) EO 14086.

216 Ve výjimečných případech (zejména pokud takový postup nelze provést z důvodu potřeby řešit nový nebo vyvíjející se zpravodajský požadavek) může tyto priority stanovit přímo prezident nebo vedoucí složky zpravodajské komunity, kteří musí v zásadě použít stejná kritéria, jaká jsou popsána v oddíle 2 písm. b) bodě iii) části A odst. 1 až 3, viz oddíl 4 písm. n) EO 14086.

217 Oddíl 2 písm. b) bod iii) písm. c) EO 14086.

218 Oddíl 2 písm. b) a písm. c) bod i) písm. a) EO 14086.

219 Oddíl 2 písm. c) bod i) písm. A) EO 14086.

220 Oddíl 2 písm. c) bod i) písm. A) EO 14086.

221 Oddíl 2 písm. c) bod i) písm. b) EO 14086.

je třeba náležitě zohlednit příslušné faktory, jako je povaha sledovaného cíle, intenzita sběru, včetně doby jeho trvání, pravděpodobný přínos sběru ke sledovanému cíli, rozumně předvídatelné důsledky pro jednotlivce a povaha a citlivost shromažďovaných údajů[222] .

(134) Pokud jde o druh shromažďování údajů pro účely signálového zpravodajství, shromažďování údajů v rámci Spojených států, které je pro toto zjištění přiměřenosti nejrelevantnější, neboť se týká údajů, které byly předány organizacím v USA, musí být vždy cílené, jak je podrobněji vysvětleno ve 135.-146. bodě odůvodnění. "Hromadné shromažďování"[223] se může vztahovat pouze na shromažďování údajů, které probíhá mimo území Spojených států, a to na základě příkazu EO 12333. Také v tomto případě musí být na základě EO 14086 cílený sběr prioritní[224] . Naopak hromadné shromažďování je povoleno pouze v případě, že informace nezbytné k prosazení potvrzené zpravodajské priority nelze rozumně získat cíleným shromažďováním[225] . Pokud je nutné provádět hromadný sběr údajů mimo území Spojených států, platí zvláštní ochranná opatření podle EO 14086[226] . Zaprvé musí být použity metody a technická opatření, aby se shromážděné údaje omezily pouze na ty, které jsou nezbytné k dosažení potvrzené zpravodajské priority, a zároveň se minimalizovalo shromažďování nerelevantních informací[227] . Za druhé, EO omezuje použití hromadně shromažďovaných informací (včetně dotazování) na šest konkrétních cílů, včetně ochrany před terorismem, braním rukojmí a držením osob v zajetí cizí vládou, organizací nebo osobou nebo jejich jménem; ochrany před zahraniční špionáží, sabotáží nebo atentátem; ochrany před hrozbami vyplývajícími z vývoje, držení nebo šíření zbraní hromadného ničení nebo souvisejících technologií a hrozeb atd.[228] A konečně, jakékoliv hromadné dotazování na zpravodajské informace o signálech může probíhat pouze v případě, že je to nezbytné k dosažení potvrzené zpravodajské priority, při sledování těchto šesti cílů a v souladu s politikami a postupy, které vhodně

222 Oddíl 2 písm. c) bod i) písm. b) EO 14086.

223 Tj. sběr velkého množství zpravodajských signálů, které jsou z technických nebo operativních důvodů získávány bez použití diskriminantů (například bez použití specifických identifikátorů nebo selekčních termínů), viz § 4 písm. b) EO 14086. Podle EO 14086 a jak je dále vysvětleno ve 134. bodě odůvodnění, hromadný sběr podle EO 12333 probíhá pouze v případě, že je to nezbytné k dosažení konkrétních potvrzených zpravodajských priorit, a podléhá řadě omezení a ochranných opatření, jejichž cílem je zajistit, aby přístup k údajům nebyl nediskriminační. Hromadné shromažďování je proto třeba postavit do protikladu ke shromažďování na všeobecném a nerozlišujícím základě ("hromadné sledování") bez omezení a ochranných opatření.

224 Oddíl 2 písm. c) bod ii) část A EO 14086.

225 Oddíl 2 písm. c) bod ii) část A EO 14086.

226 Specifická pravidla pro hromadný sběr podle EO 14086 se nevztahují na dočasné získávání údajů bez rozlišovacích znaků (např. specifických podmínek výběru nebo identifikátorů), pokud jsou tyto údaje použity na krátkou dobu potřebnou k dokončení počáteční technické fáze cíleného sběru a ihned poté jsou vymazány (oddíl 2 písm. c) bod ii) písm. D) EO 14086). V tomto scénáři je jediným účelem hromadného sběru umožnit cílené shromažďování informací použitím specifického identifikátoru nebo selekčního termínu a toto použití je výhradním použitím údajů původně shromážděných hromadně. V takovém scénáři jsou do vládních databází vkládány pouze údaje, které odpovídají aplikaci určitého diskriminačního znaku, zatímco ostatní údaje jsou zničeny. Takový cílený sběr se proto řídí obecnými pravidly, která se vztahují na sběr signálů zpravodajských služeb, zejména oddílem 2 písm. a) a oddílem 2 písm. c) bodem i) EO 14086.

227 Oddíl 2 písm. c) bod ii) část A EO 14086.

228 Oddíl 2 písm. c) bod ii) písm. b) EO 14086. V případě, že se objeví nové požadavky na národní bezpečnost, například nové hrozby pro národní bezpečnost, může prezident tento seznam aktualizovat. Tyto aktualizace musí být v zásadě zveřejněny, pokud prezident nerozhodne, že by to samo o sobě představovalo riziko pro národní bezpečnost Spojených států (oddíl 2 písm. c) bod ii) písm. c) EO 14086). Pokud jde o dotazy na hromadně shromažďované údaje, viz oddíl 2 písm. c) bod iii) písm. d) EO 14086.

zohlednit dopad dotazů na soukromí a občanské svobody všech osob bez ohledu na jejich státní příslušnost nebo místo jejich pobytu[229] .

(135) Kromě požadavků EO 14086 podléhá shromažďování údajů o signálech, které byly předány organizaci ve Spojených státech, zvláštním omezením a ochranným opatřením upraveným v oddíle 702 FISA[230] . Oddíl 702 FISA umožňuje shromažďování zahraničních zpravodajských informací prostřednictvím cílení na osoby, o nichž se důvodně předpokládá, že se nacházejí mimo území Spojených států, a to za nucené pomoci amerických poskytovatelů služeb elektronických komunikací[231] . Za účelem shromažďování zahraničních zpravodajských informací podle oddílu 702 FISA předkládají generální prokurátor a ředitel národního zpravodajství každoročně Soudu pro dohled nad zahraničním zpravodajstvím (FISC) osvědčení, v nichž jsou uvedeny kategorie zahraničních zpravodajských informací, které mají být získány[232] . K osvědčením musí být přiloženy postupy zaměřování, minimalizace a dotazování, které rovněž schvaluje soud a které jsou pro zpravodajské agentury USA právně závazné[233] .

(136) FISC je nezávislý soud[234] zřízený federálním zákonem, proti jehož rozhodnutím se lze odvolat k Soudu pro kontrolu zahraničního zpravodajství (Foreign Intelligence Surveillance Court of Review, FISCR)[235] a nakonec k Nejvyššímu soudu Spojených států[236] . FISC (a FISCR) se opírá o stálý panel pěti právníků a pěti technických odborníků, kteří mají odborné znalosti v oblasti národní bezpečnosti i občanských svobod[237] . Z této skupiny soud jmenuje jednotlivce, který slouží jako *amicus curiae,* aby pomáhal při projednávání každé žádosti o vydání příkazu nebo o přezkum, která podle názoru soudu představuje nový nebo významný výklad práva, pokud soud neshledá, že takové jmenování není vhodné[238] . Tím je zajištěno zejména to, aby se v posouzení soudu náležitě projevily ohledy na ochranu soukromí. Soud může rovněž jmenovat jednotlivce nebo organizaci jako amicus curiae, a to i za účelem poskytnutí technických odborných znalostí,

---

[229] Oddíl 2 písm. a) bod ii) bod A ve spojení s oddílem 2 písm. c) bod iii) bod D EO 14086. Viz také příloha VII.

[230] 50 U.S.C. § 1881.

[231] 50 U.S.C. § 1881a (a). Jak uvedl PCLOB, sledování podle § 702 "spočívá zejména v tom, že se zaměřuje výhradně na konkrétní [neamerické] osoby, o nichž bylo učiněno individualizované rozhodnutí" (Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 if the Foreign Intelligence Surveillance Act, 2. července 2014, Section 702 Report, s. 111). Viz také zpráva NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702 (Provádění zákona o sledování zahraničního zpravodajství ze strany NSA), 16. dubna 2014. Pojem "poskytovatel služeb elektronických komunikací" je definován v 50 U.S.C. § 1881 (a)(4).

[232] 50 U.S.C. § 1881a (g).

[233] 50 U.S.C.1881a (i).

[234] FISC se skládá ze soudců, které jmenuje předseda Nejvyššího soudu Spojených států z řad soudců, kteří zasedají ve funkci.
soudci okresních soudů USA, kteří byli dříve jmenováni prezidentem a potvrzeni Senátem. Soudci, kteří mají doživotní mandát a mohou být odvoláni pouze z dobrého důvodu, působí ve FISC na rozložené sedmileté funkční období. FISA vyžaduje, aby soudci byli vybráni z nejméně sedmi různých zemí.
Soudní obvody USA. Viz 50 U.S.C. § 1803 (a). Soudcům pomáhají zkušení soudní právníci, kteří tvoří právní personál soudu a připravují právní analýzy žádostí o vymáhání pohledávek. Viz dopis ctihodného Reggieho B. Waltona, předsedy soudu pro dohled nad zahraničním zpravodajstvím USA, ctihodnému Patricku J. Leahymu, předsedovi Výboru pro soudnictví Senátu USA (29. července 2013) (Waltonův dopis), s. 2, k dispozici na https://fas.org/irp/news/2013/07/fisc-leahy.pdf.

[235] FISCR se skládá ze soudců jmenovaných předsedou Nejvyššího soudu Spojených států amerických, kteří jsou vybráni z řad
okresní soudy USA nebo odvolací soudy, jejichž funkční období je rozloženo na sedm let. Viz 50

U.S.C. § 1803 (b).

236 Viz 50 U.S.C. §§ 1803 b), 1861 a f), 1881 a h), 1881 a i)(4).

237 50 U.S.C. § 1803 (i)(1), (3)(A).

238 50 U.S.C. § 1803 (i)(2)(A).

kdykoli to uzná za vhodné, nebo na návrh povolí jednotlivci nebo organizaci podat stanovisko *amicus curiae*[239] .

(137) FISC přezkoumává osvědčení a související postupy (zejména postupy zaměřování a minimalizace) z hlediska souladu s požadavky zákona FISA. Pokud se domnívá, že požadavky nejsou splněny, může osvědčení zcela nebo částečně zamítnout a požádat o změnu postupů[240] . V tomto ohledu FISC opakovaně potvrdil, že se jeho přezkum postupů podle § 702 týkajících se zaměřování a minimalizace neomezuje pouze na postupy v písemné podobě, ale zahrnuje také způsob, jakým vláda tyto postupy provádí[241] .

(138) Jednotlivá rozhodnutí o zaměření provádí NSA (zpravodajská agentura odpovědná za zaměření podle článku 702 FISA) v souladu s postupy pro zaměření schválenými FISC, které vyžadují, aby NSA na základě všech okolností posoudila, že zaměření na konkrétní osobu pravděpodobně povede k získání kategorie zahraničních zpravodajských informací uvedených v osvědčení[242] . Toto posouzení musí být konkrétní a založené na faktech a vycházet z analytického úsudku, specializovaného výcviku a zkušeností analytika, jakož i z povahy zahraničních zpravodajských informací, které mají být získány[243] . Zaměření se provádí určením tzv. selektorů, které identifikují konkrétní komunikační prostředky, jako je e-mailová adresa nebo telefonní číslo cíle, nikdy však klíčová slova nebo jména osob[244] .

(139) Analytici NSA nejprve identifikují osoby, které se nenacházejí v USA a jejichž sledování povede na základě posouzení analytiků k získání příslušných zahraničních zpravodajských informací uvedených v osvědčení[245] . Jak je uvedeno v postupech NSA pro sledování cílů, NSA může zaměřit sledování na cíl pouze tehdy, pokud se již o cíli něco dozvěděla[246] . To může vyplývat z informací z různých zdrojů, například z lidského zpravodajství. Prostřednictvím těchto dalších zdrojů se analytik musí dozvědět také o konkrétním selektoru (tj. komunikačním účtu), který potenciální cíl používá. Jakmile jsou tyto individualizované osoby identifikovány a jejich zaměření schváleno.

---

239 50 U.S.C. § 1803 (i)(2)(B).

240 Viz např. FISC Stanovisko z 18 října 2018, k dispozici na na adrese https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct1 8.pdf, jak potvrdil Soud pro kontrolu zahraničních zpravodajských služeb ve svém stanovisku ze dne 12. července 2019, k dispozici na adrese na adrese https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12 Jul19.pdf.

241 Viz např. FISC, Memorandum Opinion and Order na 35 (18. listopadu 2020) (schváleno ke zveřejnění 26. dubna 2021), (příloha D).

242 50 U.S.C. § 1881a(a), Postupy používané Národní bezpečnostní agenturou pro zaměřování osob, o nichž se důvodně předpokládá, že se nacházejí mimo území Spojených států, za účelem získání zahraničních zpravodajských informací podle § 702 zákona o dohledu nad zahraničním zpravodajstvím z roku 1978, ve znění pozdějších předpisů. ve znění pozdějších předpisů, z března 2018 (NSA zaměřené na postupy), k dispozici na adrese na adrese https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27 Mar18.pdf, s. 1-4, dále vysvětleno ve zprávě PCLOB, s. 41-42.

243 Postupy NSA při zaměřování, s. 4.

244 Viz PCLOB, Zpráva o oddílu 702, str. 32-33, 45 s dalšími odkazy. Viz také pololetní hodnocení dodržování postupů a pokynů vydaných podle oddílu 702 zákona o dohledu nad zahraničním zpravodajstvím, předložené generálním prokurátorem a ředitelem Národního zpravodajství, vykazované období: Prosinec 2016 - 31. květen 2017, s. 41 (říjen 2018), k dispozici na adrese:

https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

[245] PCLOB, Zpráva o oddílu 702, s. 42-43.

[246] Postupy NSA při zaměřování, s. 2.

rozsáhlý kontrolní mechanismus v rámci NSA[247] , budou "úkolovány" (tj. vyvíjeny a aplikovány) selektory identifikující komunikační prostředky (např. e-mailové adresy) používané cíli[248] .

(140) Národní bezpečnostní orgán musí zdokumentovat věcný základ pro výběr cíle[249] a v pravidelných intervalech po počátečním zaměření potvrdit, že standard zaměření je nadále plněn[250] . Jakmile přestane být standard zaměřování splněn, musí být sběr dat ukončen[251] . Výběr každého cíle ze strany NSA a záznam o každém zaznamenaném posouzení a zdůvodnění cílení jsou každé dva měsíce přezkoumávány z hlediska dodržování postupů pro cílení úředníky úřadů pro dohled nad zpravodajskými službami na ministerstvu spravedlnosti, kteří jsou povinni oznámit jakékoli porušení FISC a Kongresu[252] . Písemná dokumentace NSA usnadňuje dohled FISC nad tím, zda jsou konkrétní osoby řádně zaměřeny podle oddílu 702 FISA, v souladu s jeho dozorovými pravomocemi popsanými v 165. až 166. bodě odůvodnění[253] . A konečně, ředitel Národního zpravodajství (DNI) je rovněž povinen každoročně informovat o celkovém počtu cílů podle oddílu 702 FISA ve veřejných výročních statistických zprávách o transparentnosti. Společnosti, které obdrží směrnice FISA podle oddílu 702, mohou zveřejňovat souhrnné údaje (prostřednictvím zpráv o transparentnosti) o obdržených žádostech[254] .

(141) Pokud jde o další právní základy pro shromažďování osobních údajů předávaných organizacím v USA, platí pro ně jiná omezení a záruky. Obecně platí, že hromadné shromažďování údajů je výslovně zakázáno podle § 402 zákona FISA (registrace pomocí pera a oprávnění k zachycení a sledování) a prostřednictvím NSL, a místo toho se vyžaduje použití specifických "výběrových podmínek"[255] .

(142) Pro provádění tradičního individualizovaného elektronického sledování (podle § 105 zákona FISA) musí zpravodajské agentury předložit FISC žádost s uvedením skutečností a okolností, které odůvodňují přesvědčení, že existuje pravděpodobná

247 PCLOB, Zpráva o sekci 702, s. 46. Například NSA musí ověřit, že existuje spojení mezi cílem a vybírajícím, musí zdokumentovat zahraniční zpravodajské informace, jejichž získání se očekává, tyto informace musí být přezkoumány a schváleny dvěma vedoucími analytiky NSA a celý proces bude sledován pro následné přezkoumání souladu ze strany ODNI a ministerstva spravedlnosti. Viz NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16. dubna 2014.

248 50 U.S.C. § 1881a (h).

249 Postupy NSA při zaměřování, s. 8. Viz také PCLOB, Zpráva o sekci 702, s. 46. Neposkytnutí písemného zdůvodnění představuje incident v oblasti dodržování dokumentace, který musí být nahlášen FISC a Kongresu. Viz pololetní hodnocení dodržování postupů a pokynů vydaných podle oddílu 702 zákona o dohledu nad zahraničním zpravodajstvím, předložené generálním prokurátorem a ředitelem Národního zpravodajství, vykazované období: Prosinec 2016 - 31. květen 2017, s. 41 (říjen 2018), Zpráva DOJ/ODNI o dodržování předpisů pro FISC za období prosinec 2016 - květen 2017, s. A-6, k dispozici na https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

250 Viz Podání vlády USA Soudu pro dohled nad zahraničním zpravodajstvím, 2015 Summary of Notable Section 702 Requirements, na str. 2-3 (15. července 2015) a informace uvedené v příloze VII.

251 Viz Podání vlády USA pro Soud pro dohled nad zahraničním zpravodajstvím, 2015 Summary of Notable Section 702 Requirements (Souhrn významných požadavků oddílu 702), na str. 2-3 (15. července 2015), které stanoví, že vláda "[p]okud vláda později vyhodnotí, že se neočekává, že by pokračující úkolování cílového selektoru vedlo k získání zahraničních zpravodajských informací, vyžaduje se okamžité odpojení a prodlení může mít za následek incident, který podléhá ohlášení". Viz také informace uvedené v příloze VII.

252 PCLOB, Zpráva o sekci 702, s. 70-72; Pravidlo 13(b) jednacího řádu zpravodajských služeb Spojených států amerických. . Soudu pro zpravodajské služby, k dispozici na na adrese https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

253 Viz také Zpráva ministerstva spravedlnosti/ODNI o dodržování předpisů pro FISC za období prosinec 2016 - květen 2017, str. A-6.

254 50 U.S.C. § 1874.

255 50 U.S. Code § 1842(c)(3) a, pokud jde o NSL, 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); a 18 U.S.C. § 2709(a).

důvod, že zařízení používá nebo se chystá použít cizí mocnost nebo zástupce cizí mocnosti[256] . FISC mimo jiné posoudí, zda na základě předložených skutečností existuje pravděpodobný důvod, že tomu tak skutečně je[257] .

(143) K provedení prohlídky prostor nebo majetku, která má vést k prověření, zabavení atd. informací, materiálů nebo majetku (např. počítačového zařízení) na základě § 301 zákona FISA, je nutná žádost o vydání příkazu FISC[258] . Taková žádost musí mimo jiné prokázat, že existuje pravděpodobný důvod, že cílem prohlídky je cizí mocnost nebo agent cizí mocnosti; že prostor nebo majetek, který má být prohledán, obsahuje zahraniční zpravodajské informace a že prostor, který má být prohledán, je ve vlastnictví, užívání, držení nebo je přepravován do nebo od (agenta) cizí mocnosti[259] .

(144) Podobně instalace registračních zařízení nebo zařízení pro sledování a vyhledávání (podle § 402 zákona FISA) vyžaduje žádost o vydání příkazu FISC (nebo soudce magistrátu USA) a použití specifického výběrového termínu, tj. termínu, který konkrétně identifikuje osobu, účet atd. a který se používá k omezení rozsahu požadovaných informací v co největší možné míře[260] . Toto oprávnění se netýká obsahu sdělení, ale je zaměřeno spíše na informace o zákazníkovi nebo účastníkovi využívajícím službu (např. jméno, adresa, účastnické číslo, délka/typ přijaté služby, zdroj/mechanismus platby).

(145) Článek 501 FISA[261] , který umožňuje shromažďování obchodních záznamů běžného dopravce (tj. jakékoli osoby nebo subjektu, který za úplatu přepravuje osoby nebo majetek po zemi, po železnici, po vodě nebo vzduchem), veřejného ubytovacího zařízení (např. hotelu, motelu nebo hostince), půjčovny vozidel nebo fyzického skladovacího zařízení (tj. zařízení, které poskytuje prostory pro skladování zboží a materiálu nebo služby související s tímto skladováním)[262] , rovněž vyžaduje podání žádosti k FISC nebo soudci magistrátu. V této žádosti musí být uvedeny požadované záznamy a konkrétní a vypovídající skutečnosti, které dávají důvod se domnívat, že osoba, jíž se záznamy týkají, je cizí mocností nebo agentem cizí mocnosti[263] .

(146) Konečně, NSL jsou povoleny různými zákony a umožňují vyšetřujícím orgánům získat určité informace (bez obsahu komunikace) od určitých subjektů (např. finančních institucí, agentur poskytujících úvěrové informace, poskytovatelů elektronických komunikací) obsažené v úvěrových zprávách, finančních záznamech a elektronických záznamech o účastnících a transakcích[264] . Zákon o NSL, který opravňuje k přístupu k elektronické komunikaci, může používat pouze FBI a vyžaduje, aby žádosti obsahovaly termín, který konkrétně identifikuje osobu, subjekt, telefonní číslo nebo účet, a potvrzení, že informace jsou relevantní pro povolené vyšetřování národní bezpečnosti, aby

256 "Agent cizí moci" může zahrnovat osoby, které nejsou členy USA a podílejí se na mezinárodním terorismu nebo mezinárodním šíření zbraní hromadného ničení (včetně přípravných akcí) (50 U.S.C. § 1801 (b)(1)).

257 50 U.S.C. § 1804. Viz také § 1841 odst. 4, pokud jde o volbu podmínek výběru.

258 50 U.S.C. § 1821 ODST. 5.

259 50 U.S.C. § 1823(a).

260 50 U.S.C. § 1842 s § 1841 odst. 2 a § 3127 hlavy 18.

261 50 U.S.C. § 1862.

262 50 U.S.C. §§ 1861-1862.

263 50 U.S.C. § 1862(b).

264 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; a 18 U.S.C. § 2709.

ochranu před mezinárodním terorismem nebo tajnými zpravodajskými aktivitami[265] . Příjemci NSL mají právo napadnout je u soudu[266] .

3.2.1.3 Další využití shromážděných informací

(147) Zpracování osobních údajů shromážděných americkými zpravodajskými službami prostřednictvím signálového zpravodajství podléhá řadě ochranných opatření.

(148) Za prvé, každá zpravodajská služba musí zajistit odpovídající zabezpečení údajů a zabránit přístupu neoprávněných osob k osobním údajům shromážděným prostřednictvím signálového zpravodajství. V tomto ohledu různé nástroje, včetně zákonů, pokynů a norem, dále specifikují minimální požadavky na bezpečnost informací, které musí být zavedeny (např. vícefaktorová autentizace, šifrování atd.)[267] . Přístup ke shromážděným údajům musí být omezen na oprávněné, vyškolené pracovníky, kteří potřebují znát informace pro plnění svých úkolů[268] . Obecněji řečeno, zpravodajské agentury musí svým zaměstnancům poskytnout odpovídající školení, včetně postupů pro hlášení a řešení porušení zákona (včetně EO 14086)[269] .

(149) Za druhé, zpravodajské agentury musí dodržovat standardy zpravodajského společenství pro přesnost a objektivitu, zejména pokud jde o zajištění kvality a spolehlivosti údajů, zohlednění alternativních zdrojů informací a objektivitu při provádění analýz[270] .

(150) Za třetí, pokud jde o uchovávání údajů, EO 14086 objasňuje, že osobní údaje osob, které nejsou občany USA, podléhají stejným lhůtám pro uchovávání jako údaje osob, které nejsou občany USA.
Osoby z USA[271] .[272] .

(151) Za čtvrté, na šíření osobních údajů shromážděných prostřednictvím signálového zpravodajství se vztahují zvláštní pravidla. Obecně platí, že osobní údaje o osobách, které nejsou členy USA, mohou být šířeny pouze v případě, že se jedná o stejný typ informací, které mohou být šířeny o osobách z USA, např. informace potřebné k ochraně bezpečnosti osob nebo organizací (jako jsou cíle, oběti nebo rukojmí mezinárodních operací).

265 18 U.S.C. § 2709(b).

266 Např. 18 U.S.C. § 2709(d).

267 Oddíl 2 písm. c) bod iii) část B odst. 1 EO 14086. Viz také hlava VIII zákona o národní bezpečnosti (podrobně popisující požadavky na přístup k utajovaným informacím), E.O. 12333, oddíl 1.5 (požadující po vedoucích agentur zpravodajského společenství, aby se řídili pokyny pro sdílení a bezpečnost informací, ochranu soukromí informací a dalšími právními požadavky), směrnice o národní bezpečnosti 42, "Národní politika pro bezpečnost telekomunikačních a informačních systémů národní bezpečnosti" (ukládající Výboru pro národní bezpečnostní systémy poskytovat výkonným útvarům a agenturám pokyny pro systémovou bezpečnost systémů národní bezpečnosti), a Národní bezpečnostní memorandum 8, "Zlepšení kybernetické bezpečnosti systémů národní bezpečnosti, ministerstva obrany a zpravodajské komunity" (stanoví časový plán a pokyny pro implementaci požadavků na kybernetickou bezpečnost systémů národní bezpečnosti, včetně vícefaktorového ověřování, šifrování, cloudových technologií a služeb detekce koncových bodů).

268 Oddíl 2 písm. c) bod iii) část B odst. 2 EO 14086. Kromě toho lze k osobním údajům, u nichž nebylo učiněno konečné rozhodnutí o uchovávání, přistupovat pouze za účelem učinění nebo podpory takového rozhodnutí nebo za účelem provádění schválených správních, testovacích, vývojových, bezpečnostních nebo dohledových funkcí (oddíl 2 písm. c) bod iii) část B odst. 3 EO 14086).

269 Oddíl 2 písm. d) bod ii) EO 14086.

270 Oddíl 2 písm. c) bod iii) písm. c) EO 14086.

271 Oddíl 2 písm. c) bod iii) část A odst. 2 písm. a) až c) EO 14086. Obecněji řečeno, každá agentura musí zavést zásady a postupy určené k minimalizaci šíření a uchovávání osobních údajů shromážděných prostřednictvím zpravodajských signálů (oddíl 2 písm. c) bod iii) písm. a) EO 14086).

272 Článek 309 zákona o autorizaci zpravodajských služeb na fiskální rok 2015.

teroristických organizací)[273] . Osobní údaje navíc nesmí být šířeny pouze z důvodu státní příslušnosti nebo země pobytu osoby nebo za účelem obcházení požadavků EO 14086[274] . Kromě toho se šíření v rámci
Vláda USA může uskutečnit pouze v případě, že oprávněná a vyškolená osoba má důvodné přesvědčení, že příjemce potřebuje informace znát a bude je náležitě chránit[275] . Pro určení, zda lze osobní údaje šířit příjemcům mimo vládu USA (včetně zahraniční vlády nebo mezinárodní organizace), je třeba vzít v úvahu účel šíření, povahu a rozsah šířených údajů a možnost škodlivého dopadu na dotčenou osobu (osoby)[276] .

(152) A konečně, mimo jiné i proto, aby se usnadnil dohled nad dodržováním platných právních požadavků, jakož i účinná náprava, je každá zpravodajská agentura povinna vést příslušnou dokumentaci o shromažďování zpravodajských informací o signálech. Požadavky na dokumentaci zahrnují takové prvky, jako je faktický základ pro posouzení, že určitá sběrná činnost je nezbytná k dosažení potvrzené zpravodajské priority[277] .

3.2.2 Dohled

(153) Činnost amerických zpravodajských služeb podléhá dohledu různých orgánů.

(154) Zaprvé, EO 14086 vyžaduje, aby každá zpravodajská agentura měla vedoucí pracovníky v oblasti práva, dohledu a dodržování předpisů, kteří zajistí dodržování platných právních předpisů USA[278] . Zejména musí provádět pravidelný dohled nad činnostmi v oblasti signálového zpravodajství a zajistit nápravu jakéhokoli nesouladu. Zpravodajské agentury musí těmto úředníkům poskytnout přístup ke všem relevantním informacím, aby mohli vykonávat své funkce dohledu, a nesmí podnikat žádné kroky, které by bránily jejich činnostem dohledu nebo je nevhodně ovlivňovaly[279] . Kromě toho musí být každý závažný případ nedodržení[280] , který zjistí úředník provádějící dohled nebo jakýkoli jiný zaměstnanec, neprodleně oznámen vedoucímu zpravodajské agentury a řediteli národního zpravodajství, který musí zajistit, aby byla přijata veškerá nezbytná opatření k nápravě a zabránění opakování závažného případu nedodržení[281] .

(155) Tuto funkci dohledu plní úředníci s určenou funkcí v oblasti dodržování předpisů, jakož i úředníci pro ochranu soukromí a občanských svobod a generální inspektoři[282] .

(156) Stejně jako v případě orgánů činných v trestním řízení existují ve všech zpravodajských agenturách úředníci pro ochranu soukromí a občanských svobod[283] . Pravomoci těchto úředníků

---

273 Oddíl 2 písm. c) bod iii) část A odst. 1 písm. a) a oddíl 5 písm. d) EO 14086 ve spojení s oddílem 2.3 EO 12333.

274 Oddíl 2 písm. c) bod iii) část A odst. 1 písm. b) a e) EO 14086 .

275 Oddíl 2 písm. c) bod iii) část A odst. 1 písm. c) EO 14086.

276 Oddíl 2 písm. c) bod iii) část A odst. 1 písm. d) EO 14086.

277 Oddíl 2 písm. c) bod iii) písm. e) EO 14086.

278 Oddíl 2 písm. d) bod i) písm. A) až B) EO 14086.

279 Oddíl 2 písm. d) bod i) písm. B) až C) EO 14086.

280 Tj. systémové nebo úmyslné nedodržování platných právních předpisů USA, které by mohlo narušit pověst nebo integritu složky zpravodajské komunity nebo jinak zpochybnit správnost činnosti zpravodajské komunity, a to i s ohledem na významný dopad na zájmy dotčené osoby nebo osob v oblasti soukromí a občanských svobod, viz § 5 písm. l) EO 14086.

281 Oddíl 2 písm. d) bod iii) EO 14086.

282 Oddíl 2 písm. d) bod i) písm. b) EO 14086.

obvykle zahrnují dohled nad postupy, které mají zajistit, aby příslušné oddělení/agentura náležitě zohledňovaly obavy o soukromí a občanské svobody a zavedly odpovídající postupy pro řešení stížností osob, které se domnívají, že bylo porušeno jejich soukromí nebo občanské svobody (a v některých případech, jako je ODNI, mohou mít samy pravomoc stížnosti prošetřit[284]). Vedoucí zpravodajských agentur musí zajistit, aby úředníci pro ochranu soukromí a občanských svobod měli k dispozici zdroje pro plnění svého mandátu, aby měli přístup ke všem materiálům a pracovníkům nezbytným pro výkon svých funkcí a aby byli informováni o navrhovaných změnách politiky a aby s nimi byly konzultovány[285] . Úředníci pro ochranu soukromí a občanských svobod pravidelně podávají zprávy Kongresu a PCLOB, včetně počtu a povahy stížností, které útvar/agentura obdržel, se shrnutím vyřízení těchto stížností, provedených přezkumů a šetření a dopadu činností prováděných úředníkem[286] .

(157) Za druhé, každá zpravodajská služba má nezávislého generálního inspektora, který je mimo jiné odpovědný za dohled nad zahraničními zpravodajskými aktivitami. V rámci ODNI tak existuje Úřad generálního inspektora zpravodajské komunity s komplexní působností pro celou zpravodajskou komunitu, který je oprávněn vyšetřovat stížnosti nebo informace týkající se údajného nezákonného jednání nebo zneužití pravomoci v souvislosti s programy a činnostmi ODNI a/nebo zpravodajské komunity[287] . Stejně jako v případě orgánů činných v trestním řízení (viz 105. bod odůvodnění) jsou tito generální inspektoři ze zákona nezávislí[288] a jsou odpovědní za provádění auditů a vyšetřování týkajících se programů a

---

283 Viz 42 U.S.C. § 2000ee-1. Patří sem například Ministerstvo zahraničí, Ministerstvo spravedlnosti, Ministerstvo vnitřní bezpečnosti, Ministerstvo obrany, NSA, CIA, FBI a ODNI.

284 Viz oddíl 3 písm. c) EO 14086.

285 42 U.S.C. § 2000ee-1(d).

286 Viz 42 U.S.C. § 2000ee-1 (f)(1),(2). Například ze zprávy Úřadu pro občanské svobody, soukromí a transparentnost NSA za období leden 2021 - červen 2021 vyplývá, že provedl 591 přezkumů dopadů na občanské svobody a soukromí v různých souvislostech, např. s ohledem na činnosti shromažďování, ujednání a rozhodnutí o sdílení informací, rozhodnutí o uchovávání údajů atd. s přihlédnutím k různým faktorům, jako je množství a typ informací spojených s danou činností, dotčené osoby, účel a předpokládané využití údajů, zavedená ochranná opatření ke zmírnění možných rizik pro soukromí atd. (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Podobně je tomu i v případě zprávy Úřadu pro ochranu soukromí a občanských svobod CIA za leden až červen 2019 poskytují informace o dohledových činnostech úřadu, např. přezkum dodržování pokynů generálního prokurátora podle EO 12333, pokud jde o uchovávání a šíření informací, pokyny poskytované k provádění směrnice PPD 28 a požadavky na identifikaci a řešení případů narušení bezpečnosti údajů a přezkumy používání údajů. a nakládání s údaji . osobních údajů informací (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi- Annual-Report.pdf).

287 Generálního inspektora jmenuje prezident, schvaluje ho Senát a může ho odvolat pouze prezident.

288 Generální inspektoři mají jisté funkční období a mohou být odvoláni pouze prezidentem, který musí Kongresu písemně sdělit důvody takového odvolání. To nutně neznamená, že jsou zcela osvobozeni od pokynů. V některých případech může vedoucí oddělení zakázat generálnímu inspektorovi zahájit, provést nebo dokončit audit nebo vyšetřování, pokud je to považováno za nezbytné pro zachování důležitých národních (bezpečnostních) zájmů. O výkonu této pravomoci však musí být informován Kongres, který by na základě toho mohl příslušného ředitele volat k odpovědnosti. Viz např. zákon o generálním inspektorovi z roku 1978, § 8 (pro ministerstvo obrany); § 8E (pro ministerstvo spravedlnosti), § 8G písm. d) odst. 2 písm. a), b) (pro NSA); 50. Zákon o generálním inspektorovi z roku 1978. U.S.C. § 403q písm. b) (pro CIA); Intelligence Authorization Act For the Fiscal Year 2010, § 405 písm. f) (pro zpravodajskou komunitu).

operace prováděné příslušnou agenturou pro účely národního zpravodajství, a to i s ohledem na zneužití nebo porušení zákona[289] . Mají přístup ke všem záznamům, zprávám, auditům, revizím, dokumentům, písemnostem, doporučením nebo jiným relevantním materiálům, v případě potřeby na základě předvolání, a mohou podávat svědectví[290] . Generální inspektoři předávají případy podezření na trestné činy k trestnímu stíhání a předkládají vedoucím agentur doporučení k nápravě[291] . Jejich doporučení jsou sice nezávazná, ale jejich zprávy, včetně zpráv o následných opatřeních (nebo jejich nedostatku)[292] , jsou zpravidla zveřejňovány a zasílány Kongresu, který na jejich základě může vykonávat svou vlastní funkci dohledu (viz 160. bod odůvodnění)[293] .

(158) Za třetí, Rada pro dohled nad zpravodajskými službami (IOB), která je zřízena v rámci Poradního výboru prezidenta pro zpravodajské služby (PIAB), dohlíží na dodržování ústavy a všech platných pravidel ze strany amerických zpravodajských orgánů[294] . PIAB je poradním orgánem v rámci výkonné kanceláře prezidenta, který se skládá ze 16 členů jmenovaných prezidentem z řad osob mimo vládu USA. IOB se skládá z maximálně pěti členů jmenovaných prezidentem z řad členů PIAB. Podle EO 12333[295] jsou vedoucí všech zpravodajských agentur povinni hlásit IOB jakoukoli zpravodajskou činnost, u níž existuje důvodné podezření, že by mohla být nezákonná nebo v rozporu s výkonným nařízením nebo prezidentskou směrnicí. Aby se zajistilo, že IOB bude mít přístup k informacím nezbytným k výkonu své

---

289 Inspector General Act of 1978, ve znění pozdějších předpisů, Pub. L. 117-108 ze dne 8. dubna 2022. Jak je například vysvětleno v pololetních zprávách pro Kongres za období od 1. dubna 2021 do 31. března 2022, generální inspektor NSA provedl hodnocení nakládání s informacemi o amerických osobách shromážděnými podle EO 12333, procesu čištění údajů signálového zpravodajství, automatizovaného nástroje pro cílení používaného NSA a dodržování pravidel pro dokumentaci a dotazování s ohledem na shromažďování údajů podle oddílu 702 FISA a vydal v této souvislosti několik doporučení (viz https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-.%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d, s. 5-8 a https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d.%3d&timestamp=1657810395907, s. 10-13). Viz také nedávné audity a vyšetřování provedené generálním inspektorem zpravodajské komunity v oblasti bezpečnosti informací a neoprávněného vyzrazování informací. . utajovaných informací národních bezpečnosti informací (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, str. 8, 11 a https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, s. 19-20).

290 Viz § 6 zákona o generálním inspektorovi z roku 1978.

291 Viz *tamtéž*. §§ 4, 6-5.

292 Pokud jde o následné kroky v návaznosti na zprávy a doporučení generálních inspektorů, viz. např. reakce na zprávu generálního inspektora DoJ, která zjistila, že FBI nebyla dostatečně transparentní vůči FISC v žádostech z let 2014 až 2019, což vedlo k reformám, které mají zlepšit dodržování předpisů, dohled a odpovědnost v FBI (např. ředitel FBI nařídil více než 40 nápravných opatření, včetně 12 specifických pro proces FISA týkajících se dokumentace, dohledu, vedení spisů, školení a auditů) (viz https://www.justice.gov/opa/pr/department-justice-and-federal- bureau-investigation-announce-critical-reforms-enhance. a https://oig.justice.gov/reports/2019/o20012.pdf). Viz např. také audit generálního inspektora DoJ týkající se rolí a odpovědností úřadu generálního poradce FBI při dohledu nad dodržováním platných zákonů, zásad a postupů týkajících se činností FBI v oblasti národní bezpečnosti a dodatek 2, který obsahuje dopis FBI, v němž přijímá všechna doporučení. V této souvislosti je v dodatku 3 uveden přehled následných opatření a informací, které generální inspektor požadoval od FBI, aby mohl svá doporučení uzavřít (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).

293 Viz zákon o generálním inspektorovi z roku 1978, §§ 4(5), 5.

294 Viz EO 13462.

295 Oddíl 1.6 písm. c) EO 12333.

funkcí, EO 13462 nařizuje řediteli Národního zpravodajství a vedoucím zpravodajských agentur poskytovat veškeré informace a pomoc, kterou IOB určí jako potřebnou pro výkon svých funkcí, v rozsahu povoleném zákonem[296] . IOB je zase povinna informovat prezidenta o zpravodajských činnostech, o nichž se domnívá, že mohou být v rozporu s právem USA (včetně exekutivních příkazů) a že se jimi generální prokurátor, ředitel národního zpravodajství nebo vedoucí zpravodajské agentury dostatečně nezabývají[297] . Kromě toho je IOB povinna informovat generálního prokurátora o možném porušení trestního práva.

(159) Za čtvrté, zpravodajské agentury podléhají dohledu PCLOB, nezávislé agentury v rámci výkonné moci, která se skládá z pětičlenné rady složené z obou stran, jmenované prezidentem na pevně stanovené šestileté období se souhlasem Senátu[298] . Podle svého zakládajícího statutu je PCLOB pověřena odpovědností v oblasti protiteroristické politiky a jejího provádění s ohledem na ochranu soukromí a občanských svobod. Při přezkumu činnosti zpravodajských služeb může mít přístup ke všem relevantním záznamům, zprávám, auditům, posudkům, dokumentům, spisům a doporučením agentur, včetně utajovaných informací, vést rozhovory a vyslechnout svědectví[299] . Přijímá zprávy od úředníků pro občanské svobody a ochranu soukromí několika federálních ministerstev/agentur[300] , může vydávat doporučení vládě a zpravodajským agenturám a pravidelně podává zprávy výborům Kongresu a prezidentovi[301] . Zprávy výboru, včetně zpráv pro Kongres, musí být v co největší míře zveřejňovány[302] . PCLOB vydala několik zpráv o dohledu a následných opatřeních, včetně analýzy programů provozovaných na základě oddílu 702 FISA a ochrany soukromí v této souvislosti, provádění PPD 28 a EO 12333[303] . PCLOB byl rovněž pověřen výkonem zvláštních funkcí dohledu, pokud jde o provádění EO 14086, zejména přezkoumáváním, zda jsou postupy agentur v souladu s EO (viz 120. bod odůvodnění), a hodnocením fungování nápravného mechanismu (viz 186. bod odůvodnění).

(160) Za páté, kromě mechanismů dohledu v rámci výkonné moci mají zvláštní výbory v Kongresu USA (zpravodajský výbor Sněmovny reprezentantů a výbor Senátu a soudní výbor) odpovědnost za dohled nad všemi zahraničními zpravodajskými aktivitami USA. Členové těchto výborů mají přístup k utajovaným informacím i zpravodajským metodám a programům[304] . Výbory vykonávají svůj dohled

---

296 Oddíl 8(a) EO 13462.

297 Oddíl 6(b) EO 13462.

298 Členové rady musí být vybíráni výhradně na základě své odborné kvalifikace, dosažených výsledků, veřejného postavení, odborných znalostí v oblasti občanských svobod a soukromí a příslušných zkušeností, a to bez ohledu na politickou příslušnost. V žádném případě nesmí být více než tři členové rady příslušníky stejné politické strany. Osoba jmenovaná do rady nesmí být po dobu svého působení v radě voleným úředníkem, funkcionářem nebo zaměstnancem federální vlády, s výjimkou funkce člena rady. Viz 42 U.S.C. § 2000ee (h).

299 42 U.S.C. § 2000ee (g).

300 Viz 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Patří mezi ně alespoň Ministerstvo spravedlnosti, Ministerstvo obrany, Ministerstvo vnitřní bezpečnosti, ředitel Národní zpravodajské služby a Ústřední zpravodajská služba, plus jakékoli další ministerstvo, agentura nebo složka výkonné moci, které PCLOB určí jako vhodné pro pokrytí.

301 42 U.S.C. § 2000ee, (e).

302 42 U.S.C. § 2000ee (f).

303 K dispozici na adrese https://www.pclob.gov/Oversight.

304 50 U.S.C. § 3091).

funguje různými způsoby, zejména prostřednictvím slyšení, vyšetřování, přezkumů a zpráv[305] .

(161) Kongresové výbory dostávají pravidelné zprávy o zpravodajské činnosti, včetně zpráv od generálního prokurátora, ředitele národních zpravodajských služeb, zpravodajských agentur a dalších orgánů dohledu (např. generálních inspektorů), viz 156.-157. bod odůvodnění. Podle zákona o národní bezpečnosti zejména "[p]ředseda zajistí, aby výbory Kongresu pro zpravodajské služby byly plně a aktuálně informovány o zpravodajských činnostech Spojených států, včetně všech významných předpokládaných zpravodajských činností, jak to vyžaduje tato podkapitola"[306] . Kromě toho "[p]ředseda zajistí, aby byly výborům Kongresu pro zpravodajskou činnost neprodleně oznámeny veškeré nezákonné zpravodajské činnosti, jakož i veškerá nápravná opatření, která byla přijata nebo jsou plánována v souvislosti s takovou nezákonnou činností"[307] .

(162) Kromě toho ze zvláštních zákonů vyplývají další požadavky na podávání zpráv. FISA zejména vyžaduje, aby generální prokurátor "plně informoval" senátní a sněmovní výbory pro zpravodajské služby a soudnictví o činnostech vlády podle určitých částí FISA[308] . Vyžaduje rovněž, aby vláda poskytla výborům Kongresu kopie všech rozhodnutí, příkazů nebo stanovisek FISC nebo FISCR, které obsahují "významnou konstrukci nebo výklad" ustanovení FISA. Pokud jde o sledování podle oddílu 702 FISA, parlamentní dohled se vykonává prostřednictvím zákonem požadovaných zpráv zpravodajskému a soudnímu výboru, jakož i častých brífinků a slyšení. Ty zahrnují pololetní zprávu generálního prokurátora popisující používání oddílu 702 FISA s podklady, včetně zpráv ministerstva spravedlnosti a ODNI o dodržování předpisů a popisu všech případů nedodržování předpisů[309] , a samostatné pololetní hodnocení generálního prokurátora a DNI dokumentující dodržování postupů zaměřování a minimalizace[310] .

(163) Kromě toho FISA vyžaduje, aby vláda USA každoročně zveřejňovala Kongresu (a veřejnosti) počet vyžádaných a obdržených příkazů FISA a odhady počtu příkazů FISA.

---

[305] Výbory například pořádají tematická slyšení (viz n a p ř . nedávné slyšení ve Sněmovně reprezentantů pro soudnictví). výboru na "digitální dragnets", https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983, a slyšení výboru pro zpravodajské služby Sněmovny reprezentantů, které se konalo v roce 2012. výboru . na . používání . AI podle . Inteligence Společenství, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263) pravidelný dohledová slyšení, např. . . FBI a DoJ národní . oddělení, viz https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 a https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899. Jak uvádí . příklad vyšetřování viz vyšetřování senátního výboru pro zpravodajské služby týkající se ruského vměšování do voleb v roce 2016. USA volby, viz https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures. Pokud jde o zpravodajství, viz např. přehled (dozorové) činnosti výboru ve zprávě senátního výboru pro zpravodajské služby za období 4 ledna 2019 - 3 Leden 2021 na . Senátu, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4.

[306] Viz 50 U.S.C. § 3091(a)(1). Toto ustanovení obsahuje obecné požadavky, pokud jde o dohled Kongresu v oblasti národní bezpečnosti.

[307] Viz 50 U.S.C. § 3091(b).

[308] Viz 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

[309] Viz 50 U.S.C. § 1881f.

[310] Viz 50 U.S.C. § 1881a(l)(1).

počtu amerických i neamerických osob, které jsou předmětem sledování, mimo jiné[311] . Zákon rovněž vyžaduje další veřejné podávání zpráv o počtu vydaných NSL, opět jak ve vztahu k americkým, tak neamerickým osobám (a zároveň umožňuje příjemcům příkazů a osvědčení FISA, jakož i žádostí o NSL, vydávat za určitých podmínek zprávy o transparentnosti)[312] .

(164) Obecněji řečeno, zpravodajská komunita USA vyvíjí různé snahy o zajištění transparentnosti svých (zahraničních) zpravodajských aktivit. Například v roce 2015 ODNI přijala Zásady transparentnosti zpravodajských služeb a Plán provádění transparentnosti a nařídila každé zpravodajské agentuře, aby jmenovala úředníka pro transparentnost zpravodajských služeb, který bude podporovat transparentnost a vést iniciativy v oblasti transparentnosti[313] . V rámci těchto snah zpravodajské společenství zveřejnilo a nadále zveřejňuje odtajněné části politik, postupů, zpráv o dohledu, zpráv o činnostech podle § 702 FISA a EO 12333, rozhodnutí FISC a další materiály, a to i na specializované internetové stránce "IC on the Record", kterou spravuje ODNI[314] .

(165) A konečně, shromažďování osobních údajů podle oddílu 702 zákona FISA podléhá kromě dohledu orgánů dohledu uvedených ve 154. až 160. bodě odůvodnění také dohledu FISC[315] . Podle pravidla 13 jednacího řádu FISC jsou pracovníci odpovědní za dodržování předpisů ve zpravodajských agenturách USA povinni hlásit veškerá porušení postupů zaměřování, minimalizace a dotazování podle 702 FISA DoJ a ODNI, které je následně hlásí FISC. Kromě toho DoJ a ODNI předkládají FISC pololetní společné hodnotící zprávy o dohledu, které určují trendy v oblasti dodržování postupů zaměřování, poskytují statistické údaje, popisují kategorie případů nedodržování předpisů, podrobně popisují důvody, proč k určitým případům nedodržování postupů zaměřování došlo, a nastiňují opatření, která zpravodajské agentury přijaly, aby zabránily jejich opakování[316] .

(166) V případě potřeby (např. pokud je zjištěno porušení postupů zaměřování) může Soudní dvůr nařídit příslušné zpravodajské agentuře, aby přijala nápravná opatření[317] . Nápravná opatření v

---

311 50 U.S.C. § 1873(b). Kromě toho podle § 402 "ředitel Národního zpravodajství po konzultaci s generálním prokurátorem provede přezkum odtajnění každého rozhodnutí, příkazu nebo stanoviska vydaného Soudem pro dohled nad zahraničním zpravodajstvím nebo Soudem pro přezkum dohledu nad zahraničním zpravodajstvím (jak je definován v § 601 písm. e)), které obsahuje významnou konstrukci nebo výklad jakéhokoli ustanovení zákona, včetně jakékoli nové nebo významné konstrukce nebo výkladu pojmu "specifický výběrový pojem", a v souladu s tímto přezkumem zpřístupní veřejnosti v co největší možné míře každé takové rozhodnutí, příkaz nebo stanovisko".

312 50 U.S.C. §§ 1873(b)(7) a 1874.

313 https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic.

314 Viz "IC on the Record", dostupné na https://icontherecord.tumblr.com/.

315 FISC v minulosti dospěl k závěru, že "je zřejmé, že prováděcí agentury, jakož i [ODNI] a [odbor národní bezpečnosti ministerstva spravedlnosti] věnují značné zdroje svým povinnostem v oblasti dodržování předpisů a dohledu podle oddílu 702". Obecně platí, že případy nedodržení jsou neprodleně zjišťovány a jsou přijímána příslušná nápravná opatření, včetně vyčištění informací, které byly získány neoprávněně nebo které jinak podléhají požadavkům na zničení podle platných postupů". Soud FISA, Memorandum Opinion and Order [nadpis redigován] (2014), k dispozici na adrese https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

316 *Viz např.* zpráva DOJ/ODNI FISA 702 Compliance Report to FISC for June 2018 - Nov. 2018, 21-65.

317 50 U.S.C. § 1803(h). Viz také PCLOB, Zpráva o sekci 702, s. 76. Kromě toho viz memorandové stanovisko a příkaz FISC ze dne 3. října 2011 jako příklad příkazu k odstranění nedostatků, v němž bylo vládě nařízeno, aby zjištěné nedostatky odstranila do 30 dnů. K dispozici na adrese

mohou být různá, od individuálních až po strukturální opatření, např. od ukončení získávání údajů a vymazání neoprávněně získaných údajů až po změnu praxe shromažďování údajů, včetně pokynů a školení pro zaměstnance[318] . Kromě toho FISC při každoročním přezkumu osvědčení podle § 702 posuzuje případy nedodržení předpisů, aby určil, zda jsou předložená osvědčení v souladu s požadavky FISA. Stejně tak, pokud FISC zjistí, že vládní osvědčení nebyla dostatečná, a to i z důvodu konkrétních incidentů týkajících se dodržování předpisů, může vydat tzv. příkaz k odstranění nedostatků, který vládě ukládá, aby do 30 dnů napravila porušení předpisů, nebo jí ukládá, aby přestala nebo nezačala provádět osvědčení podle oddílu 702. V takovém případě může FISC vydat příkaz k odstranění nedostatků. V neposlední řadě FISC posuzuje trendy, které pozoruje v otázkách dodržování předpisů, a může požadovat změny postupů nebo dodatečný dohled a podávání zpráv, aby řešil trendy v oblasti dodržování předpisů[319] .

3.2.3 Náprava

(167) Jak je podrobněji vysvětleno v 168.-191. bodě odůvodnění, ve Spojených státech existuje řada možností, jak subjektům údajů umožnit podat žalobu k nezávislému a nestrannému soudu se závaznými pravomocemi. Společně umožňují fyzickým osobám získat přístup ke svým osobním údajům, nechat přezkoumat zákonnost přístupu vlády k jejich údajům a v případě zjištění porušení zajistit nápravu tohoto porušení, včetně opravy nebo výmazu jejich osobních údajů.

(168) Zaprvé, na základě výnosu 14086, doplněného nařízením generálního tajemníka, kterým se zřizuje Soud pro přezkum ochrany údajů, se zřizuje zvláštní mechanismus pro vyřizování a řešení stížností fyzických osob týkajících se činností amerického zpravodajství v oblasti signálů. Každá fyzická osoba v EU[320] je oprávněna podat mechanismu nápravy stížnost týkající se údajného porušení právních předpisů USA upravujících zpravodajské činnosti v oblasti signálů (např. EO 14086, oddíl 702 FISA, EO 12333), které nepříznivě ovlivňuje její zájmy v oblasti soukromí a občanských svobod[321] .

(169) Subjekt údajů v Unii, který si přeje podat takovou stížnost, ji musí předložit dozorovému úřadu v členském státě EU, který je příslušný pro dohled nad vnitrostátními právními předpisy.

---

https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. Viz Waltonův dopis, oddíl 4, str. 10 -11. Viz také stanovisko FISC ze dne 18. října 2018, dostupné na https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin._18Oct18.pdf, jak potvrdil Soud pro kontrolu zahraničních zpravodajských služeb ve svém stanovisku ze dne 12. července 2019, k dispozici

n

a adrese https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, ve kterém FISC mimo jiné nařídil vládě, aby splnila určité požadavky na oznamování, dokumentaci a podávání zpráv FISC.

318 Viz např. FISC, Memorandum Opinion and Order na str. 76 (6. prosince 2019) (schváleno ke zveřejnění 4. září 2020), ve kterém FISC nařídil vládě, aby do 28. února 2020 předložila písemnou zprávu o krocích, které vláda podniká ke zlepšení procesů identifikace a odstraňování zpráv odvozených z informací FISA 702, které byly odvolány z důvodů dodržování předpisů, jakož i o dalších záležitostech. Viz také příloha VII.

319 Viz příloha VII.

320 Mechanismus nápravy v oblasti zpravodajských signálů je k dispozici osobám ze zemí nebo organizací regionální hospodářské integrace, které byly generálním prokurátorem USA označeny jako "způsobilé státy" (§ 3 písm. f) EO 14086). Podle [Místo pro označení EU/EHP generální tajemnicí] byla EU/EHP označena jako "kvalifikovaný stát".

[321] Viz § 4 písm. k) bod iv) EO 14086, který stanoví, že stížnost k mechanismu nápravy musí podat stěžovatel jednající vlastním jménem (tj. nikoli jako zástupce vlády, nevládní nebo mezivládní organizace).

bezpečnostní služby a/nebo zpracování osobních údajů orgány veřejné moci[322] . To zajišťuje snadný přístup k mechanismu nápravy tím, že umožňuje jednotlivcům obrátit se na orgán "blízko domova", s nímž mohou komunikovat ve svém vlastním jazyce. Příslušné vnitrostátní orgány budou stížnosti předávat mechanismu nápravy.

(170) Podání stížnosti k mechanismu nápravy podléhá nízkým požadavkům na přípustnost, neboť jednotlivci nemusí prokazovat, že jejich údaje byly skutečně předmětem činnosti amerického signálového zpravodajství[323] . Současně je třeba poskytnout určité základní informace, aby mechanismus pro zjednávání nápravy mohl zahájit přezkum, např. pokud jde o osobní údaje, o nichž se důvodně předpokládá, že byly předány do USA, a prostředky, jimiž se předpokládá, že byly předány; totožnost amerických zpravodajských služeb.Vládní subjekty USA, o nichž se předpokládá, že se podílely na údajném porušení (pokud jsou známy); základ pro tvrzení, že došlo k porušení práva USA (ačkoli to opět nevyžaduje prokázání, že osobní údaje byly skutečně shromážděny zpravodajskými službami USA), a povahu požadované nápravy.

(171) Prvotní šetření stížností k tomuto mechanismu nápravy provádí ODNI CLPO, jehož stávající zákonná úloha a pravomoci byly rozšířeny o tyto konkrétní kroky přijaté podle EO 14086[324] . V rámci zpravodajského společenství je CLPO mimo jiné odpovědný za zajištění toho, aby ochrana občanských svobod a soukromí byla vhodně začleněna do politik a postupů ODNI a zpravodajských agentur; dohlíží na dodržování platných požadavků na občanské svobody a soukromí ze strany ODNI a provádí posouzení dopadů na soukromí[325] . CLPO ODNI může odvolat pouze ředitel národního zpravodajství z důvodu jeho odvolání,
Tj. v případě pochybení, zneužití pravomoci, porušení bezpečnosti, zanedbání povinností nebo neschopnosti[326] .

(172) Při provádění přezkumu má CLPO ODNI přístup k informacím pro své posouzení a může se spolehnout na vynucenou pomoc úředníků pro ochranu soukromí a občanských svobod v různých zpravodajských agenturách[327] . Zpravodajské agentury mají zakázáno bránit přezkumu ze strany ODNI CLPO nebo jej nevhodně ovlivňovat. To se týká i ředitele národních zpravodajských služeb, který nesmí do přezkumu zasahovat[328] . Při přezkoumávání stížnosti musí ODNI CLPO uplatňovat zákon "nestranně" s ohledem na zájmy národní bezpečnosti v oblasti signálních zpravodajských činností i na ochranu soukromí[329] .

(173) V rámci přezkumu ODNI CLPO zjišťuje, zda nedošlo k porušení platných právních předpisů.
USA a v takovém případě rozhodne o vhodné nápravě[330] . Ta se týká opatření, která plně napravují zjištěné porušení, jako je ukončení nezákonného získávání údajů, vymazání nezákonně shromážděných údajů, vymazání výsledků nevhodně provedených dotazů na jinak zákonně shromážděné údaje,

322 Oddíl 4 písm. d) bod v) EO 14086.
323 Oddíl 4 písm. k) EO 14086. Stížnost je nepřípustná, pokud je neopodstatněná, šikanózní nebo podaná ve zlé víře.
324 Oddíl 3 písm. c) bod iv) EO 14086. Viz také zákon o národní bezpečnosti z roku 1947, 50 U.S.C. §403-3d, oddíl 103D týkající se úlohy CLPO v rámci ODNI.
325 50 U.S.C. § 3029 (b).
326 Oddíl 3 písm. c) bod iv) EO 14086.
327 Oddíl 3 písm. c) bod iii) EO 14086.
328 Oddíl 3 písm. c) bod iv) EO 14086.
329 Oddíl 3 písm. c) bod i) část B písm. i) a iii) EO 14086.
330 Oddíl 3 písm. c) bod i) EO 14086.

omezit přístup k zákonně shromážděným údajům pouze na příslušně vyškolený personál nebo odvolat zpravodajské zprávy obsahující údaje získané bez zákonného povolení nebo údaje, které byly nezákonně rozšířeny[331] . Rozhodnutí ODNI CLPO o jednotlivých stížnostech (včetně nápravy) jsou pro dotčené zpravodajské agentury závazná[332] .

(174) ODNI CLPO musí vést dokumentaci o svém přezkumu a vypracovat utajované rozhodnutí, v němž vysvětlí základ pro svá skutková zjištění, rozhodnutí o tom, zda došlo ke krytému porušení, a stanovení vhodné nápravy[333] . Pokud přezkum ODNI CLPO odhalí porušení některého z orgánů podléhajících dohledu FISC, musí CLPO rovněž předložit utajovanou zprávu asistentovi generálního prokurátora pro národní bezpečnost, který je následně povinen oznámit nedodržení FISC, který může přijmout další donucovací opatření (v souladu s postupem popsaným v 165.-166. bodě odůvodnění)[334] .

(175) Po ukončení přezkumu ODNI CLPO prostřednictvím vnitrostátního orgánu informuje stěžovatele, že "přezkum buď nezjistil žádné zahrnuté porušení, nebo ODNI CLPO vydal rozhodnutí vyžadující odpovídající nápravu"[335] . To umožňuje chránit důvěrnost činností prováděných za účelem ochrany národní bezpečnosti a zároveň poskytnout jednotlivcům rozhodnutí potvrzující, že jejich stížnost byla řádně prošetřena a vyřízena. Proti tomuto rozhodnutí se navíc může jednotlivec odvolat. Za tímto účelem bude (s)oud informován o možnosti odvolat se k DPRC za účelem přezkoumání rozhodnutí CLPO (viz 176. a další body odůvodnění) a o tom, že v případě, že by byl soud příslušný, bude vybrán zvláštní advokát, který bude hájit zájmy stěžovatele[336] .

(176) Každý stěžovatel, stejně jako každá složka zpravodajské komunity, může požádat o přezkum rozhodnutí ODNI CLPO u Soudu pro přezkum ochrany údajů (DPRC). Takové žádosti o přezkum musí být podány do 60 dnů od obdržení oznámení ODNI CLPO, že jeho přezkum byl ukončen, a musí obsahovat veškeré informace, které si jednotlivec přeje DPRC poskytnout (např. argumenty týkající se právních otázek nebo aplikace práva na skutkové okolnosti případu)[337] . Subjekty údajů z Unie mohou opět podat žádost prostřednictvím svých vnitrostátních orgánů.

(177) DPRC je nezávislý soud zřízený generálním prokurátorem na základě EO 14086[338] . Skládá se z nejméně šesti soudců, které jmenuje generální prokurátor po konzultaci s PCLOB, ministrem obchodu a ředitelem národního zpravodajství na čtyřleté funkční období s možností prodloužení[339] . Při jmenování soudců generálním prokurátorem se vychází z kritérií, která výkonná moc používá při posuzování kandidátů na federální soudce, přičemž se přihlíží k případným předchozím soudním

331 Oddíl 4 písm. a) EO 14086.
332 Oddíl 3 písm. c) a d) EO 14086.
333 Oddíl 3 písm. c) bod i) písm. F) až G) EO 14086.
334 Viz také oddíl 3 písm. c) bod i) písm. d) EO 14086.
335 Oddíl 3 písm. c) bod i) část E odst. 1 EO 14086.
336 Oddíl 3 písm. c) bod i) část E odst. 2 až 3 EO 14086.
337 Oddíly 201.6(a)-(b) nařízení AG.
338 oddíl 3 písm. d) bod i) a nařízení AG. Nejvyšší soud Spojených států uznal možnost generálního prokurátora zřídit nezávislé orgány s rozhodovací pravomocí, včetně rozhodování v jednotlivých případech, viz zejména rozsudky *United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954) a *United States v. Nixon*, 418 U.S. 683, 695 (1974).
339 Oddíl 3 písm. d) bod i) bod A EO 14086 a oddíl 201.3 písm. a) nařízení AG.

zkušenosti[340] . Kromě toho musí být soudci právníci z praxe (tj. aktivní členové advokátní komory s dobrou pověstí a řádnou licencí k výkonu právnické praxe) a musí mít odpovídající zkušenosti v oblasti práva soukromí a národní bezpečnosti. Generální prokurátor musí usilovat o to, aby alespoň polovina soudců měla v daném okamžiku předchozí soudní praxi, a všichni soudci musí být držiteli bezpečnostní prověrky, aby mohli přistupovat k utajovaným informacím o národní bezpečnosti[341] .

(178) Do DPRC mohou být jmenovány pouze osoby, které splňují kvalifikační předpoklady uvedené v bodě 177 odůvodnění a které v době svého jmenování nebo v předchozích dvou letech nebyly zaměstnanci výkonné moci. Stejně tak nesmí mít soudci během svého funkčního období v DPRC žádné úřední povinnosti ani zaměstnání v rámci vlády USA (kromě funkce soudce v DPRC)[342] .

(179) Nezávislost rozhodovacího procesu je zajištěna řadou záruk. Zejména je zakázáno, aby výkonná moc (generální prokurátor a zpravodajské služby) zasahovala do přezkumu DPRC nebo jej nevhodně ovlivňovala[343] . Samotný výbor DPRC je povinen rozhodovat případy nestranně[344] a pracuje podle vlastního jednacího řádu (přijatého většinou hlasů)[345] . Kromě toho může soudce DPRC odvolat pouze generální prokurátor z důvodu (tj. pochybení, zneužití pravomoci, porušení bezpečnosti, zanedbání povinností nebo neschopnost), a to po řádném zohlednění norem platných pro federální soudce, které jsou stanoveny v pravidlech pro řízení o chování soudců a soudců[346] .

(180) Žádosti o přijetí do DPRC posuzují senáty složené ze tří soudců, včetně předsedy, kteří musí jednat v souladu s Kodexem chování soudců USA[347] . Každému senátu pomáhá zvláštní advokát[348] , který má přístup ke všem informacím týkajícím se případu, včetně utajovaných informací[349] . Úkolem zvláštního advokáta je zajistit, aby byly zastoupeny zájmy stěžovatele a aby

---

340 Oddíl 201.3 písm. b) nařízení AG.

341 Oddíl 3 písm. d) bod i) písm. b) EO 14086.

342 Oddíl 3 písm. d) bod i) bod A EO 14086 a oddíl 201.3 písm. a) a c) nařízení AG. Osoby jmenované do DPRC se mohou podílet na mimosoudních činnostech, včetně podnikání, finančních aktivit, neziskových fundraisingových a fiduciárních činností, jakož i na výkonu právnické praxe, pokud tyto činnosti nenarušují nestranný výkon jejich povinností nebo účinnost či nezávislost DPRC (oddíl 201.7 písm. c) nařízení AG).

343 Oddíl 3 písm. d) body iii) až iv) EO 14086 a oddíl 201.7 písm. d) nařízení AG.

344 Oddíl 3 písm. d) bod i) písm. d) EO 14086 a oddíl 201.9 nařízení AG.

345 [Místo pro jednací řád (bude zveřejněn)].

346 Oddíl 3 písm. d) bod iv) EO 14086 a oddíl 201.7 písm. d) nařízení AG.

347 Oddíl 3 písm. d) bod i) písm. b) EO 14086 a oddíl 201.7 písm. a) až c) nařízení AG. Úřad pro ochranu soukromí a občanských svobod Ministerstva spravedlnosti (OPCL), který je odpovědný za poskytování administrativní podpory DPRC a zvláštním advokátům (viz oddíl 201.5 nařízení AG), vybírá tříčlenný senát na základě rotace, přičemž se snaží zajistit, aby v každém senátu byl alespoň jeden soudce s předchozí soudní praxí (pokud žádný ze soudců v senátu takovou praxi nemá, předsedá senátu soudce, kterého OPCL vybral jako prvního).

348 Oddíl 201.4 Nařízení AG. Nejméně dva zvláštní advokáti jsou jmenováni generálním prokurátorem po konzultaci s ministrem obchodu, ředitelem národního zpravodajství a PCLOB, a to na dvě funkční období, která lze obnovit. Zvláštní advokáti musí mít odpovídající zkušenosti v oblasti práva soukromí a národní bezpečnosti, musí být zkušenými advokáty, aktivními členy advokátní komory s dobrou pověstí a řádně oprávněnými k výkonu advokacie. Kromě toho nesmějí být v době svého prvního jmenování po dobu předchozích dvou let zaměstnanci výkonné moci. Pro každé přezkoumání žádosti vybere předseda senátu zvláštního advokáta, který je porotě nápomocen, viz oddíl 201.8 písm. a) nařízení AG.

349 Oddíl 201.8 písm. c) a 201.11 nařízení AG.

komise DPRC je dobře informována o všech relevantních právních a skutkových otázkách[350] . Za účelem dalšího informování o svém stanovisku k žádosti o přezkum podané k výboru DPRC jednotlivcem si může zvláštní zástupce vyžádat informace od stěžovatele prostřednictvím písemných otázek[351] .

(181) DPRC přezkoumává rozhodnutí učiněná ODNI CLPO (jak pokud jde o to, zda došlo k porušení platných právních předpisů USA, tak pokud jde o vhodnou nápravu), a to minimálně na základě záznamu o šetření ODNI CLPO, jakož i veškerých informací a podání poskytnutých stěžovatelem, zvláštním zástupcem nebo zpravodajskou agenturou[352] . Komise DPRC má přístup ke všem informacím potřebným k provedení přezkumu, které může získat prostřednictvím ODNI CLPO (komise může např. požádat CLPO o doplnění jeho záznamu o další informace nebo skutková zjištění, pokud je to pro provedení přezkumu nezbytné)[353] .

(182) Při uzavírání přezkumu může DPRC (1) rozhodnout, že neexistují důkazy, které by naznačovaly, že došlo k činnostem signálového zpravodajství zahrnujícím osobní údaje stěžovatele, (2) rozhodnout, že zjištění ODNI CLPO byla právně správná a podložená podstatnými důkazy, nebo (3) pokud DPRC nesouhlasí se zjištěními ODNI CLPO (zda došlo k porušení platných právních předpisů USA nebo k odpovídající nápravě), vydat vlastní zjištění[354] .

(183) Ve všech případech přijímá výbor DPRC písemné rozhodnutí většinou hlasů. V případě, že přezkum odhalí porušení platných pravidel, v rozhodnutí se uvedou veškerá vhodná nápravná opatření, která zahrnují vymazání nezákonně shromážděných údajů, vymazání výsledků nevhodně provedených dotazů, omezení přístupu k zákonně shromážděným údajům na příslušně vyškolený personál nebo stažení zpravodajských zpráv obsahujících údaje získané bez zákonného povolení nebo které byly nezákonně šířeny[355] . Rozhodnutí výboru DPRC je závazné, pokud jde o stížnost, která mu byla předložena[356] . Kromě toho, pokud přezkum odhalí porušení jakéhokoli orgánu podléhajícího dohledu FISC, musí DPRC rovněž předložit utajovanou zprávu asistentovi generálního prokurátora pro národní bezpečnost, který je následně povinen oznámit nedodržení předpisů FISC, který může přijmout další donucovací opatření (v souladu s postupem popsaným v 165. až 166. bodě odůvodnění)[357] .

(184) Každé rozhodnutí komise DPRC je předáno ODNI CLPO[358] . V případech, kdy přezkum výboru DPRC byl zahájen na základě žádosti stěžovatele, je stěžovatel prostřednictvím vnitrostátního orgánu vyrozuměn o tom, že výbor DPRC dokončil přezkum a že "přezkum buď nezjistil žádné zahrnuté porušení, nebo že výbor DPRC

---

350 Oddíl 3 písm. d) bod i) písm. C EO 14086 a oddíl 201.8 písm. e) nařízení AG. Zvláštní advokát nevystupuje jako zástupce stěžovatele ani s ním nemá vztah advokáta a klienta.

351 Viz oddíl 201.8 písm. d) bod e) nařízení AG. Takové dotazy nejprve přezkoumá OPCL po konzultaci s příslušnou složkou zpravodajské komunity s cílem identifikovat a vyloučit jakékoli utajované nebo důvěrné či chráněné informace, než je předá stěžovateli. Další informace, které zvláštní zástupce obdrží v reakci na takové otázky, jsou zahrnuty do podání zvláštního zástupce pro DPRC.

352 Oddíl 3 písm. d) bod i) písm. d) EO 14086.

353 Oddíl 3 písm. d) bod iii) EO 14086 a oddíl 201.9 písm. b) nařízení AG.

354 Oddíl 3 písm. d) bod i) písm. e) EO 14086 a oddíl 201.9 písm. c) až e) nařízení AG. Pokud jde o definici "vhodné nápravy", viz oddíl 4 písm. a) EO 14086.

355 Oddíl 4 písm. a) EO 14086.

356 Oddíl 3 písm. d) bod ii) EO 14086 a oddíl 201.9 písm. g) nařízení AG.

357 Oddíl 3 písm. d) bod i) písm. f) EO 14086 a oddíl 201.9 písm. i) nařízení AG.

358 Oddíl 201.9 písm. h) nařízení AG.

vydala rozhodnutí, které vyžaduje odpovídající nápravu"[359] . Úřad pro ochranu soukromí a občanských svobod ministerstva spravedlnosti vede záznamy o všech informacích přezkoumávaných výborem DPRC a o všech vydaných rozhodnutích, které jsou k dispozici k posouzení jako nezávazný precedens pro budoucí výbory DPRC[360] .

(185) DoC je rovněž povinna vést záznamy o každém stěžovateli, který podal stížnost[361] . V zájmu zvýšení transparentnosti musí DoC nejméně jednou za pět let kontaktovat příslušné zpravodajské agentury, aby ověřil, zda byly informace týkající se přezkumu provedeného DPRC odtajněny[362] . Pokud tomu tak je, bude dotyčná osoba informována o tom, že tyto informace mohou být k dispozici podle platných právních předpisů (tj. že může požádat o přístup k nim podle zákona o svobodném přístupu k informacím, viz 191. bod odůvodnění).

(186) Správné fungování tohoto mechanismu nápravy bude podléhat pravidelnému a nezávislému hodnocení. Přesněji řečeno, podle EO 14086 podléhá fungování mechanismu nápravy každoročnímu přezkumu ze strany PCLOB, nezávislého orgánu (viz 159. bod odůvodnění)[363] . V rámci tohoto přezkumu bude PCLOB posuzovat, zda ODNI CLPO a DPRC vyřizovaly stížnosti včas, zda získaly plný přístup k potřebným informacím, zda byly v procesu přezkumu řádně zohledněny podstatné záruky podle EO 14086 a zda zpravodajské společenství plně dodržovalo rozhodnutí ODNI CLPO a DPRC. PCLOB vypracuje zprávu o výsledku svého přezkumu určenou prezidentovi, generálnímu prokurátorovi, řediteli národních zpravodajských služeb, vedoucím zpravodajských agentur, ODNI CLPO a výborům Kongresu pro zpravodajské služby, která bude rovněž zveřejněna v neutajované verzi - a následně bude podkladem pro pravidelný přezkum fungování tohoto rozhodnutí, který bude provádět Komise. Generální prokurátor, ředitel Národního zpravodajství, ODNI CLPO a vedoucí zpravodajských agentur jsou povinni provést nebo jinak řešit všechna doporučení obsažená v těchto zprávách. Kromě toho bude PCLOB každoročně vydávat veřejné osvědčení o tom, zda mechanismus nápravy vyřizuje stížnosti v souladu s požadavky EO 14086.

(187) Kromě zvláštního mechanismu nápravy zřízeného podle EO 14086 jsou k dispozici i možnosti nápravy před běžnými soudy USA[364] .

(188) FISA a související zákon zejména umožňují jednotlivcům podat občanskoprávní žalobu na Spojené státy o náhradu škody v penězích, pokud byly informace o nich nezákonně a úmyslně použity nebo zveřejněny[365] ; žalovat USA.

359 Oddíl 3 písm. d) bod i) bod H EO 14086 a oddíl 201.9 písm. h) nařízení AG.

360 Oddíl 201.9 písm. j) zemědělského nařízení.

361 Oddíl 3 písm. d) bod v) bod A EO 14086.

362 Oddíl 3 písm. d) bod v) EO 14086.

363 Oddíl 3 písm. e) EO 14086. Viz také https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.

364 Přístup k těmto cestám je podmíněn prokázáním "stání". Tento standard, který se vztahuje na každého jednotlivce bez ohledu na státní příslušnost, vychází z požadavku "případu nebo sporu" podle článku III Ústavy USA. Podle Nejvyššího soudu to vyžaduje, aby (1) jednotlivec utrpěl "skutečnou újmu" (tj. újmu právem chráněného zájmu, která je konkrétní a specifikovaná a skutečná nebo bezprostředně hrozící), (2) existovala příčinná souvislost mezi újmou a jednáním, které je napadeno u soudu, a (3) je pravděpodobné, nikoli spekulativní, že příznivé rozhodnutí soudu bude řešit tuto újmu (viz *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992)).

365 18 U.S.C. § 2712.

vládní úředníci jednající v osobním postavení o náhradu škody v penězích[366] ; a napadnout zákonnost sledování (a usilovat o potlačení informací) v případě, že vláda USA hodlá použít nebo zveřejnit jakékoli informace získané nebo získané z elektronického sledování proti jednotlivci v soudním nebo správním řízení v USA[367] . Obecněji řečeno, pokud vláda hodlá použít informace získané během zpravodajských operací proti podezřelému v trestním řízení, ústavní a zákonné požadavky[368] ukládají povinnost zveřejnit určité informace, aby obžalovaný mohl napadnout zákonnost shromažďování a použití důkazů vládou.

(189) Kromě toho existuje několik specifických možností, jak se domáhat právní ochrany proti vládním úředníkům v případě nezákonného přístupu vlády k osobním údajům nebo jejich používání, a to i pro údajné účely národní bezpečnosti (tj. zákon o počítačových podvodech a zneužívání počítačů[369] ; zákon o ochraně soukromí v oblasti elektronických komunikací[370] ; a zákon o právu na finanční soukromí[371]). Všechny tyto právní žaloby se týkají konkrétních údajů, cílů a/nebo typů přístupu (např. vzdálený přístup k počítači přes internet) a jsou k dispozici za určitých podmínek (např. úmyslné/úmyslné jednání, jednání mimo úřední postavení, vzniklá škoda).

(190) Obecnější možnost nápravy nabízí APA[372] , podle níž "každá osoba, která utrpěla právní újmu v důsledku činnosti agentury nebo která byla činností agentury nepříznivě dotčena nebo poškozena", je oprávněna požádat o soudní přezkum[373] . To zahrnuje možnost požádat soud, aby "považoval za nezákonné a zrušil opatření, zjištění a závěry agentury, které byly shledány [...] svévolnými, rozmarnými, zneužitím pravomoci nebo jinak nebyly v souladu se zákonem"[374] . Například v roce 2015 rozhodl federální odvolací soud na základě žaloby APA, že hromadné shromažďování metadat o telefonních hovorech vládou USA nebylo povoleno článkem 501 FISA[375] .

(191) A konečně, kromě opravných prostředků uvedených v 168.-190. bodě odůvodnění má každá fyzická osoba právo požádat o přístup k existujícím záznamům federální agentury podle zákona FOIA, včetně případů, kdy tyto záznamy obsahují osobní údaje fyzické osoby[376] . Získání takového přístupu může rovněž usnadnit zahájení řízení před obecnými soudy, a to i na podporu prokázání aktivní legitimace. Agentury mohou odepřít přístup k informacím, které spadají pod určité vyjmenované výjimky, včetně přístupu k utajovaným informacím o národní bezpečnosti a informacím týkajícím se vyšetřování orgánů činných v trestním řízení[377] , ale stěžovatelé, kteří

---

366 50 U.S.C. § 1810.

367 50 U.S.C. § 1806.

368 *Viz Brady v. Maryland,* 373 U.S. 83 (1963) a Jencksův zákon, 18 U.S.C. § 3500.

369 18 U.S.C. § 1030.

370 18 U.S.C. §§ 2701-2712.

371 12 U.S.C. § 3417.

372 5 U.S.C. § 702.

373 Obecně platí, že soudnímu přezkumu podléhá pouze "konečné" opatření agentury - nikoli "předběžné, procesní nebo mezitímní" opatření agentury. Viz 5 U.S.C. § 704.

374 5 U.S.C. § 706 ODST. 2 PÍSM. A).

375 *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015), Program hromadného shromažďování telefonních hovorů napadený v těchto případech byl ukončen zákonem USA FREEDOM Act v roce 2015.

376 5 U.S.C. § 552. Podobné zákony existují i na úrovni jednotlivých států.

377 V takovém případě obdrží osoba obvykle pouze standardní odpověď, v níž agentura odmítne potvrdit nebo vyvrátit existenci jakýchkoli záznamů. Viz *ACLU* v. *CIA*, 710 F.3d 422 (D.C. Cir. 2014).

jsou s odpovědí nespokojeni, mají možnost ji napadnout správní a následně soudní cestou (u federálních soudů)[378] .

(192) Z výše uvedeného vyplývá, že pokud donucovací orgány USA a orgány národní bezpečnosti přistupují k osobním údajům, které spadají do oblasti působnosti tohoto rozhodnutí, řídí se tento přístup právním rámcem, který stanoví podmínky, za nichž lze přístup uskutečnit, a zajišťuje, že přístup k údajům a jejich další použití je omezeno na to, co je nezbytné a přiměřené sledovanému cíli veřejného zájmu. Těchto záruk se mohou dovolávat fyzické osoby, které mají účinné právo na nápravu.

4. ZÁVĚR

(193) Komise se domnívá, že Spojené státy - prostřednictvím zásad vydaných americkou DoC - zajišťují úroveň ochrany osobních údajů předávaných z Unie certifikovaným organizacím ve Spojených státech podle rámce EU a USA pro ochranu osobních údajů, která je v zásadě rovnocenná úrovni zaručené nařízením (EU) 2016/679.

(194) Komise se navíc domnívá, že účinné uplatňování zásad je zaručeno povinnou transparentností a správou DPF ze strany DoC. Kromě toho mechanismy dohledu a opravné prostředky v právu USA jako celek umožňují, aby bylo porušení pravidel ochrany údajů v praxi zjištěno a potrestáno, a nabízejí subjektu údajů právní prostředky k získání přístupu k osobním údajům, které se ho týkají, a případně k opravě nebo výmazu těchto údajů.

(195) Na základě dostupných informací o právním řádu USA, včetně informací obsažených v přílohách VI a VII, se Komise domnívá, že jakýkoli zásah orgánů veřejné moci USA do základních práv fyzických osob, jejichž osobní údaje jsou předávány z Unie do Spojených států podle rámce EU a USA pro ochranu soukromí, bude ve veřejném zájmu, zejména pro účely vymáhání trestního práva a národní bezpečnosti, omezen na to, co je nezbytně nutné k dosažení daného legitimního cíle, a že proti takovému zásahu existuje účinná právní ochrana. S ohledem na výše uvedená zjištění by proto mělo být rozhodnuto, že Spojené státy zajišťují odpovídající úroveň ochrany ve smyslu článku 45 nařízení (EU) 2016/679, vykládaného s ohledem na Listinu základních práv Evropské unie, pro osobní údaje předávané z Evropské unie organizacím certifikovaným podle rámce EU a USA pro ochranu osobních údajů.

(196) Vzhledem k tomu, že omezení, ochranná opatření a mechanismus nápravy stanovené v EO 14086 jsou základními prvky právního rámce USA, na němž je založeno posouzení Komise, je vstup tohoto rozhodnutí v platnost podmíněn přijetím aktualizovaných politik a postupů k provedení EO 14086 všemi zpravodajskými agenturami USA a určením Unie jako způsobilé organizace pro účely mechanismu nápravy.

5. ÚČINKY TOHOTO ROZHODNUTÍ A OPATŘENÍ ORGÁNŮ PRO OCHRANU ÚDAJŮ

(197) Členské státy a jejich orgány jsou povinny přijmout opatření nezbytná k dodržení aktů orgánů Unie, neboť se předpokládá, že tyto akty jsou zákonné a v souladu s právními předpisy.

---

[378] Soud rozhoduje de novo o tom, zda jsou záznamy zadržovány oprávněně, a může vládu přimět, aby k nim poskytla přístup (5 U.S.C. § 552(a)(4)(B)).

proto vyvolávají právní účinky, dokud nejsou odvolány, zrušeny v rámci žaloby na neplatnost nebo prohlášeny za neplatné na základě žádosti o rozhodnutí o předběžné otázce nebo námitky protiprávnosti.

(198) Rozhodnutí Komise o přiměřenosti přijaté podle čl. 45 odst. 3 nařízení (EU) 2016/679 je proto závazné pro všechny orgány členských států, kterým je určeno, včetně jejich nezávislých dozorových úřadů. Zejména předávání údajů od správce nebo zpracovatele v Unii certifikovaným organizacím ve Spojených státech může probíhat bez nutnosti získat jakékoli další povolení.

(199) Je třeba připomenout, že podle čl. 58 odst. 5 nařízení (EU) 2016/679 a jak vysvětlil Soudní dvůr v rozsudku ve věci *Schrems*[379] , pokud vnitrostátní orgán pro ochranu údajů zpochybní, a to i na základě stížnosti, slučitelnost rozhodnutí Komise o odpovídající ochraně se základními právy jednotlivce na soukromí a ochranu údajů, musí mu vnitrostátní právo poskytnout právní prostředek, aby mohl tyto námitky předložit vnitrostátnímu soudu, který může být požádán o předložení předběžné otázky Soudnímu dvoru[380] .

6. SLEDOVÁNÍ A PŘEZKUM TOHOTO ROZHODNUTÍ

(200) Podle judikatury Soudního dvora[381] a jak je uznáno v čl. 45 odst. 4 nařízení (EU) 2016/679, by Komise měla po přijetí rozhodnutí o odpovídající ochraně průběžně sledovat příslušný vývoj ve třetí zemi, aby posoudila, zda třetí země stále zajišťuje v zásadě rovnocennou úroveň ochrany. Taková kontrola je v každém případě nutná, pokud Komise obdrží informace, které v tomto ohledu vzbuzují oprávněné pochybnosti.

(201) Komise by proto měla průběžně sledovat situaci ve Spojených státech, pokud jde o právní rámec a skutečnou praxi zpracování osobních údajů, jak je posuzováno v tomto rozhodnutí. Pro usnadnění tohoto procesu by měly orgány Spojených států neprodleně informovat Komisi o podstatném vývoji v této oblasti.
právního řádu USA, které mají dopad na právní rámec, jenž je předmětem tohoto rozhodnutí, jakož i na jakýkoli vývoj postupů souvisejících se zpracováním osobních údajů posuzovaných v tomto rozhodnutí, a to jak pokud jde o zpracování osobních údajů certifikovanými organizacemi ve Spojených státech, tak o omezení a záruky platné pro přístup orgánů veřejné moci k osobním údajům.

(202) Aby Komise mohla účinně vykonávat svou kontrolní funkci, měly by ji členské státy informovat o všech příslušných opatřeních přijatých vnitrostátními orgány pro ochranu údajů, zejména pokud jde o dotazy nebo stížnosti subjektů údajů z Unie týkající se předávání osobních údajů z Unie certifikovaným organizacím ve Spojených státech. Komise by měla být rovněž informována o jakýchkoli náznakách, že opatření orgánů veřejné moci Spojených států odpovědných za prevenci, vyšetřování, odhalování nebo stíhání trestných činů nebo za národní bezpečnost, včetně všech orgánů dohledu, nezajišťují požadovanou úroveň ochrany.

---

379 *Schrems*, bod 65.

380 *Schrems*, bod 65: "Je povinností vnitrostátního zákonodárce stanovit právní prostředky, které umožní dotčenému vnitrostátnímu orgánu dozoru předložit námitky, které považuje za důvodné, vnitrostátním soudům, aby mohly, pokud sdílejí jeho pochybnosti o platnosti rozhodnutí Komise, podat žádost o rozhodnutí o předběžné otázce za účelem přezkoumání platnosti tohoto rozhodnutí."

381 *Schrems*, bod 76.

(203) V souladu s čl. 45 odst. 3 nařízení (EU) 2016/679[382] by Komise po přijetí tohoto rozhodnutí měla pravidelně přezkoumávat, zda jsou zjištění týkající se přiměřenosti úrovně ochrany zajištěné Spojenými státy v rámci DPF mezi EU a USA stále věcně a právně odůvodněná. Vzhledem k tomu, že zejména EO 14086 a nařízení o AG vyžadují vytvoření nových mechanismů a zavedení nových ochranných opatření, mělo by být toto rozhodnutí podrobeno prvnímu přezkumu do jednoho roku od jeho vstupu v platnost, aby se ověřilo, zda byly všechny příslušné prvky plně provedeny a zda v praxi účinně fungují. Po tomto prvním přezkumu a v závislosti na jeho výsledku rozhodne Komise v úzké konzultaci s výborem zřízeným podle čl. 93 odst. 1 nařízení (EU) 2016/679 o periodicitě budoucích přezkumů. V každém případě by se následné přezkumy měly konat nejméně jednou za čtyři roky[383] .

(204) Za účelem provedení přezkumů by se Komise měla setkat s DoC, FTC a DoT, případně za účasti dalších útvarů a agentur zapojených do provádění DPF EU a USA, a v záležitostech týkajících se přístupu vlády k údajům také se zástupci DoJ, ODNI (včetně CLPO), dalších složek zpravodajského společenství, DPRC a zvláštních advokátů. Účast na tomto zasedání by měla být otevřena zástupcům členů Evropského sboru pro ochranu osobních údajů.

(205) Přezkumy by se měly týkat všech aspektů fungování tohoto rozhodnutí, a zejména uplatňování a provádění zásad, přičemž zvláštní pozornost by měla být věnována ochraně poskytované v případě dalšího předávání, vývoji příslušné judikatury, účinnosti výkonu individuálních práv, monitorování a prosazování dodržování zásad, jakož i omezením a zárukám s ohledem na přístup vlády, včetně účinnosti mechanismů dohledu a opravných prostředků.

(206) Na základě tohoto přezkumu by Komise měla vypracovat veřejnou zprávu, kterou předloží Evropskému parlamentu a Radě.

7. POZASTAVENÍ, ZRUŠENÍ NEBO ZMĚNA TOHOTO ROZHODNUTÍ

(207) Pokud dostupné informace, zejména informace vyplývající z monitorování tohoto rozhodnutí nebo poskytnuté orgány USA nebo členských států, odhalí, že úroveň ochrany poskytovaná údajům předávaným podle tohoto rozhodnutí již nemusí být dostatečná, měla by o tom Komise neprodleně informovat příslušné orgány USA a požádat je, aby ve stanovené přiměřené lhůtě přijaly vhodná opatření.

(208) Pokud po uplynutí této stanovené lhůty příslušné orgány USA tato opatření nepřijmou nebo jinak uspokojivě neprokáží, že toto rozhodnutí je i nadále založeno na odpovídající úrovni ochrany, zahájí Komise postup podle čl. 93 odst. 2 nařízení (EU) 2016/679 s cílem částečně nebo zcela pozastavit nebo zrušit toto rozhodnutí.

---

382 Podle čl. 45 odst. 3 nařízení (EU) 2016/679 "[p]rováděcí akt stanoví mechanismus pravidelného přezkumu, [...] který zohlední veškerý relevantní vývoj ve třetí zemi nebo mezinárodní organizaci.".

383 Čl. 45 odst. 3 nařízení (EU) 2016/679 stanoví, že pravidelný přezkum se musí konat "nejméně jednou za čtyři roky". Viz také Evropský sbor pro ochranu osobních údajů, Adequacy Referential, WP 254 rev. 01.

(209) Případně Komise zahájí tento postup s cílem změnit rozhodnutí, zejména tím, že předávání údajů podmíní dalšími podmínkami nebo omezí rozsah zjištění přiměřenosti pouze na předávání údajů, u nichž je i nadále zajištěna odpovídající úroveň ochrany.

(210) Komise by měla zejména zahájit postup pozastavení nebo zrušení v případě:

(a) náznaky, že organizace, které obdržely osobní údaje od Unie podle tohoto rozhodnutí, nedodržují zásady a že příslušné orgány dohledu a prosazování toto nedodržování účinně neřeší;

(b) náznaky, že orgány USA nedodržují platné podmínky a omezení pro přístup orgánů veřejné moci USA k osobním údajům předávaným v rámci DPF mezi EU a USA pro účely vymáhání práva a národní bezpečnosti; nebo

(c) neúčinné řešení stížností subjektů údajů z Unie, včetně stížností ze strany ODNI CLPO a/nebo DPRC.

(211) Komise by rovněž měla zvážit zahájení postupu vedoucího ke změně, pozastavení nebo zrušení tohoto rozhodnutí, pokud příslušné orgány USA neposkytnou informace nebo vysvětlení nezbytné pro posouzení úrovně ochrany poskytované osobním údajům předávaným z Unie do Spojených států nebo pokud jde o soulad s tímto rozhodnutím. V tomto ohledu by Komise měla zohlednit, do jaké míry lze příslušné informace získat z jiných zdrojů.

(212) V řádně odůvodněných naléhavých případech, například pokud by došlo ke změně nařízení EO 14086 nebo nařízení AG způsobem, který by narušil úroveň ochrany popsanou v tomto rozhodnutí, využije Komise možnosti přijmout v souladu s postupem uvedeným v čl. 93 odst. 3 nařízení (EU) 2016/679 okamžitě použitelné prováděcí akty, kterými se pozastavuje, zrušuje nebo mění toto rozhodnutí.

8. ZÁVĚREČNÉ ÚVAHY

(213) [PLACEHOLDER pro odkaz na stanovisko Evropského sboru pro ochranu osobních údajů]

(214) [PLACEHOLDER pro odkaz na usnesení Evropského parlamentu]

(215) [MÍSTO pro odkaz na stanovisko výboru zřízeného podle čl. 93 odst. 1 nařízení (EU) 2016/679].

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Pro účely článku 45 nařízení (EU) 2016/679 Spojené státy zajišťují odpovídající úroveň ochrany osobních údajů předávaných z Unie organizacím ve Spojených státech, které jsou uvedeny na "Rámcovém seznamu ochrany osobních údajů", který vede a zveřejňuje Ministerstvo obchodu USA v souladu s oddílem I.3 přílohy I.

Článek 2

Kdykoli příslušné orgány v členských státech v zájmu ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů uplatní své pravomoci podle článku 58 nařízení (EU) 2016/679, pokud jde o předávání údajů uvedené v článku 1 tohoto rozhodnutí, dotčený členský stát o tom neprodleně informuje Komisi.

Článek 3

1. Komise průběžně sleduje uplatňování právního rámce, který je předmětem tohoto rozhodnutí, včetně podmínek, za nichž se provádí další předávání, vykonávají se individuální práva a orgány veřejné moci USA mají přístup k údajům předávaným na základě tohoto rozhodnutí, s cílem posoudit, zda Spojené státy nadále zajišťují odpovídající úroveň ochrany podle článku 1.
2. Členské státy a Komise se budou vzájemně informovat o případech, kdy se ukáže, že orgány Spojených států, které mají zákonnou pravomoc prosazovat dodržování zásad stanovených v příloze I, nezajišťují účinné mechanismy odhalování a dohledu, které by umožnily odhalit a potrestat porušení zásad stanovených v příloze I v praxi.
3. Členské státy a Komise se budou vzájemně informovat o jakýchkoli náznakách, že zásahy orgánů veřejné moci USA odpovědných za prosazování národní bezpečnosti, prosazování práva nebo jiných veřejných zájmů do práva fyzických osob na ochranu jejich osobních údajů překračují rámec toho, co je nezbytné a přiměřené, a/nebo že proti těmto zásahům neexistuje účinná právní ochrana.
4. Po uplynutí jednoho roku ode dne oznámení tohoto rozhodnutí členským státům a následně nejméně každé čtyři roky Komise vyhodnotí zjištění uvedené v čl. 1 odst. 1 na základě všech dostupných informací, včetně informací získaných v rámci přezkumu provedeného společně s příslušnými orgány Spojených států.
5. Pokud má Komise poznatky, že odpovídající úroveň ochrany již není zajištěna, informuje o tom příslušné orgány USA. V případě potřeby rozhodne o pozastavení, změně nebo zrušení tohoto rozhodnutí nebo o omezení jeho působnosti v souladu s čl. 45 odst. 5 nařízení (EU) 2016/679. Komise může takové rozhodnutí přijmout také v případě, že jí nedostatečná spolupráce vlády USA brání určit, zda Spojené státy nadále zajišťují odpovídající úroveň ochrany.

Článek 4

Toto rozhodnutí je určeno členským státům. V

Bruselu,

Za Komisi Didier
REYNDERS člen Komise

EVROPSKÁ KOMISE

Brusel, XXX [...](2022)
XXX návrh

PŘÍLOHY 1 až 7

PŘÍLOHY

na

Prováděcí rozhodnutí Komise

podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o odpovídající úrovni ochrany osobních údajů podle rámce EU a USA pro ochranu osobních údajů.

PŘÍLOHA I

RÁMCOVÉ ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ MEZI EU A USA VYDANÉ MINISTERSTVEM OBCHODU USA

I. PŘEHLED

1. Spojené státy a Evropská unie (dále jen "EU") sice sdílejí závazek posílit ochranu soukromí, právní stát a uznat význam transatlantických toků dat pro naše občany, ekonomiky a společnosti, ale Spojené státy k ochraně soukromí přistupují jinak než EU. Spojené státy používají sektorový přístup, který se opírá o kombinaci právních předpisů, regulace a samoregulace. Ministerstvo obchodu USA (dále jen "ministerstvo") vydává rámcové zásady ochrany osobních údajů mezi EU a USA, včetně doplňkových zásad (dále společně jen "zásady") a přílohy I zásad (dále jen "příloha I"), na základě své zákonné pravomoci podporovat, propagovat a rozvíjet mezinárodní obchod (15 U.S.C. § 1512). Zásady byly vypracovány po konzultaci s Evropskou komisí (dále jen "Komise"), průmyslem a dalšími zúčastněnými stranami s cílem usnadnit obchod mezi Spojenými státy a EU. Zásady, které jsou klíčovou součástí rámce EU a USA pro ochranu osobních údajů ("EU-U.S. DPF"), poskytují organizacím ve Spojených státech spolehlivý mechanismus pro předávání osobních údajů z EU do Spojených států a zároveň zajišťují, aby subjekty údajů v EU nadále využívaly účinných záruk a ochrany, jak je vyžadováno evropskými právními předpisy, pokud jde o zpracování jejich osobních údajů při jejich předávání do zemí mimo EU. Zásady jsou určeny výhradně způsobilým organizacím ve Spojených státech, které přijímají osobní údaje z EU za účelem splnění podmínek pro uplatnění DPF mezi EU a USA, a tedy pro využití rozhodnutí Komise o odpovídající ochraně.[1] Zásady nemají vliv na uplatňování nařízení (EU) 2016/679 (dále jen "obecné nařízení o ochraně osobních údajů" nebo "GDPR")[2] , které se vztahuje na zpracování osobních údajů v členských státech EU. Zásady rovněž neomezují povinnosti týkající se ochrany osobních údajů, které jinak platí podle práva USA.

2. Aby se organizace mohla při předávání osobních údajů z EU spoléhat na DPF EU - USA, musí ministerstvu (nebo jím pověřené osobě) sama potvrdit, že dodržuje zásady. Zatímco rozhodnutí organizací vstoupit takto do DPF EU a USA je zcela dobrovolné, účinné dodržování zásad je povinné: organizace, které se samy osvědčí ministerstvu a veřejně prohlásí, že se zavázaly dodržovat zásady, musí zásady plně dodržovat. Aby organizace mohla vstoupit do DPF EU a USA, musí a) být

[1] Za předpokladu, že se rozhodnutí Komise o přiměřenosti ochrany poskytované rámcem pro ochranu údajů mezi EU a USA vztahuje na Island, Lichtenštejnsko a Norsko, bude se rámec pro ochranu údajů mezi EU a USA vztahovat jak na EU, tak na tyto tři země. Proto budou odkazy na EU a její členské státy chápány jako odkazy zahrnující Island, Lichtenštejnsko a Norsko.

[2] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016, kterým se mění a doplňuje nařízení (EU) 2016/679 (Úř. věst.
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).

podléhat vyšetřovacím a donucovacím pravomocem Federální obchodní komise (dále jen "FTC"), Ministerstva dopravy USA (dále jen "DOT") nebo jiného statutárního orgánu, který účinně zajistí dodržování Zásad *(v budoucnu mohou být jako příloha připojeny další statutární orgány USA uznané EU)*; b) veřejně prohlásit svůj závazek dodržovat Zásady; c) veřejně zveřejnit své zásady ochrany osobních údajů v souladu s těmito Zásadami; a d) plně je provádět[3] . Nedodržení zásad ze strany organizace může být vymáháno FTC podle oddílu 5 zákona o Federální obchodní komisi (FTC), který zakazuje nekalé nebo klamavé jednání v obchodě nebo při ovlivňování obchodu (15 U.S.C. § 45); ministerstvem dopravy podle 49 U.S.C. § 41712, který zakazuje dopravci nebo zprostředkovateli prodeje letenek nekalé nebo klamavé praktiky v letecké dopravě nebo při prodeji letecké dopravy; nebo podle jiných zákonů nebo předpisů, které takové jednání zakazují.

3. Ministerstvo bude vést a zpřístupňovat veřejnosti autoritativní seznam amerických organizací, které se samy ministerstvu osvědčily a prohlásily, že se zavázaly dodržovat zásady (dále jen "seznam rámce ochrany osobních údajů"). Výhody DPF EU a USA jsou zajištěny ode dne, kdy ministerstvo zařadí organizaci na seznam rámce ochrany osobních údajů. Ministerstvo vyškrtne ze Seznamu rámcových zásad ochrany osobních údajů ty organizace, které dobrovolně odstoupí ze Seznamu EU.
USA nebo nedokončí každoroční recertifikaci ministerstvu; tyto organizace musí buď nadále uplatňovat zásady na osobní údaje, které obdržely v rámci DPF EU - USA, a každoročně potvrdit ministerstvu svůj závazek tak činit (*tj. po dobu, po* kterou tyto informace uchovávají), nebo zajistit "přiměřenou" ochranu informací jiným povoleným způsobem (například pomocí smlouvy, která plně odráží požadavky příslušných standardních smluvních doložek přijatých Komisí), nebo informace vrátit či vymazat. Ministerstvo rovněž vyřadí ze seznamu Rámce pro ochranu osobních údajů ty organizace, které trvale nedodržují zásady; tyto organizace musí vrátit nebo vymazat osobní údaje, které obdržely v rámci Rámce pro ochranu osobních údajů mezi EU a USA. Vyškrtnutí organizace ze seznamu Rámce ochrany soukromí údajů znamená, že již nemá nárok využívat rozhodnutí Komise o odpovídající ochraně osobních údajů, aby mohla přijímat osobní údaje z EU.

4. Ministerstvo rovněž povede a zpřístupní veřejnosti autoritativní evidenci amerických organizací, které se dříve samy certifikovaly ministerstvu, ale které byly ze seznamu Rámce ochrany osobních údajů vyřazeny. Ministerstvo poskytne jasné upozornění, že tyto organizace nejsou účastníky Rámcového rámce ochrany soukromí EU a USA; že vyřazení ze seznamu Rámcového rámce ochrany soukromí údajů znamená, že tyto organizace nemohou tvrdit, že jsou v souladu s Rámcovým rámcem ochrany soukromí EU a USA, a musí se vyvarovat jakýchkoli prohlášení nebo zavádějících postupů, které by naznačovaly, že se účastní Rámcového rámce ochrany soukromí EU a USA; a že tyto organizace již nemají nárok využívat rozhodnutí Komise o přiměřenosti pro přijímání osobních údajů z EU. Organizace, která nadále tvrdí, že se účastní DPF EU-U.S. nebo

[3] Rámcové zásady štítu EU-USA na ochranu soukromí byly změněny na "Rámcové zásady EU-USA na ochranu soukromí". (*Viz* Doplňkové zásady pro vlastní certifikaci).

po vyřazení z rámcového seznamu pro ochranu osobních údajů učiní další nepravdivá prohlášení týkající se DPF EU a USA, může být předmětem donucovacích opatření ze strany FTC, ministerstva dopravy nebo jiných donucovacích orgánů.

5. Dodržování těchto zásad může být omezené: (a) v rozsahu nezbytném pro splnění soudního příkazu nebo požadavků veřejného zájmu, vymáhání práva nebo národní bezpečnosti, včetně případů, kdy zákon nebo vládní nařízení vytvářejí protichůdné povinnosti; (b) zákonem, soudním příkazem nebo nařízením vlády, které vytvářejí výslovná oprávnění, za předpokladu, že při uplatňování jakéhokoli takového oprávnění může organizace prokázat, že její nedodržování Zásad je omezeno na rozsah nezbytný pro splnění převažujících oprávněných zájmů podporovaných takovým oprávněním; nebo c) pokud je účinkem nařízení GDPR povolit výjimky nebo odchylky, za podmínek v něm stanovených, pokud se takové výjimky nebo odchylky uplatňují ve srovnatelných souvislostech. V této souvislosti zahrnují záruky v právu USA na ochranu soukromí a občanských svobod záruky požadované exekutivním příkazem 14086[4] za podmínek v něm stanovených (včetně jeho požadavků na nezbytnost a přiměřenost). V souladu s cílem posílit ochranu soukromí by organizace měly usilovat o úplné a transparentní provádění těchto zásad, včetně snahy uvést ve svých zásadách ochrany soukromí, kde se uplatní výjimky ze zásad povolených výše uvedeným písmenem b). Ze stejného důvodu se od organizací očekává, že v případech, kdy je podle Zásad a/nebo práva USA přípustná volba, zvolí vyšší ochranu, pokud je to možné.

6. Organizace jsou povinny uplatňovat zásady na všechny osobní údaje předávané na základě DPF EU a USA po jejich vstupu do DPF EU a USA. Organizace, která se rozhodne rozšířit výhody DPF EU-U.S. na osobní údaje týkající se lidských zdrojů předávané z EU za účelem použití v rámci pracovněprávního vztahu, musí tuto skutečnost uvést při sebeosvědčení ministerstvu a splnit požadavky stanovené v Doplňkových zásadách pro sebeosvědčení.

7. Na otázky výkladu a dodržování Zásad a příslušných zásad ochrany osobních údajů organizacemi, které se účastní DPF EU a USA, se vztahují právní předpisy USA, s výjimkou případů, kdy se tyto organizace zavázaly spolupracovat s orgány EU pro ochranu údajů (dále jen "orgány pro ochranu údajů"). Není-li uvedeno jinak, platí všechna ustanovení Zásad tam, kde jsou relevantní.

8. Definice:

   a. "Osobní údaje" a "osobní informace" jsou údaje o identifikované nebo identifikovatelné osobě, které spadají do působnosti GDPR, které organizace ve Spojených státech získala z EU a které jsou zaznamenány v jakékoli formě.

   b. "Zpracováním" osobních údajů se rozumí jakákoli operace nebo soubor operací s osobními údaji, které jsou prováděny automatizovaně nebo neautomatizovaně, jako je shromažďování, zaznamenávání, uspořádávání, uchovávání, přizpůsobování a další zpracování osobních údajů.

[4] Výkonný příkaz ze 7. října 2022 "Posílení záruk pro zpravodajské aktivity Spojených států v oblasti signálů".

nebo pozměňování, vyhledávání, nahlížení, používání, zveřejňování nebo šíření a vymazání nebo zničení.

c. "Správcem" se rozumí osoba nebo organizace, která sama nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.

9. Datem účinnosti Zásad a přílohy I Zásad je datum vstupu v platnost rozhodnutí Evropské komise o přiměřenosti.

II. PRINCIPY

1. UPOZORNĚNÍ

a. Organizace musí informovat jednotlivce o:

i. o své účasti v Rámci pro ochranu osobních údajů mezi EU a USA a o odkazu na tento seznam nebo jeho webovou adresu,

ii. typy shromažďovaných osobních údajů a případně americké subjekty nebo americké dceřiné společnosti organizace, které rovněž dodržují tyto zásady,

iii. svůj závazek podřídit Zásadám všechny osobní údaje získané z EU na základě DPF EU - USA,

iv. účely, pro které shromažďuje a používá jejich osobní údaje,

v. jak se na organizaci obrátit s případnými dotazy nebo stížnostmi, včetně příslušné instituce v EU, která může na takové dotazy nebo stížnosti reagovat,

vi. typ nebo totožnost třetích stran, kterým poskytuje osobní údaje, a účely, pro které tak činí,

vii. právo fyzických osob na přístup ke svým osobním údajům,

viii. možnosti a prostředky, které organizace nabízí jednotlivcům k omezení používání a zveřejňování jejich osobních údajů,

ix. nezávislý orgán pro řešení sporů, který je určen k řešení stížností a bezplatnému poskytnutí odpovídajícího opravného prostředku jednotlivci, a zda se jedná o: (1) komisi zřízenou orgány pro ochranu údajů, (2) poskytovatele alternativního řešení sporů se sídlem v EU nebo (3) poskytovatele alternativního řešení sporů se sídlem ve Spojených státech,

x. podléhají vyšetřovacím a donucovacím pravomocem FTC, ministerstva dopravy nebo jakéhokoli jiného oprávněného zákonného orgánu USA,

xi. možnost, aby se jednotlivec za určitých podmínek dovolával závazného rozhodčího řízení,[5]

xii. požadavek na zpřístupnění osobních údajů v reakci na zákonné žádosti orgánů veřejné moci, včetně splnění požadavků národní bezpečnosti nebo prosazování práva, a

xiii. svou odpovědnost v případech dalšího předání třetím stranám.

b. Toto oznámení musí být poskytnuto jasným a zřetelným jazykem v okamžiku, kdy jsou fyzické osoby poprvé požádány, aby organizaci poskytly osobní údaje, nebo co nejdříve poté, ale v každém případě předtím, než organizace tyto údaje použije k jinému účelu, než pro který byly původně shromážděny nebo zpracovány předávající organizací, nebo je poprvé sdělí třetí straně.

2. CHOICE

a. Organizace musí jednotlivcům nabídnout možnost volby (*tj.* odhlášení), zda jejich osobní údaje mají být (i) zpřístupněny třetí straně nebo (ii) použity k účelu, který se podstatně liší od účelu (účelů), pro který byly původně shromážděny nebo následně jednotlivci schváleny. Fyzickým osobám musí být poskytnuty jasné, zřetelné a snadno dostupné mechanismy pro uplatnění volby.

b. Odchylně od předchozího odstavce není nutné poskytnout možnost volby, pokud se zpřístupnění provádí třetí straně, která jedná jako zástupce, aby plnila úkoly jménem organizace a podle jejích pokynů. Organizace však musí se zástupcem vždy uzavřít smlouvu.

c. V případě citlivých informací (*tj.* osobních údajů uvádějících zdravotní stav, rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení, členství v odborech nebo informace uvádějící sexuální život jednotlivce) musí organizace získat výslovný souhlas (tj. opt in) od jednotlivců, pokud mají být tyto informace (i) poskytnuty třetí straně nebo (ii) použity k jinému účelu, než pro který byly původně shromážděny nebo následně schváleny jednotlivci prostřednictvím uplatnění opt in volby. Kromě toho by organizace měla považovat za citlivé všechny osobní údaje získané od třetí strany, pokud je třetí strana identifikuje a považuje za citlivé.

[5] *Viz např.* oddíl c) zásady regresu, vymáhání a odpovědnosti.

3. ODPOVĚDNOST ZA DALŠÍ PŘEDÁNÍ

a. Při předávání osobních údajů třetí straně, která vystupuje jako správce, musí organizace dodržovat zásady oznamování a volby. Organizace musí také uzavřít smlouvu se správcem, který je třetí stranou, která stanoví, že tyto údaje mohou být zpracovávány pouze pro omezené a konkrétní účely v souladu se souhlasem poskytnutým jednotlivcem a že příjemce poskytne stejnou úroveň ochrany jako Zásady a oznámí organizaci, pokud zjistí, že tuto povinnost již nemůže splnit. Smlouva musí stanovit, že v případě takového zjištění správce, který je třetí stranou, zpracování ukončí nebo podnikne jiné přiměřené a vhodné kroky k nápravě.

b. Pro předání osobních údajů třetí straně, která jedná jako zprostředkovatel, musí organizace: (i) předávat tyto údaje pouze pro omezené a konkrétní účely; (ii) ujistit se, že zprostředkovatel je povinen poskytovat alespoň stejnou úroveň ochrany soukromí, jakou vyžadují Zásady; (iii) přijmout přiměřené a vhodné kroky k zajištění toho, aby zprostředkovatel účinně zpracovával předávané osobní údaje způsobem, který je v souladu s povinnostmi organizace podle Zásad; (iv) požadovat, aby zprostředkovatel organizaci informoval, pokud zjistí, že již nemůže splnit svůj závazek poskytnout stejnou úroveň ochrany, jakou vyžadují Zásady; (v) na základě oznámení, včetně oznámení podle bodu (iv), přijmout přiměřené a vhodné kroky k zastavení a nápravě neoprávněného zpracování; a (vi) na požádání poskytnout ministerstvu shrnutí nebo reprezentativní kopii příslušných ustanovení smlouvy s tímto zprostředkovatelem o ochraně osobních údajů.

4. SECURITY

a. Organizace, které vytvářejí, uchovávají, používají nebo šíří osobní údaje, musí přijmout přiměřená a vhodná opatření na jejich ochranu před ztrátou, zneužitím a neoprávněným přístupem, zveřejněním, pozměněním a zničením, přičemž musí řádně zohlednit rizika spojená se zpracováním a povahu osobních údajů.

5. INTEGRITA DAT A OMEZENÍ ÚČELU

a. V souladu se zásadami musí být osobní údaje omezeny na informace, které jsou relevantní pro účely zpracování.[6] Organizace nesmí zpracovávat osobní údaje způsobem, který je neslučitelný s účely, pro které byly shromážděny nebo následně schváleny jednotlivcem. V rozsahu nezbytném pro tyto účely musí organizace přijmout přiměřená opatření, aby zajistila, že osobní údaje jsou spolehlivé pro zamýšlené použití, přesné, úplné,

[6] V závislosti na okolnostech mohou být příklady slučitelných účelů zpracování ty, které přiměřeně slouží vztahům se zákazníky, dodržování předpisů a právním aspektům, auditu, bezpečnosti a prevenci podvodů, zachování nebo obraně zákonných práv organizace nebo jiným účelům, které odpovídají očekávání rozumné osoby vzhledem ke kontextu shromažďování.

a proudu. Organizace musí zásady dodržovat po celou dobu, kdy tyto informace uchovává.

b. Informace mohou být uchovávány ve formě, která identifikuje nebo umožňuje identifikovat[7] jednotlivce, pouze po dobu, po kterou slouží účelu zpracování ve smyslu 5 písm. a). Tato povinnost nebrání organizacím zpracovávat osobní údaje po delší dobu po dobu a v rozsahu, v jakém takové zpracování přiměřeně slouží účelům archivace ve veřejném zájmu, publicistiky, literatury a umění, vědeckého nebo historického výzkumu a statistické analýzy. V těchto případech se na takové zpracování vztahují ostatní zásady a ustanovení DPF EU a USA. Organizace by měly při dodržování tohoto ustanovení přijmout přiměřená a vhodná opatření.

6. ACCESS

a. Fyzické osoby musí mít přístup k osobním údajům, které o nich organizace uchovává, a musí mít možnost tyto údaje opravit, změnit nebo vymazat, pokud jsou nepřesné nebo byly zpracovány v rozporu se zásadami, s výjimkou případů, kdy by zátěž nebo náklady spojené s poskytnutím přístupu byly nepřiměřené rizikům pro soukromí fyzické osoby v daném případě nebo kdy by byla porušena práva jiných osob než fyzické osoby.

7. REGRESNÍ NÁROK, VYMÁHÁNÍ A ODPOVĚDNOST

a. Účinná ochrana soukromí musí zahrnovat spolehlivé mechanismy pro zajištění dodržování zásad, opravné prostředky pro osoby, které jsou nedodržováním zásad dotčeny, a důsledky pro organizaci v případě, že zásady nejsou dodržovány. Tyto mechanismy musí zahrnovat minimálně:

i. snadno dostupné nezávislé mechanismy odvolání, pomocí nichž jsou stížnosti a spory každého jednotlivce prošetřeny a urychleně vyřešeny bez nákladů pro jednotlivce a s odkazem na Zásady a přiznána náhrada škody, pokud to stanoví platné právní předpisy nebo iniciativy soukromého sektoru;

ii. následné postupy pro ověřování, zda jsou prohlášení a ujištění organizací o jejich postupech ochrany soukromí pravdivá a zda byly postupy ochrany soukromí zavedeny tak, jak byly předloženy, a zejména s ohledem na případy nesouladu, a

iii. povinnosti k nápravě problémů vzniklých v důsledku nedodržování zásad organizacemi, které oznámily, že se jimi řídí, a důsledky pro tyto organizace.

[7] V této souvislosti platí, že pokud by vzhledem k prostředkům identifikace, které lze s přiměřenou pravděpodobností použít (mimo jiné s ohledem na náklady a dobu potřebnou k identifikaci a dostupnou technologii v době zpracování), a k formě, v níž jsou údaje uchovávány, mohla organizace nebo třetí strana, pokud by měla k údajům přístup, jednotlivce přiměřeně identifikovat, pak je tento jednotlivec "identifikovatelný".

Sankce musí být dostatečně přísné, aby bylo zajištěno jejich dodržování ze strany organizací.

b. Organizace a jejich vybrané nezávislé opravné prostředky budou neprodleně reagovat na dotazy a žádosti ministerstva o informace týkající se DPF EU a USA. Všechny organizace musí urychleně reagovat na stížnosti týkající se dodržování zásad, které jim prostřednictvím ministerstva postoupí orgány členských států EU. Organizace, které se rozhodly spolupracovat s orgány pro ochranu údajů, včetně organizací, které zpracovávají údaje o lidských zdrojích, musí v souvislosti s vyšetřováním a řešením stížností odpovídat přímo těmto orgánům.

c. Organizace jsou povinny rozhodovat nároky v rozhodčím řízení a dodržovat podmínky stanovené v příloze I za předpokladu, že se jednotlivec dovolal závazného rozhodčího řízení doručením oznámení příslušné organizaci a dodržením postupů a podmínek stanovených v příloze I.

d. V rámci dalšího předávání nese zúčastněná organizace odpovědnost za zpracování osobních údajů, které obdrží v rámci DPF EU a USA a které následně předá třetí straně jednající jejím jménem jako agent. Zúčastněná organizace zůstává odpovědná podle Zásad, pokud její zástupce zpracovává tyto osobní údaje způsobem, který není v souladu se Zásadami, ledaže by prokázala, že za událost, která vedla ke vzniku škody, není odpovědná.

e. Pokud se organizace stane předmětem soudního příkazu, který je založen na nedodržování zásad, nebo příkazu statutárního orgánu USA (např. FTC nebo DOT) uvedeného v Zásadách nebo v budoucí příloze k Zásadám, který je založen na nedodržování zásad, organizace zveřejní všechny relevantní části týkající se DPF EU a USA v jakékoli zprávě o dodržování zásad nebo hodnotící zprávě předložené soudu nebo statutárnímu orgánu USA v rozsahu, který je v souladu s požadavky na důvěrnost. Ministerstvo zřídilo zvláštní kontaktní místo pro DPF v případě jakýchkoli problémů s dodržováním předpisů ze strany zúčastněných organizací. FTC a ministerstvo dopravy budou přednostně posuzovat postoupení případů nedodržování zásad ze strany ministerstva a orgánů členských států EU a budou si včas vyměňovat informace týkající se postoupení s orgány postoupivšího státu v souladu se stávajícími omezeními důvěrnosti.

III. DOPLŇKOVÉ ZÁSADY

1. Citlivé údaje

a. Organizace nemusí získat výslovný souhlas (*tj.* opt-in) s citlivými údaji, pokud se jedná o zpracování:

i. v životně důležitém zájmu subjektu údajů nebo jiné osoby;

ii. nezbytné pro uplatnění právních nároků nebo obhajoby;

iii. nutné k poskytnutí lékařské péče nebo stanovení diagnózy;

iv. prováděné v rámci oprávněných činností nadací, sdružením nebo jiným neziskovým subjektem s politickým, filozofickým, náboženským nebo odborovým cílem a za podmínky, že se zpracování týká výhradně členů tohoto subjektu nebo osob, které s ním přicházejí pravidelně do styku v souvislosti s jeho účely, a že údaje nejsou bez souhlasu subjektů údajů zpřístupněny třetí straně;

v. nezbytné k plnění povinností organizace v oblasti pracovního práva nebo

vi. týkající se údajů, které jsou zjevně zveřejněny jednotlivcem.

2. Novinářské výjimky

a. Vzhledem k ústavní ochraně svobody tisku v USA se v případech, kdy se práva na svobodný tisk zakotvená v prvním dodatku Ústavy USA kříží se zájmy na ochranu soukromí, musí první dodatek upravovat vyvažování těchto zájmů s ohledem na činnost amerických osob nebo organizací.

b. Osobní údaje, které jsou shromážděny za účelem zveřejnění, vysílání nebo jiných forem veřejného sdělování novinářských materiálů, ať už jsou použity, nebo ne, stejně jako informace nalezené v dříve zveřejněných materiálech šířených z mediálních archivů, nepodléhají požadavkům Zásad.

3. Sekundární odpovědnost

a. Poskytovatelé internetových služeb ("ISP"), telekomunikační operátoři a další organizace nejsou podle Zásad odpovědní, pokud jménem jiné organizace pouze přenášejí, směrují, přepínají nebo ukládají do mezipaměti informace. DPF EU a USA nezakládá sekundární odpovědnost. V rozsahu, v jakém organizace působí jako pouhý kanál pro údaje předávané třetími stranami a neurčuje účely a prostředky zpracování těchto osobních údajů, by odpovědnost nenesla.

4. Provádění due diligence a auditů

a. Činnost auditorů a investičních bankéřů může zahrnovat zpracování osobních údajů bez souhlasu nebo vědomí dotyčné osoby.

jednotlivce. To je povoleno zásadami oznamování, volby a přístupu za okolností popsaných níže.

b. Veřejné akciové společnosti a společnosti v úzkém vlastnictví, včetně zúčastněných organizací, pravidelně podléhají auditům. Tyto audity, zejména ty, které se zabývají možným protiprávním jednáním, mohou být ohroženy, pokud budou předčasně zveřejněny. Podobně bude muset zúčastněná organizace, která se účastní potenciální fúze nebo převzetí, provést nebo být předmětem kontroly "due diligence". To bude často zahrnovat shromažďování a zpracování osobních údajů, například informací o vedoucích pracovnících a dalších klíčových zaměstnancích. Předčasné zveřejnění by mohlo transakci ztížit nebo dokonce porušit platné předpisy o cenných papírech. Investiční bankéři a právníci zapojení do hloubkové kontroly nebo auditoři provádějící audit mohou zpracovávat informace bez vědomí fyzické osoby pouze v rozsahu a po dobu nezbytnou ke splnění zákonných požadavků nebo požadavků veřejného zájmu a za dalších okolností, kdy by uplatnění těchto Zásad poškodilo oprávněné zájmy organizace. Mezi tyto oprávněné zájmy patří sledování dodržování zákonných povinností organizací a oprávněné účetní činnosti a potřeba zachování důvěrnosti související s případnými akvizicemi, fúzemi, společnými podniky nebo jinými podobnými transakcemi prováděnými investičními bankéři nebo auditory.

5. Úloha orgánů pro ochranu údajů

a. Organizace budou plnit svůj závazek spolupracovat s orgány pro ochranu údajů, jak je popsáno níže. V rámci DPF mezi EU a USA se americké organizace, které přijímají osobní údaje z EU, musí zavázat, že budou používat účinné mechanismy pro zajištění souladu se zásadami. Konkrétněji, jak je uvedeno v zásadě odvolání, vymáhání a odpovědnosti, zúčastněné organizace musí zajistit: (a) i) opravné prostředky pro fyzické osoby, jichž se údaje týkají; a) ii) následné postupy pro ověření, zda jsou potvrzení a tvrzení o jejich postupech v oblasti ochrany osobních údajů pravdivá; a a) iii) povinnosti k nápravě problémů vzniklých v důsledku nedodržování zásad a důsledky pro tyto organizace. Organizace může splnit písmena a) i) a a) iii) Zásad odvolatelnosti, prosazování a odpovědnosti, pokud dodržuje zde stanovené požadavky na spolupráci s orgány pro ochranu údajů.

b. Organizace se zavazuje spolupracovat s orgány pro ochranu údajů tím, že ve své autocertifikaci DPF EU - USA předložené ministerstvu prohlásí (*viz* doplňková zásada autocertifikace), že:

i. se rozhodne splnit požadavek uvedený v písmenu a) bodě i) a v písmenu a) bodě iii) zásady odvolatelnosti, vymáhání a odpovědnosti tím, že se zaváže spolupracovat s orgány pro ochranu údajů;

ii. bude spolupracovat s orgány pro ochranu údajů při vyšetřování a řešení stížností podaných na základě těchto zásad; a

iii. vyhoví všem doporučením orgánů pro ochranu údajů, pokud tyto orgány dospějí k názoru, že organizace musí přijmout konkrétní opatření k dosažení souladu se zásadami, včetně nápravných nebo kompenzačních opatření ve prospěch osob dotčených nedodržením zásad, a poskytne orgánům pro ochranu údajů písemné potvrzení, že taková opatření byla přijata.

c. Provoz panelů DPA

i. Spolupráce orgánů pro ochranu údajů bude poskytována formou informací a poradenství následujícím způsobem:

1. Poradenství orgánů pro ochranu údajů bude poskytováno prostřednictvím neformálního panelu orgánů pro ochranu údajů zřízeného na úrovni EU, který *mimo jiné* pomůže zajistit harmonizovaný a soudržný přístup.

2. Panel bude poskytovat poradenství dotčeným americkým organizacím ohledně nevyřešených stížností fyzických osob na nakládání s osobními údaji, které byly předány z EU v rámci DPF mezi EU a USA. Toto poradenství bude mít za cíl zajistit správné uplatňování Zásad a bude zahrnovat případná nápravná opatření pro dotčené osoby, která orgány pro ochranu údajů považují za vhodná.

3. Panel bude poskytovat takové poradenství v reakci na doporučení od dotčených organizací a/nebo na stížnosti obdržené přímo od jednotlivců na organizace, které se zavázaly spolupracovat s orgány pro ochranu údajů pro účely DPF EU a USA, přičemž bude tyto jednotlivce v první řadě podporovat a v případě potřeby jim pomáhat využívat interní opatření pro vyřizování stížností, která může organizace nabízet.

4. Poradenství bude vydáno až poté, co obě strany sporu dostanou přiměřenou příležitost vyjádřit se a předložit případné důkazy. Panel se bude snažit vydat radu co nejrychleji, jak to tento požadavek na řádný proces umožňuje. Obecně platí, že panel bude usilovat o poskytnutí poradenství do 60 dnů od obdržení stížnosti nebo postoupení případu, a pokud to bude možné, i rychleji.

5. Komise zveřejní výsledky posouzení stížností, které jí byly předloženy, pokud to uzná za vhodné.

6. Poskytování poradenství prostřednictvím panelu nezakládá žádnou odpovědnost panelu ani jednotlivých orgánů pro ochranu údajů.

ii. Jak bylo uvedeno výše, organizace, které se rozhodnou pro tuto možnost řešení sporů, se musí zavázat, že budou dodržovat

doporučení orgánů pro ochranu údajů. Pokud se organizace nepodřídí do 25 dnů od obdržení

a nenabídne uspokojivé vysvětlení tohoto zpoždění, komise oznámí svůj záměr buď postoupit záležitost FTC, ministerstvu dopravy nebo jinému federálnímu nebo státnímu orgánu USA, který má zákonné pravomoci k přijímání donucovacích opatření v případech podvodu nebo klamání, nebo dojde k závěru, že dohoda o spolupráci byla vážně porušena, a proto musí být považována za neplatnou. V druhém případě bude komise informovat ministerstvo, aby mohl být rámcový seznam ochrany osobních údajů řádně změněn. Jakékoli nesplnění závazku spolupracovat s orgány pro ochranu osobních údajů, jakož i nedodržení zásad, bude žalovatelné jako klamavá praktika podle oddílu 5 zákona o FTC (15 U.S.C. § 45), 49 U.S.C. § 41712 nebo jiného podobného zákona.

d. Organizace, která si přeje, aby se její výhody v rámci DPF mezi EU a USA vztahovaly na údaje o lidských zdrojích předávané z EU v souvislosti s pracovním poměrem, se musí zavázat, že bude s orgány pro ochranu údajů spolupracovat, pokud jde o tyto údaje (*viz* doplňková zásada o údajích o lidských zdrojích).

e. Organizace, které se rozhodnou pro tuto možnost, budou muset platit roční poplatek, který bude určen na pokrytí provozních nákladů panelu. Dále mohou být požádány o úhradu nezbytných nákladů na překlady, které vzniknou v souvislosti s projednáváním postoupení nebo stížností, které na ně panel podá. Výši poplatku určí ministerstvo po konzultaci s Komisí. Výběr poplatku může provádět třetí strana vybraná ministerstvem, která bude sloužit jako správce finančních prostředků vybraných pro tento účel. Oddělení bude úzce spolupracovat s Komisí a orgány pro ochranu údajů na stanovení vhodných postupů pro rozdělování finančních prostředků vybraných prostřednictvím poplatku, jakož i na dalších procesních a administrativních aspektech panelu. Oddělení a Komise se mohou dohodnout na změně četnosti výběru poplatku.

6. Vlastní certifikace

a. Výhody DPF mezi EU a USA jsou zajištěny ode dne, kdy ministerstvo zařadí organizaci na seznam rámce pro ochranu osobních údajů. Ministerstvo zařadí organizaci na rámcový seznam ochrany soukromí údajů až poté, co zjistí, že organizace předložila úplnou počáteční autocertifikaci, a vyřadí ji z tohoto seznamu, pokud dobrovolně odstoupí, nedokončí každoroční recertifikaci nebo pokud trvale nedodržuje zásady (*viz* doplňková zásada o řešení sporů a prosazování).

b. Pro prvotní vlastní certifikaci nebo následnou recertifikaci pro DPF EU - USA musí organizace pokaždé předložit ministerstvu podání vedoucího pracovníka společnosti jménem organizace.

organizace, která sama osvědčuje nebo znovu osvědčuje (podle potřeby) své dodržování zásad[8] , která obsahuje alespoň následující informace:

i. název sebecertifikující nebo re-certifikující americké organizace, jakož i název (názvy) všech jejích amerických subjektů nebo amerických dceřiných společností, které rovněž dodržují zásady, na něž se chce organizace vztahovat;

ii. popis činností organizace v souvislosti s osobními údaji, které by byly získány z EU v rámci DPF mezi EU a USA;

iii. popis příslušných zásad ochrany osobních údajů organizace, včetně:

1. pokud má organizace veřejnou webovou stránku, příslušnou webovou adresu, kde jsou zásady ochrany osobních údajů k dispozici, nebo pokud organizace nemá veřejnou webovou stránku, kde jsou zásady ochrany osobních údajů k dispozici k nahlédnutí veřejnosti; a
2. datum jeho účinnosti;

iv. kontaktní kancelář v rámci organizace pro vyřizování stížností, žádostí o přístup a jakýchkoli dalších záležitostí vyplývajících ze zásad[9] , včetně:

1. jméno (jména), pracovní zařazení (případně funkce), e-mailovou adresu (adresy) a telefonní číslo (čísla) příslušné osoby (osob) nebo příslušné kontaktní kanceláře (kanceláří) v rámci organizace a
2. příslušnou americkou poštovní adresu organizace;

v. konkrétní statutární orgán, který má pravomoc projednávat případné stížnosti na organizaci týkající se možných nekalých nebo klamavých praktik a porušení zákonů nebo předpisů upravujících ochranu soukromí (a který je uveden v Zásadách nebo v budoucí příloze Zásad);

vi. název programu na ochranu soukromí, jehož je organizace členem;

vii. způsob ověřování (*tj.* vlastní hodnocení nebo externí kontroly dodržování předpisů, včetně třetí strany, která tyto kontroly provádí);[10] a

[8] Předložení musí být provedeno prostřednictvím webových stránek ministerstva pro rámec ochrany osobních údajů osobou v rámci organizace, která je oprávněna učinit prohlášení jménem organizace a všech jejích subjektů, na které se vztahuje, ohledně dodržování zásad.

[9] Hlavní "kontaktní osoba organizace" nebo "firemní úředník organizace" nesmí být externí osobou organizace (*např.* , externí poradce nebo externí konzultant).

[10] *Viz* doplňková zásada o ověřování.

viii. příslušný nezávislý opravný mechanismus (mechanismy), který je k dispozici pro šetření nevyřešených stížností souvisejících se Zásadami.[11]

c. Pokud si organizace přeje, aby se její dávky DPF EU a USA vztahovaly na informace o lidských zdrojích předávané z EU za účelem jejich použití v rámci pracovního poměru, může tak učinit v případě, že statutární orgán uvedený v Zásadách nebo v budoucí příloze Zásad má pravomoc projednávat nároky vůči organizaci vyplývající ze zpracování informací o lidských zdrojích. Kromě toho musí organizace tuto skutečnost uvést ve svém prvním předložení autocertifikace i v každém předložení recertifikace a prohlásit, že se zavazuje spolupracovat s dotčeným orgánem nebo orgány EU v souladu s Doplňkovými zásadami pro údaje o lidských zdrojích a úlohou orgánů pro ochranu údajů (podle potřeby) a že bude dodržovat doporučení těchto orgánů. Organizace musí rovněž poskytnout odboru kopii své politiky ochrany osobních údajů v oblasti lidských zdrojů a poskytnout informace o tom, kde je tato politika ochrany osobních údajů k dispozici k nahlédnutí dotčeným zaměstnancům.

d. Ministerstvo bude vést a zveřejňovat seznam organizací, které podaly vyplněné počáteční žádosti o vlastní certifikaci, a bude tento seznam aktualizovat na základě vyplněných žádostí o roční recertifikaci a oznámení obdržených podle doplňkové zásady pro řešení sporů a prosazování práva. Takováto recertifikační podání musí být předkládána nejméně jednou ročně, jinak bude organizace ze seznamu Rámce ochrany osobních údajů vyřazena a výhody Rámce ochrany osobních údajů EU a USA již nebudou zajištěny. Všechny organizace, které ministerstvo zařadí na rámcový seznam ochrany osobních údajů, musí mít příslušné zásady ochrany osobních údajů, které jsou v souladu se zásadou oznamování, a musí v těchto zásadách ochrany osobních údajů uvést, že zásady dodržují.[12] Pokud jsou zásady ochrany osobních údajů organizace dostupné online, musí obsahovat hypertextový odkaz na internetové stránky ministerstva týkající se rámce ochrany osobních údajů a hypertextový odkaz na internetové stránky nebo formulář pro podání stížnosti na nezávislý opravný prostředek, který je k dispozici pro bezplatné prošetření nevyřešených stížností souvisejících se Zásadami pro jednotlivce.

e. Zásady se uplatňují okamžitě po vlastní certifikaci. Zúčastněné organizace, které se již dříve samy certifikovaly podle rámcových zásad štítu EU-USA na ochranu soukromí, budou muset aktualizovat své zásady ochrany osobních údajů tak, aby místo nich odkazovaly na "rámcové zásady EU a USA na ochranu osobních údajů".

[11] *Viz* doplňková zásada o řešení sporů a vymáhání práva.

[12] Organizace, která se poprvé sama certifikuje, nesmí ve své konečné verzi zásad ochrany osobních údajů uvést účast v DPF EU a USA, dokud jí ministerstvo neoznámí, že tak může učinit. Organizace musí ministerstvu poskytnout návrh politiky ochrany osobních údajů, který je v souladu se Zásadami, při předložení své první autocertifikace. Jakmile ministerstvo zjistí, že předložení počáteční autocertifikace organizace je jinak úplné, oznámí organizaci, že by měla dokončit (*např.* , případně zveřejnit) svou politiku ochrany osobních údajů, která je v souladu s DPF EU a USA. Organizace musí neprodleně informovat ministerstvo, jakmile bude příslušná politika ochrany osobních údajů dokončena, a v té době ministerstvo zařadí organizaci

na seznam rámce ochrany osobních údajů.

Tyto organizace tento odkaz uvedou co nejdříve, nejpozději však do tří měsíců od data účinnosti rámcových zásad ochrany osobních údajů mezi EU a USA.

f. Organizace musí podřídit Zásadám všechny osobní údaje získané z EU na základě DPF EU - USA. Závazek dodržovat Zásady není časově omezen ve vztahu k osobním údajům získaným během období, kdy organizace využívá výhod DPF EU a USA; její závazek znamená, že bude Zásady na tyto údaje uplatňovat po celou dobu, kdy je bude uchovávat, používat nebo zveřejňovat, a to i v případě, že následně z jakéhokoli důvodu DPF EU a USA opustí. Organizace, která si přeje z DPF EU a USA vystoupit, musí tuto skutečnost předem oznámit ministerstvu. V tomto oznámení musí rovněž uvést, jak organizace naloží s osobními údaji, které obdržela na základě DPF EU.
U.S. DPF (tj. , ponechat si údaje, vrátit je nebo je vymazat, a pokud si údaje ponechá, jaké oprávněné prostředky použije k zajištění ochrany údajů). Organizace, která vystoupí z DPF EU a USA, ale chce si tyto údaje ponechat, musí buď každoročně potvrdit ministerstvu svůj závazek nadále uplatňovat zásady na údaje, nebo zajistit "přiměřenou" ochranu údajů jiným oprávněným způsobem (například pomocí smlouvy, která plně odráží požadavky příslušných standardních smluvních doložek přijatých Komisí); v opačném případě musí organizace informace vrátit nebo vymazat.[13] Organizace, která vystoupí z FDP EU a USA, musí z příslušných zásad ochrany osobních údajů odstranit veškeré odkazy na FDP EU a USA, které naznačují, že se organizace nadále účastní FDP EU a USA a má nárok na jeho výhody.

g. Organizace, která přestane existovat jako samostatný právní subjekt v důsledku změny právní formy společnosti, například v důsledku fúze, převzetí, úpadku nebo zrušení, musí tuto skutečnost předem oznámit odboru. V oznámení by mělo být rovněž uvedeno, zda se subjekt vzniklý změnou právního postavení bude i) nadále účastnit DPF EU - USA prostřednictvím stávajícího vlastního osvědčení;
(ii) provést autocertifikaci jako nový účastník DPF EU a USA (např. *v* případě, že nový subjekt nebo přeživší subjekt již nemá existující autocertifikaci, jejímž prostřednictvím by se mohl účastnit DPF EU a USA); nebo (iii) zavést jiná ochranná opatření, jako je písemná dohoda, která zajistí trvalé uplatňování Zásad na všechny osobní údaje, které organizace obdržela v rámci DPF EU a USA a které budou uchovávány. Pokud se neuplatní ani bod i), ani bod ii), ani bod iii), musí být veškeré osobní údaje, které byly získány v rámci DPF EU-U.S., neprodleně vráceny nebo vymazány.

[13] Pokud se organizace v době vystoupení rozhodne ponechat si osobní údaje, které obdržela na základě DPF EU a USA, a každoročně potvrdí ministerstvu, že na tyto údaje nadále uplatňuje zásady, musí jednou ročně po vystoupení (tj. po uplynutí lhůty pro odstoupení od smlouvy) ministerstvu ověřit, že se na tyto údaje vztahují zásady. pokud a dokud organizace nezajistí "přiměřenou" ochranu těchto údajů jiným povoleným způsobem nebo pokud všechny tyto údaje nevrátí či nevymaže a neoznámí tento krok ministerstvu), co s těmito osobními údaji provedla, jak naloží s těmi osobními údaji, které nadále uchovává, a kdo bude sloužit jako trvalé kontaktní místo pro dotazy týkající se Zásad.

h. Pokud organizace z jakéhokoli důvodu opustí DPF EU a USA, musí odstranit všechna prohlášení, která naznačují, že se organizace nadále účastní DPF EU a USA nebo že má nárok na výhody plynoucí z DPF EU a USA.
DPF V USA. Certifikační značka EU-U.S. DPF, pokud je použita, musí být rovněž odstraněna. Jakékoli zkreslení informací o dodržování Zásad ze strany organizace může být předmětem žaloby ze strany FTC, DOT nebo jiného příslušného vládního orgánu. Zkreslená prohlášení vůči ministerstvu mohou být žalovatelná podle zákona o nepravdivých prohlášeních (18 U.S.C. § 1001).

7. Ověřování

a. Organizace musí zajistit následné postupy pro ověření, zda potvrzení a tvrzení, která učinily o svých postupech ochrany soukromí v rámci DPF EU a USA, jsou pravdivá a zda tyto postupy ochrany soukromí byly zavedeny tak, jak bylo prezentováno, a v souladu se Zásadami.

b. Aby organizace splnila požadavky na ověření podle zásady odvolání, vymáhání a odpovědnosti, musí tato osvědčení a tvrzení ověřit buď prostřednictvím vlastního hodnocení, nebo externích kontrol dodržování předpisů.

c. Pokud se organizace rozhodla pro sebehodnocení, musí toto ověření prokázat, že její zásady ochrany osobních údajů týkající se osobních údajů získaných z EU jsou přesné, komplexní, snadno dostupné, odpovídají zásadám a jsou zcela zavedeny (*tj.* jsou dodržovány). Musí rovněž uvést, že fyzické osoby jsou informovány o všech interních opatřeních pro vyřizování stížností a o nezávislém mechanismu (mechanismech), prostřednictvím kterého (kterých) mohou stížnosti podávat; že má zavedeny postupy pro školení zaměstnanců v oblasti jejich provádění a pro jejich disciplinární postih v případě jejich nedodržování; a že má zavedeny interní postupy pro pravidelné provádění objektivních přezkumů dodržování výše uvedených zásad. Prohlášení ověřující, že sebehodnocení bylo provedeno, musí být podepsáno vedoucím pracovníkem společnosti nebo jiným oprávněným zástupcem organizace alespoň jednou ročně a musí být k dispozici na žádost jednotlivců nebo v souvislosti s vyšetřováním či stížností na nedodržování předpisů.

d. Pokud se organizace rozhodla pro externí kontrolu souladu, musí toto ověření prokázat, že její zásady ochrany osobních údajů týkající se osobních údajů získaných z EU jsou přesné, komplexní, snadno dostupné, odpovídají zásadám a jsou zcela zavedeny (*tj.* jsou dodržovány). Musí rovněž uvést, že fyzické osoby jsou informovány o mechanismu (mechanismech), jehož prostřednictvím mohou podávat stížnosti. Metody přezkumu mohou zahrnovat mimo jiné audit, namátkové přezkumy, používání "návnad" nebo vhodné využití technologických nástrojů. Prohlášení ověřující, že externí přezkum shody byl úspěšně dokončen, musí být podepsáno buď osobou provádějící přezkum, nebo vedoucím pracovníkem společnosti či jiným oprávněným zástupcem organizace alespoň jednou ročně a

zpřístupněny na žádost jednotlivců nebo v souvislosti s vyšetřováním či stížností na dodržování předpisů.

e. Organizace musí uchovávat své záznamy o provádění postupů ochrany osobních údajů v EU a USA a na požádání je zpřístupnit v souvislosti s vyšetřováním nebo stížností na nedodržení předpisů nezávislému orgánu pro řešení sporů odpovědnému za vyšetřování stížností nebo agentuře s pravomocí v oblasti nekalých a klamavých praktik. Organizace musí rovněž neprodleně reagovat na dotazy a jiné žádosti o informace ze strany ministerstva týkající se dodržování zásad ze strany organizace.

8. Přístup na

a. <u>Zásada přístupu v praxi</u>

i. Podle zásad je právo na přístup k informacím základem ochrany soukromí. Zejména umožňuje jednotlivcům ověřit si správnost informací, které jsou o nich uchovávány. Zásada přístupu znamená, že fyzické osoby mají právo:

1. získat od organizace potvrzení o tom, zda organizace zpracovává osobní údaje, které se jich týkají;[14]

2. jim tyto údaje sdělily, aby si mohly ověřit jejich přesnost a zákonnost zpracování, a

3. požadovat opravu, změnu nebo výmaz údajů, pokud jsou nepřesné nebo zpracovávané v rozporu se Zásadami.

ii. Jednotlivci nemusí odůvodňovat žádosti o přístup ke svým osobním údajům. Při odpovídání na žádosti jednotlivců o přístup by se organizace měly řídit především zájmem (zájmy), který (které) k žádostem vedl (vedly). Pokud je například žádost o přístup nejasná nebo má široký rozsah, může organizace zapojit jednotlivce do dialogu, aby lépe pochopila motivaci žádosti a našla odpovídající informace. Organizace se může dotázat, s jakou částí (částmi) organizace jednotlivec komunikoval, nebo na povahu informací či jejich využití, které jsou předmětem žádosti o přístup.

iii. V souladu se základní povahou přístupu by organizace měly vždy v dobré víře usilovat o zajištění přístupu. Například v případech, kdy je třeba určité informace chránit a lze je snadno oddělit od ostatních osobních informací, které jsou předmětem žádosti o přístup, by organizace měla chráněné informace redigovat a ostatní zpřístupnit.

[14] Organizace by měla odpovědět na žádosti jednotlivce týkající se účelů zpracování, kategorií dotčených osobních údajů a příjemců nebo kategorií příjemců, kterým jsou osobní údaje zpřístupněny.

informace. Pokud organizace rozhodne, že by měl být přístup v konkrétním případě omezen, měla by osobě žádající o přístup poskytnout vysvětlení, proč k tomuto rozhodnutí dospěla, a kontaktní místo pro případné další dotazy.

b. Zátěž nebo náklady na zajištění přístupu

i. Právo na přístup k osobním údajům může být omezeno za výjimečných okolností, kdy by byla porušena oprávněná práva jiných osob než jednotlivce nebo kdy by zátěž či náklady spojené s poskytnutím přístupu byly nepřiměřené rizikům pro soukromí jednotlivce v daném případě. Náklady a zátěž jsou důležitými faktory a měly by být zohledněny, ale nejsou rozhodujícími faktory při určování, zda je poskytnutí přístupu přiměřené.

ii. Například pokud se osobní údaje používají pro rozhodnutí, která významně ovlivní jednotlivce (*např.* zamítnutí nebo poskytnutí důležitých výhod, jako je pojištění, hypotéka nebo zaměstnání), pak by v souladu s ostatními ustanoveními těchto doplňkových zásad musela organizace tyto informace zveřejnit, i když je jejich poskytnutí poměrně obtížné nebo nákladné. Pokud požadované osobní informace nejsou citlivé nebo se nepoužívají pro rozhodnutí, která významně ovlivní jednotlivce, ale jsou snadno dostupné a jejich poskytnutí není nákladné, organizace by musela přístup k těmto informacím poskytnout.

c. Důvěrné obchodní informace

i. Důvěrné obchodní informace jsou informace, které organizace podnikla kroky k jejich ochraně před zveřejněním, pokud by jejich zveřejnění pomohlo konkurentovi na trhu. Organizace mohou odepřít nebo omezit přístup v rozsahu, v jakém by poskytnutí plného přístupu odhalilo její vlastní důvěrné obchodní informace, jako jsou marketingové závěry nebo klasifikace vytvořené organizací, nebo důvěrné obchodní informace jiné organizace, které podléhají smluvnímu závazku mlčenlivosti.

ii. Pokud lze důvěrné obchodní informace snadno oddělit od ostatních osobních informací, které jsou předmětem žádosti o přístup, měla by organizace důvěrné obchodní informace redigovat a zpřístupnit nedůvěrné informace.

d. Organizace databází

i. Přístup může být zajištěn formou zpřístupnění příslušných osobních údajů organizací.

jednotlivce a nevyžaduje přístup jednotlivce do databáze organizace.

ii. Přístup musí být umožněn pouze v rozsahu, v jakém organizace osobní údaje uchovává. Zásada přístupu sama o sobě nezakládá povinnost uchovávat, udržovat, reorganizovat nebo restrukturalizovat soubory osobních informací.

e. Kdy může být přístup omezen

i. Protože organizace musí vždy v dobré víře usilovat o to, aby jednotlivcům umožnila přístup k jejich osobním údajům, jsou okolnosti, za kterých mohou organizace takový přístup omezit, omezené a veškeré důvody pro omezení přístupu musí být konkrétní. Stejně jako podle GDPR může organizace omezit přístup k informacím v rozsahu, v jakém by jejich zveřejnění mohlo narušit ochranu důležitých protichůdných veřejných zájmů, jako je národní bezpečnost; obrana nebo veřejná bezpečnost. Kromě toho může být přístup odepřen, pokud jsou osobní údaje zpracovávány výhradně pro výzkumné nebo statistické účely. Dalšími důvody pro odepření nebo omezení přístupu jsou:

1. zásahy do výkonu nebo prosazování práva nebo do soukromoprávních nároků, včetně prevence, vyšetřování nebo odhalování trestných činů nebo práva na spravedlivý proces;

2. zveřejnění, pokud by byla porušena oprávněná práva nebo důležité zájmy jiných osob;

3. porušení zákonné nebo jiné profesní výsady či povinnosti;

4. poškozování bezpečnostních vyšetřování zaměstnanců nebo řízení o stížnostech nebo v souvislosti s plánováním nástupnictví zaměstnanců a reorganizací společnosti; nebo

5. poškozování důvěrnosti nezbytné při monitorování, kontrole nebo regulačních funkcích spojených s řádným řízením nebo při budoucích nebo probíhajících jednáních týkajících se organizace.

ii. Organizace, která se domáhá výjimky, musí prokázat její nezbytnost a jednotlivcům by měly být sděleny důvody omezení přístupu a kontaktní místo pro další dotazy.

f. Právo na získání potvrzení a účtování poplatku na pokrytí nákladů na poskytnutí přístupu

i. Fyzická osoba má právo získat potvrzení o tom, zda tato organizace disponuje osobními údaji, které se jí týkají. Fyzická osoba má rovněž právo na to, aby jí byly sděleny osobní údaje, které se jí týkají. Organizace si může účtovat poplatek, který není nepřiměřený.

ii. Účtování poplatku může být oprávněné například v případech, kdy jsou žádosti o přístup zjevně nadměrné, zejména kvůli jejich opakovanému charakteru.

iii. Přístup nelze odmítnout z důvodu nákladů, pokud osoba nabídne, že náklady uhradí.

g. Opakované nebo obtěžující žádosti o přístup

i. Organizace může stanovit přiměřená omezení počtu případů, kdy bude v daném období vyhověno žádostem o přístup od určité osoby. Při stanovování těchto omezení by organizace měla zvážit takové faktory, jako je četnost aktualizace informací, účel, pro který jsou údaje používány, a povaha informací.

h. Podvodné žádosti o přístup

i. Organizace není povinna poskytnout přístup, pokud jí nejsou poskytnuty dostatečné informace, které jí umožní potvrdit totožnost osoby, která žádost podala.

i. Časový rámec pro odpovědi

i. Organizace by měly odpovídat na žádosti o přístup v přiměřené lhůtě, přiměřeným způsobem a ve formě, která je pro jednotlivce snadno srozumitelná. Organizace, která poskytuje informace subjektům údajů v pravidelných intervalech, může vyhovět žádosti jednotlivce o přístup svým pravidelným zveřejňováním, pokud by to nepředstavovalo nadměrné zdržení.

9. Údaje o lidských zdrojích

a. Zahrnutí do DPF EU a USA

i. Pokud organizace v EU předává osobní údaje o svých zaměstnancích (minulých nebo současných) shromážděné v souvislosti se zaměstnaneckým poměrem mateřské společnosti, přidružené společnosti nebo nepropojenému poskytovateli služeb ve Spojených státech, který se účastní DPF EU - USA, požívá předání výhod plynoucích ze směrnice EU DPF V USA. V takových případech se shromažďování informací a jejich zpracování před předáním řídí vnitrostátními právními předpisy členského státu EU, ve kterém byly shromážděny, a musí být dodrženy veškeré podmínky nebo omezení jejich předání podle těchto právních předpisů.

ii. Zásady jsou relevantní pouze v případě přenosu nebo přístupu k individuálně identifikovaným nebo identifikovatelným záznamům. Statistické výkazy, které se opírají o souhrnné údaje o zaměstnanosti a neobsahují žádné osobní údaje nebo používají anonymizované údaje, nevyvolávají obavy o ochranu soukromí.

b. Uplatnění zásad oznámení a volby

i. Americká organizace, která obdržela informace o zaměstnancích z EU v rámci DPF EU - USA, je může zpřístupnit třetím stranám nebo je použít pro jiné účely pouze v souladu se zásadami oznamování a volby. Například pokud organizace hodlá použít osobní údaje získané v rámci pracovního poměru pro účely nesouvisející se zaměstnáním, jako je marketingová komunikace, musí americká organizace předtím poskytnout dotčeným osobám požadovanou možnost volby, ledaže by tyto osoby již použití údajů pro tyto účely schválily. Takové použití nesmí být neslučitelné s účely, pro které byly osobní údaje shromážděny nebo následně jednotlivcem schváleny. Kromě toho nesmí být taková volba použita k omezení pracovních příležitostí nebo k přijetí jakýchkoli sankčních opatření vůči těmto zaměstnancům.

ii. Je třeba poznamenat, že některé obecně platné podmínky pro předávání z některých členských států EU mohou vylučovat další použití těchto informací i po jejich předání mimo EU a tyto podmínky bude třeba dodržovat.

iii. Kromě toho by zaměstnavatelé měli vyvinout přiměřené úsilí, aby vyhověli preferencím zaměstnanců v oblasti ochrany soukromí. To může zahrnovat například omezení přístupu k osobním údajům, anonymizaci některých údajů nebo přidělení kódů či pseudonymů, pokud skutečná jména nejsou pro daný účel řízení potřebná.

iv. V rozsahu a po dobu nezbytně nutnou k tomu, aby se zabránilo poškození schopnosti organizace při povyšování, jmenování nebo jiných podobných rozhodnutích o zaměstnání, nemusí organizace nabízet oznámení a možnost volby.

c. Uplatňování zásady přístupu

i. Doplňková zásada o přístupu poskytuje pokyny k důvodům, které mohou odůvodnit odepření nebo omezení přístupu na žádost v kontextu lidských zdrojů. Zaměstnavatelé v EU musí samozřejmě dodržovat místní předpisy a zajistit, aby zaměstnanci EU měli přístup k takovým informacím, které vyžadují právní předpisy v jejich domovských zemích, bez ohledu na místo zpracování a uchovávání údajů. DPF mezi EU a USA vyžaduje, aby organizace zpracovávající takové údaje ve Spojených státech spolupracovala při poskytování takového přístupu buď přímo, nebo prostřednictvím zaměstnavatele v EU.

d. Vymáhání práva

i. Pokud jsou osobní údaje používány pouze v souvislosti s pracovním poměrem, zůstává primární odpovědnost za údaje vůči zaměstnanci na straně organizace v EU. Z toho vyplývá, že pokud evropští zaměstnanci podávají stížnosti na porušování svých práv na ochranu údajů a

nejsou spokojeni s výsledky interního přezkumu, stížností a odvolacích řízení (nebo případných platných postupů pro podávání stížností podle smlouvy s odborovou organizací), měli by se obrátit na státní nebo vnitrostátní orgán pro ochranu údajů nebo pracovní úřad v jurisdikci, kde zaměstnanci pracují. To se týká i případů, kdy za údajné nesprávné nakládání s jejich osobními údaji odpovídá americká organizace, která informace od zaměstnavatele obdržela, a jde tedy o údajné porušení Zásad. To bude nejefektivnější způsob, jak řešit často se překrývající práva a povinnosti uložené místním pracovním právem a pracovními smlouvami, jakož i právem na ochranu údajů.

ii. Americká organizace účastnící se DPF EU - USA, která používá údaje o lidských zdrojích předávané z EU v rámci pracovněprávního vztahu a která si přeje, aby se na takové předávání vztahoval DPF EU - USA, se proto musí zavázat, že bude v takových případech spolupracovat při vyšetřováních prováděných příslušnými orgány EU a řídit se jejich doporučeními.

e. Uplatňování zásady odpovědnosti za další předávání osob

i. Pro příležitostné provozní potřeby zúčastněné organizace související se zaměstnáním, pokud jde o osobní údaje předávané podle DPF EU - USA, jako je rezervace letu, hotelového pokoje nebo pojištění, lze správcům předávat osobní údaje malého počtu zaměstnanců bez uplatnění zásady přístupu nebo uzavření smlouvy se správcem - třetí stranou, jak se jinak vyžaduje podle zásady odpovědnosti za další předávání, za předpokladu, že zúčastněná organizace dodržuje zásady oznamování a volby.

10. Závazné smlouvy pro další převody

a. Smlouvy o zpracování dat

i. Pokud jsou osobní údaje předávány z EU do Spojených států pouze pro účely zpracování, je třeba uzavřít smlouvu bez ohledu na účast zpracovatele v DPF EU - USA.

ii. Správci údajů v EU jsou povinni uzavřít smlouvu vždy, když dochází k předání údajů za účelem pouhého zpracování, a to bez ohledu na to, zda je zpracování prováděno v EU nebo mimo ni a zda se zpracovatel účastní DPF mezi EU a USA, či nikoli. Účelem smlouvy je zajistit, aby zpracovatel:

1. jedná pouze na základě pokynů z řídicí jednotky;

2. poskytuje vhodná technická a organizační opatření na ochranu osobních údajů před náhodným nebo nezákonným zničením nebo náhodnou ztrátou, změnou,

neoprávněné vyzrazení nebo přístup a rozumí tomu, zda je povolen další přenos; a

3. s ohledem na povahu zpracování pomáhá správci reagovat na fyzické osoby, které uplatňují svá práva podle těchto zásad.

iii. Vzhledem k tomu, že zúčastněné organizace poskytují odpovídající ochranu, nevyžadují smlouvy s těmito organizacemi pro pouhé zpracování předchozí povolení.

b. Převody v rámci ovládané skupiny společností nebo subjektů

i. Pokud jsou osobní údaje předávány mezi dvěma správci v rámci kontrolované skupiny společností nebo subjektů, není podle zásady odpovědnosti za další předávání vždy vyžadována smlouva. Správci údajů v rámci kontrolované skupiny společností nebo subjektů mohou takové předávání založit na jiných nástrojích, jako jsou závazná podniková pravidla EU nebo jiné nástroje uvnitř skupiny (*např.* programy shody a kontroly), které zajišťují kontinuitu ochrany osobních údajů podle Zásad. V případě takových předání zůstává zúčastněná organizace odpovědná za dodržování Zásad.

c. Přenosy mezi řadiči

i. V případě předávání údajů mezi správci nemusí být přijímající správce zúčastněnou organizací ani nemusí mít nezávislý mechanismus odvolání. Zúčastněná organizace musí s přijímajícím správcem - třetí stranou uzavřít smlouvu, která zajišťuje stejnou úroveň ochrany, jaká je k dispozici podle DPF EU a USA, přičemž nezahrnuje požadavek, aby správce - třetí strana byl zúčastněnou organizací nebo měl nezávislý mechanismus odvolání, pokud zpřístupní rovnocenný mechanismus.

11. Řešení sporů a vymáhání práva

a. Zásada odvolání, vymáhání a odpovědnosti stanoví požadavky na vymáhání DPF v EU a USA. Způsob splnění požadavků uvedených v bodě a) ii) zásady je stanoven v doplňkové zásadě o ověřování. Tato doplňková zásada se zabývá body a) i) a a) iii), které oba vyžadují nezávislé mechanismy odvolání. Tyto mechanismy mohou mít různou podobu, musí však splňovat požadavky zásady odvolatelnosti, prosazování a odpovědnosti. Organizace splňují tyto požadavky prostřednictvím následujících opatření: (i) dodržování programů ochrany soukromí vytvořených soukromým sektorem, které zahrnují zásady do svých pravidel a které zahrnují účinné mechanismy prosazování typu popsaného v zásadě odvolatelnosti, prosazování a odpovědnosti; (ii) dodržování právních nebo regulačních dozorových orgánů, které zajišťují vyřizování individuálních stížností a řešení sporů; nebo (iii)

závazek spolupracovat s orgány pro ochranu údajů se sídlem v EU nebo jejich zplnomocněnými zástupci.

b. Tento seznam je pouze ilustrativní, nikoli omezující. Soukromý sektor může navrhnout další mechanismy pro zajištění prosazování, pokud splňují požadavky zásady odvolání, prosazování a odpovědnosti a doplňkových zásad. Upozorňujeme, že požadavky zásady odvolání, prosazování a odpovědnosti doplňují požadavek, že samoregulační úsilí musí být vymahatelné podle oddílu 5 zákona FTC (15 U.S.C. § 45) zakazujícího nekalé nebo klamavé jednání, 49 U.S.C. § 41712 zakazujícího dopravci nebo zprostředkovateli letenek nekalé nebo klamavé jednání v letecké dopravě nebo při prodeji letecké dopravy nebo podle jiného zákona nebo předpisu zakazujícího takové jednání.

c. S cílem pomoci zajistit dodržování závazků v rámci DPF EU a USA a podpořit správu programu musí organizace, jakož i jejich nezávislé mechanismy odvolání, na žádost ministerstva poskytnout informace týkající se DPF EU a USA. Kromě toho musí organizace urychleně reagovat na stížnosti týkající se dodržování zásad, které jim prostřednictvím ministerstva předávají orgány pro ochranu údajů. Odpověď by se měla zabývat tím, zda je stížnost oprávněná, a pokud ano, jak organizace problém napraví. Ministerstvo bude chránit důvěrnost informací, které obdrží, v souladu s právními předpisy USA.

d. <u>Mechanismy odvolání</u>

i. Jednotlivci by měli být vybízeni, aby se s případnými stížnostmi obraceli na příslušnou organizaci dříve, než se obrátí na nezávislé opravné prostředky. Organizace musí jednotlivci odpovědět do 45 dnů od obdržení stížnosti. To, zda je mechanismus odvolání nezávislý, je věcná otázka, kterou lze prokázat zejména nestranností, transparentním složením a financováním a prokázanými výsledky. Jak vyžaduje zásada regresu, vymáhání a odpovědnosti, regresní mechanismus, který je jednotlivcům k dispozici, musí být snadno dostupný a pro jednotlivce bezplatný. Nezávislé orgány pro řešení sporů by se měly zabývat každou stížností, kterou od jednotlivců obdrží, pokud není zjevně neopodstatněná nebo neopodstatněná. To nevylučuje, aby nezávislý orgán pro řešení sporů provozující mechanismus odvolání stanovil požadavky na způsobilost, ale tyto požadavky by měly být transparentní a odůvodněné (například vyloučit stížnosti, které nespadají do oblasti působnosti programu nebo jsou určeny k projednání na jiném fóru) a neměly by mít za následek oslabení závazku zabývat se oprávněnými stížnostmi. Kromě toho by mechanismy odvolání měly jednotlivcům při podání stížnosti poskytnout úplné a snadno dostupné informace o tom, jak postup řešení sporů funguje. Tyto informace by měly zahrnovat upozornění na postupy mechanismu v oblasti ochrany osobních údajů,

v souladu se Zásadami. Měly by také spolupracovat na vývoji nástrojů, jako jsou standardní formuláře stížností, které usnadní proces řešení stížností.

ii. Nezávislé mechanismy odvolání musí na svých veřejných internetových stránkách uvádět informace o zásadách a službách, které poskytují v rámci DPF EU a USA. Tyto informace musí obsahovat: (1) informace o požadavcích Zásad na nezávislé mechanismy pro řešení sporů nebo odkaz na ně; (2) odkaz na internetové stránky ministerstva týkající se rámce pro ochranu osobních údajů; (3) vysvětlení, že jejich služby pro řešení sporů v rámci DPF EU a USA jsou poskytovány v souladu se Zásadami.
DPF USA jsou pro fyzické osoby bezplatné; (4) popis způsobu, jakým lze podat stížnost týkající se Zásad; (5) časový rámec, v němž jsou stížnosti týkající se Zásad vyřizovány; a (6) popis rozsahu možných opravných prostředků.

iii. Nezávislé mechanismy pro řešení sporů musí zveřejňovat výroční zprávu obsahující souhrnné statistiky týkající se jejich služeb řešení sporů. Výroční zpráva musí obsahovat: (1) celkový počet stížností souvisejících se Zásadami přijatých během vykazovaného roku; (2) typy přijatých stížností; (3) opatření pro kvalitu řešení sporů, jako je doba potřebná k vyřízení stížností; a (4) výsledky přijatých stížností, zejména počet a typy nápravných opatření nebo uložených sankcí.

iv. Jak je uvedeno v příloze I, jednotlivec má k dispozici možnost rozhodčího řízení, jehož cílem je zjistit, zda zúčastněná organizace porušila své povinnosti vyplývající ze Zásad ve vztahu k tomuto jednotlivci a zda takové porušení zůstalo zcela nebo částečně nenapraveno. Tato možnost je k dispozici pouze pro tyto účely. Tato možnost není k dispozici například s ohledem na výjimky ze Zásad[15] nebo s ohledem na tvrzení o přiměřenosti DPF mezi EU a USA. V rámci této možnosti rozhodčího řízení má "rozhodčí senát rámce EU a USA pro ochranu osobních údajů" (složený z jednoho nebo tří rozhodců podle dohody stran) pravomoc uložit individuální nepeněžité spravedlivé zadostiučinění (jako je přístup, oprava, výmaz nebo vrácení dotčených údajů jednotlivce) nezbytné k nápravě porušení zásad pouze ve vztahu k jednotlivci. Jednotlivci a zúčastněné organizace se budou moci domáhat soudního přezkumu a výkonu rozhodčích rozhodnutí podle amerického práva v souladu s Federálním zákonem o rozhodčím řízení.

e. <u>Opravné prostředky a sankce</u>

i. Výsledkem všech nápravných opatření poskytnutých nezávislým orgánem pro řešení sporů by mělo být, že účinky nedodržení předpisů budou

[15] Zásady, přehled, odst. 5.

budou organizací v rámci možností zrušeny nebo opraveny a že budoucí zpracování ze strany organizace bude v souladu se Zásadami a případně že zpracování osobních údajů fyzické osoby, která podala stížnost, bude ukončeno. Sankce musí být dostatečně přísné, aby zajistily dodržování Zásad ze strany organizace. Škála sankcí různého stupně přísnosti umožní orgánům pro řešení sporů vhodně reagovat na různé stupně nedodržování předpisů. Sankce by měly zahrnovat jak zveřejnění zjištění o nedodržení, tak požadavek na vymazání údajů za určitých okolností.[16] Další sankce by mohly zahrnovat pozastavení platnosti a odstranění pečeti, odškodnění fyzických osob za ztráty vzniklé v důsledku nedodržení předpisů a soudní příkazy. Nezávislé orgány pro řešení sporů v soukromém sektoru a samoregulační orgány musí o nedodržení svých rozhodnutí zúčastněnými organizacemi informovat vládní orgán s příslušnou pravomocí nebo případně soudy a ministerstvo.

f. Akce FTC

i. FTC se zavázala, že bude přednostně prověřovat podněty týkající se údajného nedodržování Zásad, které obdrží od: i) samoregulačních orgánů pro ochranu soukromí a dalších nezávislých orgánů pro řešení sporů; ii) členských států EU a iii) ministerstva, aby zjistila, zda nedošlo k porušení oddílu 5 zákona FTC zakazujícího nekalé nebo klamavé jednání nebo praktiky v obchodě. Pokud FTC dospěje k závěru, že má důvod se domnívat, že byl porušen oddíl 5, může záležitost řešit tak, že požádá o správní příkaz k zastavení a upuštění od napadených praktik nebo podá stížnost k federálnímu okresnímu soudu, což by v případě úspěchu mohlo vést k vydání rozhodnutí federálního soudu se stejným účinkem. To se týká i nepravdivých tvrzení o dodržování zásad nebo účasti na DPF EU a USA ze strany organizací, které buď již nejsou na seznamu Rámce ochrany osobních údajů, nebo se nikdy samy ministerstvu necertifikovaly. FTC může získat občanskoprávní sankce za porušení správního příkazu k zastavení a upuštění a může vést občanskoprávní nebo trestní řízení pro pohrdání soudem za porušení příkazu federálního soudu. FTC bude o všech takových krocích informovat ministerstvo. Ministerstvo vyzývá ostatní vládní orgány, aby jej informovaly o konečném rozhodnutí v případě jakýchkoli takových postoupení nebo jiných rozhodnutí určujících dodržování Zásad.

g. Trvalé nedodržování předpisů

[16] Nezávislé orgány pro řešení sporů mají možnost rozhodnout, za jakých okolností tyto sankce použijí. Jedním z faktorů, které je třeba vzít v úvahu při rozhodování o tom, zda by měl být požadován výmaz údajů, je citlivost dotčených údajů, stejně jako to, zda organizace shromažďovala, používala nebo zveřejňovala informace v hrubém rozporu se zásadami.

i. Pokud organizace trvale nedodržuje Zásady, nemá již nárok na využívání DPF EU - USA. Organizace, které trvale nedodržují Zásady, budou ministerstvem vyřazeny ze seznamu Rámce pro ochranu osobních údajů a musí vrátit nebo vymazat osobní údaje, které obdržely v rámci DPF EU-U.S..

ii. K soustavnému nedodržování zásad dochází, pokud organizace, která se sama certifikovala ministerstvu, odmítá dodržovat konečné rozhodnutí samoregulačního orgánu, nezávislého orgánu pro řešení sporů nebo vládního orgánu pro ochranu soukromí, nebo pokud takový orgán, včetně ministerstva, zjistí, že organizace často nedodržuje zásady do té míry, že její tvrzení o dodržování zásad již není důvěryhodné. V případech, kdy takové zjištění učiní jiný orgán než ministerstvo, musí organizace tyto skutečnosti neprodleně oznámit ministerstvu. Pokud tak neučiní, může být žalováno podle zákona o nepravdivých prohlášeních (18 U.S.C. § 1001). Odstoupení organizace od samoregulačního programu pro ochranu soukromí v soukromém sektoru nebo od nezávislého mechanismu řešení sporů ji nezbavuje povinnosti dodržovat zásady a představovalo by trvalé nedodržování zásad.

iii. Ministerstvo vyškrtne organizaci z rámcového seznamu pro ochranu osobních údajů za trvalé nedodržování předpisů, a to i v reakci na jakékoli oznámení, které obdrží o takovém nedodržování předpisů od samotné organizace, samoregulačního orgánu pro ochranu osobních údajů nebo jiného nezávislého orgánu pro řešení sporů nebo od vládního orgánu, avšak až poté, co organizaci nejprve poskytne 30denní lhůtu a možnost reagovat[17] . V souladu s tím bude ze seznamu rámce ochrany osobních údajů vedeného ministerstvem zřejmé, které organizace mají zajištěny a které již nemají zajištěny výhody vyplývající z rámce ochrany osobních údajů mezi EU a USA.

iv. Organizace, která žádá o účast v samoregulačním orgánu pro účely rekvalifikace pro DPF EU a USA, musí tomuto orgánu poskytnout úplné informace o své předchozí účasti v DPF EU a USA.

[17] Odbor v oznámení uvede lhůtu, která bude nutně kratší než 30 dnů, kterou má organizace na oznámení reagovat.

12. Volba - načasování odhlášení

a. Účelem zásady volby je obecně zajistit, aby osobní údaje byly používány a zveřejňovány způsobem, který je v souladu s očekáváním a volbou jednotlivce. Jednotlivec by proto měl mít možnost kdykoli uplatnit "opt-out" volbu, že osobní údaje budou použity k přímému marketingu, s výhradou přiměřených omezení stanovených organizací, jako je například poskytnutí času organizaci na to, aby byl opt-out účinný. Organizace může rovněž požadovat dostatečné informace k potvrzení totožnosti fyzické osoby, která o "opt out" žádá. Ve Spojených státech mohou mít jednotlivci možnost využít této možnosti prostřednictvím centrálního programu "opt-out". V každém případě by měl mít jednotlivec k dispozici snadno dostupný a cenově přijatelný mechanismus pro uplatnění této možnosti.

b. Stejně tak může organizace používat informace pro určité účely přímého marketingu, pokud není možné poskytnout jednotlivci možnost odmítnout před použitím informací, pokud mu organizace současně (a na jeho žádost kdykoli) neprodleně poskytne možnost odmítnout (bez jakýchkoli nákladů pro jednotlivce) přijímat další sdělení v rámci přímého marketingu a organizace toto přání jednotlivce splní.

13. Cestovní informace

a. Rezervace cestujících leteckou společností a další cestovní informace, jako jsou informace o věrnostních letenkách nebo rezervace hotelů a informace o zvláštních potřebách, jako je stravování v souladu s náboženskými požadavky nebo fyzická pomoc, mohou být předávány organizacím mimo EU za několika různých okolností. Podle GDPR mohou být osobní údaje, pokud neexistuje rozhodnutí o odpovídající ochraně, předány do třetí země, pokud jsou poskytnuty vhodné záruky ochrany údajů podle článku 46 GDPR nebo pokud je ve zvláštních situacích splněna jedna z podmínek článku 49 GDPR (*např.* pokud subjekt údajů s předáním výslovně souhlasil). Organizace v USA, které se přihlásily k DPF mezi EU a USA, poskytují odpovídající ochranu osobních údajů, a proto mohou přijímat předávání údajů z EU na základě článku 45 GDPR, aniž by musely zavést nástroj pro předávání údajů podle článku 46 GDPR nebo splnit podmínky článku 49 GDPR. Vzhledem k tomu, že DPF mezi EU a USA obsahuje zvláštní pravidla pro citlivé informace, mohou být takové informace (které může být nutné shromažďovat například v souvislosti s potřebou fyzické pomoci zákazníků) zahrnuty do předávání zúčastněným organizacím. Ve všech případech však musí organizace předávající informace respektovat právní předpisy členského státu EU, v němž působí, které mohou *mimo jiné* stanovit zvláštní podmínky pro nakládání s citlivými údaji.

14. Farmaceutické a lékařské výrobky

a. <u>Uplatňování právních předpisů EU/členských států nebo zásad</u>

i. Na shromažďování osobních údajů a jejich zpracování před předáním do Spojených států se vztahují právní předpisy EU/členského státu. Zásady se vztahují na údaje po jejich předání do Spojených států. Údaje používané pro farmaceutický výzkum a jiné účely by měly být v případě potřeby anonymizovány.

b. Budoucí vědecký výzkum

i. Osobní údaje získané v rámci konkrétních lékařských nebo farmaceutických výzkumných studií často hrají cennou roli v budoucím vědeckém výzkumu. Pokud jsou osobní údaje shromážděné pro jednu výzkumnou studii předány americké organizaci v rámci DPF EU - USA, může tato organizace údaje použít pro novou vědeckovýzkumnou činnost, pokud byla v první instanci řádně informována a byla jí poskytnuta možnost volby. Toto oznámení by mělo obsahovat informace o jakémkoli budoucím konkrétním využití údajů, jako je pravidelné sledování, související studie nebo marketing.

ii. Je zřejmé, že nelze specifikovat všechna budoucí využití údajů, protože nové výzkumné využití může vyplynout z nových poznatků o původních údajích, z nových lékařských objevů a pokroků a z vývoje v oblasti veřejného zdraví a regulace. Oznámení by proto mělo případně obsahovat vysvětlení, že osobní údaje mohou být použity v budoucích lékařských a farmaceutických výzkumných činnostech, které nejsou předvídány. Pokud toto použití není v souladu s obecným účelem (účely) výzkumu, pro který byly osobní údaje původně shromážděny nebo s nímž osoba dodatečně souhlasila, je třeba získat nový souhlas.

c. Odstoupení od klinického hodnocení

i. Účastníci se mohou kdykoli rozhodnout nebo být požádáni o odstoupení z klinického hodnocení. Veškeré osobní údaje shromážděné před odstoupením mohou být i nadále zpracovávány spolu s dalšími údaji shromážděnými v rámci klinického hodnocení, pokud to však bylo účastníkovi v oznámení v době, kdy souhlasil s účastí, vysvětleno.

d. Převody pro účely regulace a dohledu

i. Farmaceutické společnosti a společnosti vyrábějící zdravotnické prostředky mohou poskytovat osobní údaje z klinických hodnocení prováděných v EU regulačním orgánům ve Spojených státech pro účely regulace a dohledu. Podobná předávání jsou povolena i jiným stranám než regulačním orgánům, například pobočkám společností a dalším výzkumným pracovníkům, v souladu se zásadami oznamování a volby.

e. "Zaslepené" studie

i. V zájmu zajištění objektivity v mnoha klinických studiích

nemohou mít účastníci a často ani zkoušející přístup k informacím o tom, jakou léčbu může každý účastník podstoupit.

přijímání. Tím by byla ohrožena platnost výzkumné studie a jejích výsledků. Účastníkům takových klinických studií (označovaných jako "zaslepené" studie) nemusí být v průběhu studie poskytnut přístup k údajům o jejich léčbě, pokud bylo toto omezení vysvětleno při vstupu účastníka do studie a zveřejnění takových informací by ohrozilo integritu výzkumného úsilí.

ii. Souhlas s účastí ve zkoušce za těchto podmínek je přiměřeným vzdáním se práva na přístup. Po ukončení studie a analýze výsledků by účastníci měli mít přístup ke svým údajům, pokud o to požádají. Měli by o něj požádat primárně lékaře nebo jiného poskytovatele zdravotní péče, u kterého byli v rámci klinického hodnocení léčeni, případně sekundárně zadávající organizaci.

f. Sledování bezpečnosti a účinnosti výrobku

i. Farmaceutická společnost nebo společnost vyrábějící zdravotnické prostředky nemusí uplatňovat Zásady s ohledem na zásady oznamování, volby, odpovědnosti za další přenos a přístupu při svých činnostech sledování bezpečnosti a účinnosti výrobků, včetně hlášení nežádoucích účinků a sledování pacientů/subjektů užívajících určité léčivé přípravky nebo zdravotnické prostředky, pokud dodržování Zásad narušuje soulad s regulačními požadavky. To platí jak s ohledem na hlášení, která podávají například poskytovatelé zdravotní péče farmaceutickým společnostem a společnostem vyrábějícím zdravotnické prostředky, tak s ohledem na hlášení, která podávají farmaceutické společnosti a společnosti vyrábějící zdravotnické prostředky vládním agenturám, jako je Úřad pro kontrolu potravin a léčiv.

g. Data kódovaná klíčem

i. Výzkumná data jsou při svém vzniku vždy jednoznačně kódována klíčem hlavního řešitele, aby nebyla odhalena identita jednotlivých subjektů údajů. Farmaceutické společnosti, které takový výzkum sponzorují, tento klíč nedostávají. Jedinečný klíčový kód má pouze výzkumný pracovník, aby mohl za zvláštních okolností (*např.* v případě potřeby následné lékařské péče) identifikovat subjekt výzkumu. Na předávání takto kódovaných údajů z EU do Spojených států, které jsou podle práva EU osobními údaji, by se zásady vztahovaly.

15. Veřejné záznamy a veřejně dostupné informace

a. Organizace musí na osobní údaje z veřejně dostupných zdrojů uplatňovat zásady bezpečnosti, integrity údajů a omezení účelu a odvolání, vymáhání a odpovědnosti. Tyto zásady se vztahují i na osobní údaje shromážděné z veřejně přístupných záznamů (tj. takových záznamů, které vedou vládní agentury nebo subjekty na jakékoli úrovni a do nichž může nahlížet široká veřejnost).

b. Na informace z veřejných záznamů není nutné uplatňovat zásady oznamování, volby nebo odpovědnosti při dalším předávání, pokud nejsou kombinovány s informacemi z neveřejných záznamů a jsou dodrženy veškeré podmínky pro konzultaci stanovené příslušnou jurisdikcí. Rovněž není obecně nutné uplatňovat zásady oznamování, volby nebo odpovědnosti při dalším předávání na veřejně dostupné informace, pokud evropský předávající neuvede, že tyto informace podléhají omezením, která vyžadují uplatnění těchto zásad ze strany organizace pro zamýšlené použití. Organizace nenesou žádnou odpovědnost za to, jak takové informace použijí ti, kteří je získají ze zveřejněných materiálů.

c. Pokud se zjistí, že organizace úmyslně zveřejnila osobní údaje v rozporu se zásadami, aby mohla ona nebo jiné osoby využít těchto výjimek, přestane mít nárok na výhody vyplývající z DPF EU a USA.

d. Zásadu přístupu není nutné uplatňovat na informace z veřejných záznamů, pokud nejsou kombinovány s jinými osobními údaji (kromě malého množství použitého k indexování nebo uspořádání informací z veřejných záznamů); je však třeba dodržovat veškeré podmínky pro nahlížení stanovené příslušnou jurisdikcí. Naproti tomu v případě, že jsou informace z veřejných záznamů kombinovány s jinými informacemi z neveřejných záznamů (kromě těch, které jsou výslovně uvedeny výše), musí organizace poskytnout přístup ke všem takovým informacím za předpokladu, že se na ně nevztahují jiné povolené výjimky.

e. Stejně jako u informací z veřejných rejstříků není nutné poskytovat přístup k informacím, které jsou již veřejně dostupné široké veřejnosti, pokud nejsou kombinovány s neveřejně dostupnými informacemi. Organizace, které se zabývají prodejem veřejně dostupných informací, mohou za odpověď na žádost o přístup účtovat obvyklý poplatek organizace. Případně mohou jednotlivci požádat o přístup ke svým informacím organizaci, která údaje původně sestavila.

16. Žádosti o přístup od orgánů veřejné moci

a. Za účelem zajištění transparentnosti, pokud jde o zákonné žádosti orgánů veřejné moci o přístup k osobním informacím, mohou zúčastněné organizace dobrovolně vydávat pravidelné zprávy o transparentnosti týkající se počtu žádostí o osobní informace, které obdržely od orgánů veřejné moci za účelem

z důvodů vymáhání práva nebo národní bezpečnosti, pokud je takové zpřístupnění přípustné podle platných právních předpisů.

b. Informace poskytnuté zúčastněnými organizacemi v těchto zprávách spolu s informacemi, které byly zveřejněny zpravodajskou komunitou, a dalšími informacemi mohou být použity při pravidelném společném přezkumu fungování DPF EU a USA v souladu se zásadami.

c. Absence oznámení v souladu s písmenem a) bodem xii) zásady oznamování nebrání organizaci v odpovědi na jakoukoli zákonnou žádost ani ji neomezuje.

PŘÍLOHA I: ARBITRÁLNÍ MODEL

Tato příloha I stanoví podmínky, za kterých jsou organizace účastnící se DPF EU a USA povinny rozhodovat nároky podle dohody o regresních nárocích, vymáhání a odpovědnosti. Princip. Níže popsaná možnost závazného rozhodčího řízení se vztahuje na některé "zbytkové" nároky týkající se údajů, na které se vztahuje DPF EU a USA. Účelem této možnosti je poskytnout rychlý, nezávislý a spravedlivý mechanismus pro řešení jakýchkoli tvrzených porušení zásad, které nebyly vyřešeny žádným z ostatních mechanismů DPF EU a USA, podle volby jednotlivců.

A. Oblast působnosti

Tato možnost rozhodčího řízení je k dispozici jednotlivci, aby v případě zbytkových nároků určil, zda zúčastněná organizace porušila své povinnosti vyplývající ze Zásad ve vztahu k tomuto jednotlivci a zda takové porušení zůstalo zcela nebo částečně nenapraveno. Tato možnost je k dispozici pouze pro tyto účely. Tato možnost není k dispozici například s ohledem na výjimky ze Zásad[18] nebo s ohledem na tvrzení o přiměřenosti DPF mezi EU a USA.

B. Dostupné opravné prostředky

V rámci této možnosti rozhodčího řízení je "rámcový rozhodčí senát EU a USA pro ochranu osobních údajů" (rozhodčí senát složený z jednoho nebo tří rozhodců, jak se strany dohodnou) oprávněn uložit individuální nepeněžité spravedlivé zadostiučinění (například přístup, opravu,
vymazání nebo vrácení dotčených údajů jednotlivce), které jsou nezbytné k nápravě porušení Zásad pouze ve vztahu k danému jednotlivci. Toto jsou jediné pravomoci panelu pro ochranu soukromí EU a USA, pokud jde o nápravná opatření. Při zvažování nápravných opatření EU
Rámcový panel USA pro ochranu osobních údajů je povinen zvážit další nápravná opatření, která již byla uložena jinými mechanismy v rámci rámce EU a USA pro ochranu osobních údajů. Žádná náhrada škody, náklady, poplatky ani jiné prostředky nápravy nejsou k dispozici. Každá strana si hradí své vlastní náklady na právní zastoupení.

C. Požadavky před arbitráží

Osoba, která se rozhodne využít této možnosti rozhodčího řízení, musí před zahájením rozhodčího řízení učinit následující kroky: (1) vznést tvrzené porušení přímo u organizace a poskytnout jí příležitost vyřešit problém ve lhůtě stanovené v oddíle (d)(i) Doplňkových zásad pro řešení sporů a prosazování práva; (2) využít nezávislý mechanismus odvolání podle Zásad, a to bez jakýchkoli nákladů pro jednotlivce; a (3) vznést problém prostřednictvím DPA jednotlivce na ministerstvo a poskytnout ministerstvu příležitost vyvinout maximální úsilí k vyřešení problému ve lhůtách stanovených v dopise Odboru mezinárodního obchodu ministerstva, a to bez jakýchkoli nákladů pro jednotlivce.

Tuto možnost rozhodčího řízení nelze uplatnit, pokud stejné tvrzené porušení Zásad (1) bylo již dříve předmětem závazného rozhodčího řízení; (2) bylo předmětem pravomocného rozsudku vydaného v soudním řízení, jehož byl jednotlivec účastníkem; nebo (3) bylo již dříve stranami urovnáno. Tuto možnost navíc nelze uplatnit, pokud orgán pro ochranu údajů (1) má pravomoc podle doplňkové zásady o úloze orgánů pro ochranu údajů nebo doplňkové zásady o údajích o lidských zdrojích nebo (2) má pravomoc řešit

[18] Zásady, přehled, odst. 5.

tvrzené porušení přímo s organizací. Pravomoc orgánu pro ochranu údajů řešit stejný nárok proti správci údajů v EU sama o sobě nevylučuje uplatnění této možnosti rozhodčího řízení proti jinému právnímu subjektu, který není vázán pravomocí orgánu pro ochranu údajů.

D. Závaznost rozhodnutí

Rozhodnutí jednotlivce využít této možnosti závazného rozhodčího řízení je zcela dobrovolné. Rozhodnutí rozhodčího soudu jsou závazná pro všechny strany rozhodčího řízení. Po uplatnění rozhodčího řízení se jednotlivec vzdává možnosti domáhat se nápravy téhož tvrzeného porušení u jiného soudu, s výjimkou toho, že pokud nepeněžní spravedlivé zadostiučinění nevede k úplné nápravě tvrzeného porušení, nevylučuje uplatnění rozhodčího řízení ze strany jednotlivce nárok na náhradu škody, který je jinak k dispozici u soudu.

E. Přezkum a prosazování

Jednotlivci a zúčastněné organizace se budou moci domáhat soudního přezkumu a výkonu rozhodčích rozhodnutí podle amerického práva v souladu s federálním zákonem o rozhodčím řízení.[19] Všechny takové případy musí být podány u federálního okresního soudu, do jehož územní působnosti spadá hlavní místo podnikání zúčastněné organizace.

Tato možnost rozhodčího řízení je určena k řešení individuálních sporů a rozhodčí rozhodnutí nemají sloužit jako přesvědčivý nebo závazný precedens v záležitostech týkajících se jiných stran, včetně budoucích rozhodčích řízení nebo řízení před soudy EU nebo USA nebo před FTC.

F. Rozhodčí komise

Strany vyberou rozhodce pro rámcový panel pro ochranu osobních údajů mezi EU a USA ze seznamu rozhodců uvedeného níže.

---

[19] Kapitola 2 Federálního zákona o rozhodčím řízení ("FAA") stanoví, že "rozhodčí smlouva nebo rozhodčí nález vyplývající z právního vztahu, ať už smluvního či jiného, který je považován za obchodní, včetně transakce, smlouvy nebo dohody popsané v [oddílu 2 FAA], spadá pod Úmluvu [o uznávání a výkonu cizích rozhodčích nálezů ze dne 10. června 1958, 21 U.S.T. 2519, T.I.A.S. č. 6997 ("Newyorská úmluva")]." 9 U.S.C. § 202. FAA dále stanoví, že "dohoda nebo rozhodčí nález vyplývající z takového vztahu, který je výhradně mezi občany Spojených států, se nepovažuje za spadající pod [Newyorskou] úmluvu, pokud se tento vztah netýká majetku nacházejícího se v zahraničí, nepředpokládá plnění nebo výkon v zahraničí nebo nemá jiný přiměřený vztah k jednomu nebo více cizím státům". *Id.* Podle kapitoly 2 "může kterákoli strana rozhodčího řízení požádat kterýkoli soud příslušný podle této kapitoly o potvrzení rozhodčího nálezu vůči kterékoli jiné straně rozhodčího řízení. Soud rozhodčí nález potvrdí, pokud neshledá některý z důvodů pro odmítnutí nebo odložení uznání nebo výkonu rozhodčího nálezu uvedených v uvedené [Newyorské] úmluvě." *Id.* § 207. Kapitola 2 dále stanoví, že "okresní soudy Spojených států. ... mají původní příslušnost pro ... žalobu nebo řízení [podle Newyorské úmluvy] bez ohledu na výši sporné částky". *Id.* § 203.

Kapitola 2 rovněž stanoví, že "kapitola 1 se použije na žaloby a řízení zahájená podle této kapitoly v rozsahu, v němž tato kapitola není v rozporu s touto kapitolou nebo s [Newyorskou] úmluvou ratifikovanou Spojenými státy." *Id.* § 208. Kapitola 1 zase stanoví, že "písemné ustanovení... ve smlouvě, která dokládá obchodní transakci, o rozhodčím řízení sporu, který následně vznikne z takové smlouvy nebo transakce, nebo o odmítnutí jejího celého plnění nebo jeho části, nebo písemná dohoda o předložení existujícího sporu vyplývajícího z takové smlouvy, transakce nebo odmítnutí k rozhodčímu řízení jsou platné, neodvolatelné a vymahatelné, s výjimkou takových důvodů, které existují podle zákona nebo podle práva pro zrušení jakékoli smlouvy.". *Id.* § 2. Kapitola 1 dále stanoví, že "kterákoli strana rozhodčího řízení může požádat takto určený soud o vydání příkazu k potvrzení rozhodčího nálezu a soud musí tento příkaz vydat, pokud není rozhodčí nález zrušen, změněn nebo opraven způsobem stanoveným v oddílech 10 a 11 [FAA]". *Id.* § 9.

V souladu s platnými právními předpisy vypracují odbor a Komise seznam nejméně deseti rozhodců, kteří budou vybráni na základě nezávislosti, bezúhonnosti a odborných znalostí. V souvislosti s tímto postupem se použijí následující ustanovení:

Rozhodci:

(1) zůstane na seznamu po dobu tří let, pokud nenastanou výjimečné okolnosti nebo nedojde k jeho vyřazení z důvodu, přičemž toto období může odbor po předchozím oznámení Komisi prodloužit o další tři roky;
(2) nepodléhá žádným pokynům žádné ze stran, žádné ze zúčastněných organizací, USA, EU nebo jakéhokoli členského státu EU, ani žádného jiného vládního orgánu, orgánu veřejné moci nebo donucovacího orgánu, ani s nimi není spojen; a
(3) musí mít oprávnění k výkonu právnické praxe ve Spojených státech a být odborníky na americké právo na ochranu soukromí s odbornými znalostmi v oblasti práva EU na ochranu údajů.

G. Rozhodčí řízení

Ministerstvo a Komise se v souladu s platnými právními předpisy dohodly na přijetí rozhodčích pravidel, kterými se řídí řízení před rámcovým panelem pro ochranu osobních údajů mezi EU a USA.[20] V případě, že bude třeba změnit pravidla, jimiž se řízení řídí, dohodnou se ministerstvo a Komise na změně těchto pravidel nebo na přijetí jiného souboru stávajících, dobře zavedených rozhodčích řízení v USA, a to podle potřeby s ohledem na všechny níže uvedené skutečnosti:

1. Jednotlivec může zahájit závazné rozhodčí řízení, s výhradou výše uvedených požadavků na předrozhodčí řízení, doručením "oznámení" organizaci. Oznámení musí obsahovat shrnutí kroků podniknutých podle odstavce C k vyřešení nároku, popis údajného porušení a podle volby jednotlivce veškeré podpůrné dokumenty a materiály a/nebo diskusi o právu týkajícím se údajného nároku.
2. Budou vypracovány postupy, které zajistí, aby se na stejné porušení, které jednotlivec tvrdí, nevztahovaly duplicitní opravné prostředky nebo postupy.
3. Souběžně s rozhodčím řízením může probíhat žaloba FTC.
4. Těchto rozhodčích řízení se nesmí účastnit žádný zástupce USA, EU nebo jakéhokoli členského státu EU ani žádný jiný vládní orgán, orgán veřejné moci nebo donucovací orgán, přičemž na žádost jednotlivce z EU může orgán pro ochranu údajů poskytnout pomoc pouze při přípravě oznámení, ale orgán pro ochranu údajů nesmí mít přístup k nálezům nebo jiným materiálům souvisejícím s těmito rozhodčími řízeními.
5. Místem konání rozhodčího řízení budou Spojené státy americké a jednotlivec si může zvolit videokonferenci nebo telefonickou účast, která mu bude poskytnuta bezplatně. Osobní účast nebude vyžadována.
6. Jazykem rozhodčího řízení bude angličtina, pokud se strany nedohodnou jinak. Na základě odůvodněné žádosti a s přihlédnutím k tomu, zda je fyzická osoba zastoupena advokátem, bude na rozhodčím jednání zajištěno tlumočení, jakož i překlad rozhodčího spisu.

[20] Mezinárodní centrum pro řešení sporů ("ICDR"), mezinárodní divize americké advokátní komory Arbitrážní asociace (dále jen "AAA") (dále jen "ICDR-AAA") byla vybrána ministerstvem, aby spravovala rozhodčí řízení podle rozhodčího fondu uvedeného v příloze I Zásad. Dne 15. září 2017 se ministerstvo a Komise dohodly na přijetí souboru rozhodčích pravidel, jimiž se budou řídit závazná rozhodčí řízení popsaná v příloze I Zásad, jakož i kodexu chování rozhodců, který je v souladu s obecně uznávanými etickými normami pro obchodní rozhodce a přílohou I Zásad.

Ministerstvo a Komise se dohodly, že upraví pravidla rozhodčího řízení a kodex chování tak, aby odrážely aktualizace v rámci DPF mezi EU a USA, a ministerstvo bude na těchto aktualizacích spolupracovat s ICDR-AAA.

materiály budou jednotlivci poskytnuty bezplatně, ledaže by panel pro rámec EU a USA pro ochranu osobních údajů shledal, že by to za okolností konkrétního rozhodčího řízení vedlo k neodůvodněným nebo nepřiměřeným nákladům.

7. Materiály předložené rozhodcům budou považovány za důvěrné a budou použity pouze v souvislosti s rozhodčím řízením.
8. V případě potřeby může být povoleno individuální zjišťování, které bude stranami považováno za důvěrné a bude použito pouze v souvislosti s rozhodčím řízením.
9. Rozhodčí řízení by mělo být ukončeno do 90 dnů od doručení oznámení dotčené organizaci, pokud se strany nedohodnou jinak.

H. Náklady

Rozhodci by měli podniknout přiměřené kroky k minimalizaci nákladů nebo poplatků za rozhodčí řízení.

Ministerstvo v souladu s platnými právními předpisy usnadní udržování fondu, do kterého budou zúčastněné organizace povinny přispívat, částečně v závislosti na velikosti organizace, a který bude pokrývat náklady na rozhodčí řízení, včetně poplatků rozhodci, až do maximální výše ("stropy"). Fond bude spravovat třetí strana, která bude pravidelně podávat ministerstvu zprávy o činnosti fondu. Ministerstvo bude ve spolupráci s třetí stranou pravidelně přezkoumávat fungování fondu, včetně potřeby upravit výši příspěvků nebo horní hranice nákladů na rozhodčí řízení, a zváží mimo jiné počet rozhodčích řízení a náklady a načasování rozhodčích řízení s tím, že zúčastněné organizace nebudou nadměrně finančně zatěžovány. Odbor oznámí Komisi výsledek těchto přezkumů s třetí stranou a předem jí oznámí veškeré úpravy výše příspěvků. Odměny advokátů nejsou pokryty tímto ustanovením ani žádným fondem podle tohoto ustanovení.

PŘÍLOHA II

Dopis ministryně obchodu USA Giny Raimondo

[...]

Ctihodný Didier Reynders
komisař pro spravedlnost
Evropská komise
Rue de la Loi/ Westraat 200
1049 Brusel
Belgie

Vážený pane komisaři Reyndersi:

Jménem Spojených států si dovoluji tímto předat balíček materiálů o rámci EU a USA pro ochranu osobních údajů, který spolu s exekutivním příkazem č. 14086 "Posílení záruk pro zpravodajské činnosti Spojených států v oblasti signálů" a částí 28 CFR 201, kterou se mění předpisy ministerstva spravedlnosti za účelem zřízení "Soudu pro přezkum ochrany údajů", odráží důležitá a podrobná jednání o posílení ochrany soukromí a občanských svobod. Výsledkem těchto jednání jsou nová ochranná opatření, která zajistí, aby činnosti signálového zpravodajství USA byly nezbytné a přiměřené při sledování stanovených cílů národní bezpečnosti, a nový mechanismus pro jednotlivce z Evropské unie (dále jen "EU"), který jim umožní domáhat se nápravy, pokud se domnívají, že se na ně činnosti signálového zpravodajství zaměřují protiprávně, což společně zajistí soukromí osobních údajů v EU. Rámec EU a USA pro ochranu osobních údajů podpoří inkluzivní a konkurenceschopnou digitální ekonomiku. Oba bychom měli být hrdí na zlepšení, která se v tomto rámci odrážejí a která posílí ochranu soukromí na celém světě. Tento balíček spolu s prováděcí vyhláškou, nařízeními a dalšími materiály dostupnými z veřejných zdrojů poskytuje velmi silný základ pro nové zjištění Evropské komise o přiměřenosti.[1]

V příloze jsou přiloženy následující materiály:

- Rámcové zásady ochrany osobních údajů mezi EU a USA, včetně doplňkových zásad (dále společně jen "zásady") a příloha I zásad (*tj*. příloha, která stanoví podmínky, za nichž jsou organizace v rámci ochrany osobních údajů povinny rozhodovat určité zbývající nároky týkající se osobních údajů, na něž se zásady vztahují);
- Dopis Úřadu pro mezinárodní obchod ministerstva, který spravuje program rámce pro ochranu osobních údajů, popisující závazky, které naše ministerstvo přijalo, aby zajistilo účinné fungování rámce pro ochranu osobních údajů mezi EU a USA;

[1] Za předpokladu, že se rozhodnutí Komise o přiměřenosti ochrany poskytované rámcem EU a USA pro ochranu soukromí vztahuje na Island, Lichtenštejnsko a Norsko, bude se balíček týkající se rámce EU a USA pro ochranu soukromí vztahovat jak na Evropskou unii, tak na tyto tři země.

- Dopis Federální obchodní komise popisující prosazování Zásad;
- Dopis ministerstva dopravy popisující prosazování Zásad;
- dopis vypracovaný Úřadem ředitele národních zpravodajských služeb týkající se ochranných opatření a omezení vztahujících se na orgány národní bezpečnosti USA; a
- Dopis vypracovaný ministerstvem spravedlnosti týkající se ochranných opatření a omezení týkajících se

Přístup vlády USA pro účely vymáhání práva a veřejného zájmu.

Úplný balíček rámcových předpisů o ochraně osobních údajů mezi EU a USA bude zveřejněn na internetových stránkách ministerstva pro ochranu osobních údajů a zásady a příloha I zásad vstoupí v platnost dnem vstupu v platnost rozhodnutí Evropské komise o odpovídající ochraně osobních údajů.

Můžete si být jisti, že Spojené státy berou tyto závazky vážně. Těšíme se na spolupráci s vámi při provádění rámce EU a USA pro ochranu osobních údajů a na další fázi tohoto procesu, kterou společně zahájíme.

S pozdravem,

Gina M. Raimondo

PŘÍLOHA III

Dopis náměstkyně ministra obchodu pro mezinárodní obchod Marisy Lago

[...]

Ctihodný Didier Reynders
komisař pro spravedlnost
Evropská komise
Rue de la Loi/Westraat 200
1049 Brusel
Belgie

Vážený pane komisaři Reyndersi:

Jménem Úřadu pro mezinárodní obchod (dále jen "ÚMT") si dovoluji popsat závazky, které Ministerstvo obchodu (dále jen "ministerstvo") přijalo s cílem zajistit ochranu osobních údajů prostřednictvím správy a dohledu nad programem rámce ochrany osobních údajů. Dokončení rámce pro ochranu osobních údajů mezi EU a USA (dále jen "rámec pro ochranu osobních údajů mezi EU a USA") je významným úspěchem pro ochranu soukromí a pro podniky na obou stranách Atlantiku, neboť poskytne jednotlivcům v EU jistotu, že jejich údaje budou chráněny a že budou mít k dispozici právní prostředky k řešení obav souvisejících s jejich údaji, a umožní tisícům podniků pokračovat v investicích a jinak se zapojit do obchodu a podnikání přes Atlantik ku prospěchu našich příslušných ekonomik a občanů. DPF mezi EU a USA odráží roky usilovné práce a spolupráce s vámi a vašimi kolegy v Evropské komisi (dále jen "Komise"). Těšíme se na další spolupráci s Komisí, abychom zajistili efektivní fungování této spolupráce.

DPF EU - USA přinese významné výhody jak jednotlivcům, tak podnikům. Zaprvé poskytuje důležitý soubor ochranných opatření pro ochranu soukromí fyzických osob z EU, které jsou předávány do Spojených států. Vyžaduje, aby zúčastněné organizace v USA vypracovaly odpovídající politiku ochrany soukromí; veřejně se zavázaly k dodržování "zásad rámce EU a USA pro ochranu osobních údajů", včetně doplňkových zásad (souhrnně "zásady").
Zásady") a přílohu I Zásad (*tj.* přílohu, která stanoví podmínky, za nichž se EU a její členské státy zavazují k dodržování Zásad).
Americké organizace DPF jsou povinny rozhodovat některé zbývající nároky týkající se osobních údajů, na které se vztahují Zásady), aby se závazek stal vymahatelným podle amerického práva[1] ; každoročně znovu osvědčují ministerstvu, že dodržují Zásady; poskytují bezplatné, nezávislé řešení sporů.

[1] Organizace, které samy potvrdily svůj závazek dodržovat zásady rámce štítu EU-USA na ochranu soukromí a chtějí využívat výhod plynoucích z účasti v rámci štítu EU-USA na ochranu soukromí, musí dodržovat "Zásady rámce EU-USA na ochranu soukromí". Tento závazek dodržovat "Rámcové zásady ochrany osobních údajů mezi EU a USA" se vztahuje na všechny členské státy.
Zásady" budou zohledněny v zásadách ochrany osobních údajů těchto zúčastněných organizací co nejdříve,

nejpozději však do tří měsíců od data nabytí účinnosti "Zásad rámce ochrany osobních údajů mezi EU a USA". (*Viz* oddíl e) doplňkových zásad o autocertifikaci).

a podléhat vyšetřovacím a donucovacím pravomocem orgánu, který je oprávněn rozhodovat o sankcích vůči jednotlivcům z EU.
statutární orgán USA uvedený v Zásadách (*např.* Federální obchodní komise (FTC) a Ministerstvo dopravy (DOT)) nebo statutární orgán USA uvedený v budoucí příloze Zásad. Zatímco rozhodnutí organizace o vlastní certifikaci je dobrovolné, jakmile se organizace veřejně zaváže k dodržování zásad DPF EU a USA, je její závazek vymahatelný podle práva USA ze strany FTC, DOT nebo jiného statutárního orgánu USA v závislosti na tom, který orgán má nad zúčastněnou organizací pravomoc. Za druhé, DPF EU-U.S. umožní podnikům ve Spojených státech, včetně dceřiných společností evropských podniků se sídlem ve Spojených státech, přijímat osobní údaje z Evropské unie, aby se usnadnily toky údajů, které podporují transatlantické
obchod. Datové toky mezi Spojenými státy a Evropskou unií jsou největší na světě a jsou základem hospodářského vztahu mezi USA a EU v hodnotě 7,1 bilionu dolarů, který podporuje miliony pracovních míst na obou stranách Atlantiku. Podniky, které se spoléhají na transatlantické datové toky, pocházejí ze všech průmyslových odvětví a patří mezi ně jak velké firmy z žebříčku Fortune 500, tak i mnoho malých a středních podniků. Transatlantické datové toky umožňují americkým organizacím zpracovávat údaje potřebné k nabízení zboží, služeb a pracovních příležitostí evropským jednotlivcům.

Ministerstvo je odhodláno úzce a produktivně spolupracovat se svými protějšky z EU na účinné správě a dohledu nad programem rámce ochrany osobních údajů. Tento závazek se odráží ve vývoji a neustálém zdokonalování různých zdrojů, které mají organizacím pomoci s procesem vlastní certifikace, ve vytvoření internetových stránek, které mají poskytovat cílené informace zúčastněným stranám, ve spolupráci s Komisí a evropskými orgány pro ochranu údajů (dále jen "orgány pro ochranu údajů") při vypracovávání pokynů, které objasňují důležité prvky Rámce pro ochranu osobních údajů mezi EU a USA, v osvětové činnosti, která má usnadnit lepší pochopení povinností organizací v oblasti ochrany údajů, a v dohledu a monitorování dodržování požadavků programu ze strany organizací.

Naše pokračující spolupráce s cennými partnery z EU umožní ministerstvu zajistit, aby DPF mezi EU a USA fungoval efektivně. Vláda Spojených států dlouhodobě spolupracuje s Komisí na prosazování společných zásad ochrany údajů, čímž překonává rozdíly v našich právních přístupech a zároveň podporuje obchod a hospodářský růst v Evropské unii a ve Spojených státech. Věříme, že DPF EU a USA, který je příkladem této spolupráce, umožní Komisi vydat nové rozhodnutí o přiměřenosti, které umožní organizacím využívat DPF EU a USA k předávání osobních údajů z Evropské unie do Spojených států v souladu s právem EU.

Správa rámcového programu ochrany osobních údajů a dohled nad ním ze strany ministerstva obchodu

Ministerstvo je pevně odhodláno účinně spravovat program rámce ochrany osobních údajů a dohlížet na něj a vynaloží odpovídající úsilí a vyčlení odpovídající zdroje, aby tento výsledek zajistilo. Ministerstvo bude vést a zpřístupňovat veřejnosti směrodatný seznam amerických organizací, které se samy ministerstvu certifikovaly a prohlásily, že se zavázaly dodržovat zásady (dále jen "seznam rámcového programu ochrany soukromí údajů"), který bude

aktualizovat na základě každoročních žádostí o opětovnou certifikaci předložených zúčastněnými organizacemi.

organizací a vyřazením organizací, pokud dobrovolně odstoupí, nedokončí každoroční recertifikaci v souladu s postupy ministerstva nebo trvale neplní požadavky. Ministerstvo rovněž povede a zpřístupní veřejnosti autoritativní záznam o amerických organizacích, které byly vyřazeny ze seznamu rámce ochrany osobních údajů, a uvede důvod, proč byla každá organizace vyřazena. Výše uvedený autoritativní seznam a evidence budou i nadále veřejně dostupné na internetových stránkách ministerstva věnovaných rámci ochrany soukromí. Na internetových stránkách rámce ochrany osobních údajů bude na viditelném místě uvedeno vysvětlení, že každá organizace vyřazená ze seznamu rámce ochrany osobních údajů musí přestat tvrdit, že se účastní rámce ochrany osobních údajů EU a USA nebo že jej dodržuje a že může získávat osobní údaje podle rámce ochrany osobních údajů EU a USA. Taková organizace nicméně musí nadále uplatňovat zásady na osobní údaje, které obdržela v době, kdy se účastnila rámce pro ochranu osobních údajů EU a USA, a to po dobu, po kterou tyto údaje uchovává. Ministerstvo se v rámci svého zastřešujícího trvalého závazku účinně spravovat program rámce ochrany osobních údajů a dohlížet na něj konkrétně zavazuje k následujícím krokům:

Ověření požadavků na vlastní certifikaci

- Před dokončením první autocertifikace organizace nebo každoroční recertifikace (dále jen "autocertifikace") a zařazením nebo ponecháním organizace na seznamu Rámce pro ochranu osobních údajů ministerstvo ověří, zda organizace splnila alespoň příslušné požadavky stanovené v Doplňkové zásadě pro autocertifikaci týkající se toho, jaké informace musí organizace poskytnout ve svém autocertifikačním podání ministerstvu, a zda ve vhodnou dobu poskytla příslušné zásady ochrany osobních údajů, které informují fyzické osoby o všech 13 vyjmenovaných prvcích stanovených v Zásadě pro oznamování. Ministerstvo ověří, zda organizace má:
    - identifikovala organizaci, která předkládá vlastní certifikaci, jakož i všechny americké subjekty nebo americké dceřiné společnosti organizace, která předkládá vlastní certifikaci a která rovněž dodržuje zásady, na něž se má vztahovat vlastní certifikace;
    - poskytl požadované kontaktní informace o organizaci (*např.* kontaktní informace o konkrétní osobě (osobách) a/nebo kanceláři (kancelářích) v rámci sebeosvědčující se organizace odpovědné za vyřizování stížností, žádostí o přístup a dalších záležitostí vyplývajících z DPF EU a USA);
    - popsal účel (účely), pro který bude organizace shromažďovat a používat osobní údaje získané z Evropské unie;
    - uvedla, jaké osobní údaje by byly získány z Evropské unie na základě DPF EU a USA, a proto by se na ně vztahovalo její vlastní osvědčení;
    - pokud má organizace veřejné internetové stránky, poskytla internetovou adresu, kde jsou příslušné zásady ochrany osobních údajů na těchto stránkách snadno dostupné, nebo pokud organizace nemá veřejné internetové stránky, poskytla odboru kopii příslušných zásad ochrany osobních údajů a místo, kde jsou tyto zásady ochrany osobních údajů k dispozici k nahlédnutí dotčeným osobám (*tj.* dotčeným zaměstnancům, pokud jsou příslušné zásady ochrany osobních údajů v oblasti lidských zdrojů).

nebo veřejnosti, pokud příslušné zásady ochrany osobních údajů nejsou zásadami ochrany osobních údajů v oblasti lidských zdrojů);

- do svých příslušných zásad ochrany osobních údajů ve vhodnou dobu (*tj.* zpočátku pouze do návrhu zásad ochrany osobních údajů poskytnutého spolu s předložením, pokud je toto předložení počáteční vlastní certifikací; jinak do konečných a případně zveřejněných zásad ochrany osobních údajů) zahrnula prohlášení, že dodržuje zásady, a hypertextový odkaz nebo internetovou adresu na tyto zásady.
na webové stránce ministerstva týkající se rámce ochrany osobních údajů (*např.* na domovské stránce nebo na webové stránce Seznam rámce ochrany osobních údajů);
- do svých příslušných zásad ochrany osobních údajů včas zahrnul všech 12 dalších vyjmenovaných prvků uvedených v zásadě oznamování (*např.* možnost dotčené fyzické osoby z EU za určitých podmínek uplatnit závazné rozhodčí řízení; požadavek na zpřístupnění osobních údajů v reakci na zákonné žádosti veřejných orgánů, včetně splnění požadavků národní bezpečnosti nebo prosazování práva; a odpovědnost v případech dalšího předávání třetím stranám);
- určil konkrétní statutární orgán, který má pravomoc projednávat případné stížnosti na organizaci týkající se možných nekalých nebo klamavých praktik a porušení zákonů nebo předpisů upravujících ochranu soukromí (a který je uveden v Zásadách nebo v budoucí příloze k Zásadám);
- identifikoval jakýkoli program ochrany osobních údajů, jehož je organizace členem;
- určil, zda je příslušnou metodou (tj. následnými postupy, které musí zajistit) pro ověřování jeho souladu se Zásadami "vlastní posouzení" (tj. *interní* ověření) nebo "externí kontrola souladu" (tj. ověření třetí stranou), a pokud určil příslušnou metodu jako externí kontrolu souladu, uvedl také třetí stranu, která tuto kontrolu provedla;
- určil vhodný nezávislý opravný mechanismus, který je k dispozici pro řešení stížností podaných podle těchto zásad, a bezplatně poskytl postižené osobě odpovídající opravný prostředek.
    - Pokud si organizace zvolila nezávislý mechanismus odvolání poskytovaný orgánem pro alternativní řešení sporů v soukromém sektoru, uvedla ve svých příslušných zásadách ochrany osobních údajů hypertextový odkaz na příslušnou webovou stránku nebo formulář pro podání stížnosti mechanismu, který je k dispozici pro prošetření nevyřešených stížností podaných podle těchto zásad, nebo jejich webovou adresu.
    - Pokud je organizace buď povinna (*tj.* , pokud jde o údaje o lidských zdrojích předávané z Evropské unie v souvislosti s pracovněprávním vztahem), nebo se rozhodla spolupracovat s příslušnými orgány pro ochranu údajů při vyšetřování a řešení stížností podaných podle Zásad, prohlásila, že se zavázala k takové spolupráci s orgány pro ochranu údajů a k dodržování jejich souvisejících doporučení přijmout konkrétní opatření k dodržování Zásad.

- Oddělení rovněž ověří, zda je předložené vlastní osvědčení organizace v souladu s jejími příslušnými zásadami ochrany osobních údajů. Pokud si sebeosvědčující se organizace přeje zahrnout některý ze svých amerických subjektů nebo amerických dceřiných společností, které mají samostatné příslušné zásady ochrany osobních údajů, ministerstvo rovněž přezkoumá příslušné zásady ochrany osobních údajů těchto zahrnutých subjektů nebo dceřiných společností, aby zajistilo, že obsahují všechny požadované prvky stanovené v

zásadě oznamování.

- Ministerstvo bude spolupracovat se statutárními orgány (*např.* FTC a DOT), aby ověřilo, zda organizace podléhají pravomoci příslušného statutárního orgánu uvedeného v jejich předložených autocertifikacích, pokud má ministerstvo důvod pochybovat o tom, že této pravomoci podléhají.
- Ministerstvo bude spolupracovat se soukromými subjekty alternativního řešení sporů, aby ověřilo, zda jsou organizace aktivně zaregistrovány pro nezávislý mechanismus odvolání uvedený v jejich předložených autocertifikacích; a bude s těmito subjekty spolupracovat, aby ověřilo, zda jsou organizace aktivně zaregistrovány pro externí kontrolu dodržování předpisů uvedenou v jejich
  předložení vlastního osvědčení, přičemž tyto orgány mohou nabízet oba typy služeb.
- Odbor bude spolupracovat s třetí stranou, kterou odbor vybral jako správce finančních prostředků vybraných prostřednictvím poplatku za panel pro ochranu údajů (*tj.* ročního poplatku určeného na pokrytí provozních nákladů panelu pro ochranu údajů), aby ověřil, zda organizace tento poplatek za příslušný rok zaplatily, pokud organizace určily orgány pro ochranu údajů jako příslušný nezávislý opravný mechanismus.
- Ministerstvo bude spolupracovat s třetí stranou vybranou ministerstvem pro správu rozhodčích řízení podle rozhodčího fondu uvedeného v příloze I zásad a pro správu tohoto fondu, aby ověřilo, zda organizace do tohoto fondu přispěly.
- Pokud odbor při přezkoumání předložených žádostí o vlastní certifikaci zjistí nějaké problémy, informuje organizace o tom, že musí všechny tyto problémy vyřešit v příslušné lhůtě stanovené odborem.[2] Oddělení je rovněž informuje, že pokud nebudou reagovat ve lhůtách určených oddělením nebo pokud nedokončí svou autocertifikaci v souladu s postupy oddělení, budou tato autocertifikační podání považována za vyřazená a že veškeré zkreslené informace o účasti organizace na DPF EU a USA nebo o jejím souladu s ním mohou být předmětem donucovacích opatření ze strany FTC, ministerstva dopravy nebo jiného příslušného vládního orgánu. Ministerstvo bude organizace informovat prostřednictvím kontaktních prostředků, které organizace poskytly ministerstvu.

Usnadnění spolupráce s orgány alternativního řešení sporů, které poskytují služby související se zásadami

- Ministerstvo bude spolupracovat se soukromými subjekty pro alternativní řešení sporů, které poskytují nezávislé mechanismy odvolání a které jsou k dispozici pro šetření nevyřešených stížností podaných podle těchto zásad, aby ověřilo, zda splňují alespoň požadavky stanovené v doplňkové zásadě pro řešení sporů a prosazování práva. Ministerstvo ověří, zda:
  - na svých veřejných internetových stránkách zveřejnit informace o zásadách a službách, které poskytují v rámci DPF EU - USA, které musí obsahovat: (1) informace nebo hypertextový odkaz na požadavky Zásad na nezávislé opravné prostředky; (2) hypertextový odkaz na internetové stránky ministerstva pro ochranu osobních údajů; (3) vysvětlení, že jejich služby řešení sporů v rámci DPF EU a USA jsou pro uživatele bezplatné.

[2] *Např.* , pokud jde o opětovné vydání osvědčení, očekává se, že organizace vyřeší všechny tyto otázky do 45 dnů; s výhradou určení jiné, vhodné lhůty ze strany ministerstva.

(4) popis způsobu, jakým lze podat stížnost týkající se Zásad; (5) časový rámec, v němž jsou stížnosti týkající se Zásad vyřizovány; a (6) popis rozsahu možných opravných prostředků. Ministerstvo bude subjektům včas oznamovat podstatné změny v dohledu a správě programu rámce ochrany osobních údajů ze strany ministerstva, pokud se takové změny chystají nebo již byly provedeny a pokud jsou tyto změny relevantní pro úlohu, kterou subjekty plní v rámci rámce ochrany osobních údajů mezi EU a USA;

- zveřejnit výroční zprávu obsahující souhrnné statistické údaje o jejich službách řešení sporů, které musí obsahovat: (1) celkový počet stížností týkajících se Zásad přijatých během vykazovaného roku; (2) typy přijatých stížností;
(3) měření kvality řešení sporů, jako je délka vyřizování stížností, a (4) výsledky přijatých stížností, zejména počet a druhy uložených nápravných opatření nebo sankcí. Ministerstvo poskytne subjektům konkrétní doplňující pokyny k tomu, jaké informace by měly v těchto výročních zprávách poskytovat, přičemž tyto požadavky rozvede (*např.* uvede konkrétní kritéria, která musí stížnost splňovat, aby byla pro účely výroční zprávy považována za stížnost související se Zásadami), a rovněž určí další typy informací, které by měly poskytovat (*např.* pokud subjekt poskytuje také ověřovací služby související se Zásadami, popis toho, jak se subjekt vyhýbá jakýmkoli skutečným nebo potenciálním střetům zájmů v situacích, kdy poskytuje organizaci jak ověřovací služby, tak služby řešení sporů). V dodatečných pokynech poskytnutých ministerstvem bude rovněž uvedeno datum, do kterého by měly být zveřejněny výroční zprávy subjektů za příslušné vykazované období.

Následné kroky vůči organizacím, které si přejí být nebo byly vyřazeny ze seznamu rámce ochrany osobních údajů

- Pokud si organizace přeje odstoupit z FPP EU a USA, bude ministerstvo požadovat, aby organizace odstranila ze všech příslušných zásad ochrany osobních údajů veškeré odkazy na FPP EU a USA, které naznačují, že se nadále účastní FPP EU a USA a že může získávat osobní údaje podle FPP EU a USA (*viz* popis závazku ministerstva vyhledávat nepravdivá tvrzení o účasti). Ministerstvo bude rovněž požadovat, aby organizace vyplnila a předložila ministerstvu příslušný dotazník k ověření:
  - své přání odstoupit;
  - co udělá s osobními údaji, které obdržel na základě DPF EU a USA v době, kdy se účastnil DPF EU a USA: a) ponechá si tyto údaje, bude nadále uplatňovat Zásady na tyto údaje a každoročně potvrdí ministerstvu svůj závazek uplatňovat Zásady na tyto údaje; b) ponechá si tyto údaje a zajistí "přiměřenou" ochranu těchto údajů jiným povoleným způsobem; nebo c) vrátí nebo vymaže všechny tyto údaje ke stanovenému datu a
  - kdo bude v rámci organizace sloužit jako stálé kontaktní místo pro dotazy týkající se zásad.

- Pokud si organizace zvolila bod a), jak je popsáno výše, bude také požadovat, aby každý rok po svém vystoupení vyplnila a předložila odboru (*tj,* k prvnímu výročí odstoupení od smlouvy, jakož i ke každému následujícímu výročí, pokud organizace nezajistí "přiměřenou" ochranu těchto údajů jiným povoleným způsobem nebo pokud všechny tyto údaje nevrátí či nevymaže a neoznámí tuto skutečnost ministerstvu) příslušný dotazník, aby ověřila, jak s těmito osobními údaji naložila, jak naloží s osobními údaji, které nadále uchovává, a kdo bude v organizaci sloužit jako trvalé kontaktní místo pro otázky týkající se zásad.
- Pokud organizace nechala svou autocertifikaci propadnout (*tj.* ani nedokončila každoroční recertifikaci dodržování zásad, ani nebyla vyřazena z rámcového seznamu pro ochranu osobních údajů z jiného důvodu, např. z důvodu odvolání), ministerstvo jí nařídí, aby vyplnila a předložila ministerstvu příslušný dotazník k ověření, zda si přeje zrušit nebo znovu certifikovat:
    - a pokud si přeje odstoupit, dále ověřit, jak naloží s osobními údaji, které obdržela na základě DPF EU a USA v době, kdy se účastnila DPF EU a USA (*viz* předchozí popis toho, co musí organizace ověřit, pokud si přeje odstoupit);
    - a pokud má v úmyslu obnovit certifikaci, dále ověřit, že během doby, kdy mu vypršel status certifikace, uplatňoval zásady na osobní údaje získané v rámci DPF EU a USA, a objasnit, jaké kroky podnikne k vyřešení nevyřešených problémů, které zdržely jeho obnovení certifikace.
- Pokud je organizace vyřazena ze seznamu Rámce pro ochranu osobních údajů z některého z následujících důvodů: a) odstoupení od Rámce pro ochranu osobních údajů EU a USA, b) nevyplnění každoroční opětovné certifikace dodržování zásad (tj. buď proces každoroční recertifikace zahájil, ale nedokončil jej včas, nebo proces každoroční recertifikace vůbec nezahájil), nebo c) "trvalé nedodržování", zašle ministerstvo kontaktní osobě (kontaktním osobám) uvedené (uvedeným) v předloženém sebeosvědčení organizace oznámení, v němž uvede důvod vyřazení a vysvětlí, že organizace musí přestat výslovně nebo nepřímo tvrdit, že se účastní rámce pro ochranu osobních údajů EU a USA nebo že jej dodržuje a že může získávat osobní údaje podle rámce pro ochranu osobních údajů EU a USA. V oznámení, které může obsahovat i další obsah přizpůsobený důvodu vyřazení, bude uvedeno, že organizace, které uvádějí nepravdivé údaje o své účasti v rámci DPF EU a USA nebo o tom, že jsou v souladu s tímto rámcem, včetně případů, kdy uvádějí, že se účastní DPF EU a USA poté, co byly vyřazeny ze seznamu rámce ochrany osobních údajů, mohou být předmětem donucovacích opatření ze strany FTC, ministerstva dopravy nebo jiného příslušného vládního orgánu.

Vyhledávání a řešení falešných žádostí o účast

- Průběžně, pokud organizace: a) odstoupí od účasti v DPF EU a USA, b) nedokončí roční recertifikaci dodržování zásad (*tj.* buď zahájila, ale nedokončila roční recertifikační proces včas, nebo roční recertifikační proces vůbec nezahájila), c) je odstraněna jako účastník DPF EU a USA zejména z důvodu "trvalého nedodržování", nebo d) nedokončí počáteční certifikační proces.

sebeosvědčení o dodržování Zásad (*tj.* zahájila, ale nedokončila včas počáteční proces sebeosvědčení), provede ministerstvo *z moci úřední* opatření k ověření, zda všechny příslušné zveřejněné zásady ochrany osobních údajů organizace neobsahují odkazy na Rámec pro ochranu osobních údajů EU a USA, které by naznačovaly, že se organizace účastní Rámce pro ochranu osobních údajů EU a USA a že může získávat osobní údaje podle Rámce pro ochranu osobních údajů EU a USA. Pokud ministerstvo takové odkazy zjistí, bude organizaci informovat o tom, že ministerstvo případně postoupí záležitost příslušné agentuře k případnému vymáhání, pokud bude organizace i nadále uvádět nepravdivé údaje o své účasti v DPF EU a EU.
DPF V USA. Odbor bude organizaci informovat prostřednictvím kontaktních prostředků, které organizace odboru poskytla, nebo v případě potřeby jiným vhodným způsobem. Pokud organizace odkazy neodstraní ani sama neosvědčí, že splňuje požadavky podle EU-
DPF USA v souladu s postupy ministerstva, ministerstvo *z moci úřední* postoupí záležitost FTC, ministerstvu dopravy nebo jinému příslušnému donucovacímu orgánu nebo přijme jiná vhodná opatření, aby zajistilo řádné používání certifikační značky EU-U.S. DPF;

- Ministerstvo vynaloží další úsilí k odhalení nepravdivých tvrzení o účasti v DPF EU a USA a nesprávného používání certifikační značky DPF EU a USA, včetně organizací, které na rozdíl od výše popsaných organizací nikdy ani nezačaly s procesem vlastní certifikace (*např.* vyhledáváním na internetu s cílem zjistit odkazy na DPF EU a USA v zásadách ochrany osobních údajů organizací). Pokud ministerstvo v rámci tohoto úsilí zjistí nepravdivá tvrzení o účasti v rámci DPF EU a USA a nesprávné používání certifikační značky DPF EU a USA, informuje organizaci o tom, že ministerstvo případně postoupí záležitost příslušné agentuře k případnému vymáhání práva, pokud bude organizace i nadále nepravdivě uvádět svou účast v rámci DPF EU a USA.
  DPF V USA. Oddělení bude organizaci informovat prostřednictvím kontaktních prostředků, pokud je organizace Oddělení poskytla, nebo v případě potřeby jiným vhodným způsobem. Pokud organizace odkazy neodstraní ani sama nepotvrdí soulad s DPF EU-SR v souladu s postupy ministerstva, ministerstvo *z moci úřední* postoupí záležitost FTC, DOT nebo jinému vhodnému donucovacímu orgánu nebo přijme jiná vhodná opatření k zajištění řádného používání certifikační značky DPF EU-SR;
- Ministerstvo neprodleně přezkoumá a vyřeší konkrétní, nepodložené stížnosti týkající se nepravdivých tvrzení o účasti EU a USA na DPF, které obdrží (*např.* stížnosti obdržené od orgánů pro ochranu údajů, nezávislých opravných prostředků poskytovaných orgány pro alternativní řešení sporů v soukromém sektoru, subjektů údajů, podniků z EU a USA a dalších typů třetích stran); a
- Odbor může přijmout další vhodná nápravná opatření. Zkreslená prohlášení vůči ministerstvu mohou být stíhána podle zákona o nepravdivých prohlášeních (18 U.S.C. § 1001).

Provádění pravidelných přezkumů a hodnocení souladu rámcového programu ochrany osobních údajů z *moci úřední.*

- Ministerstvo bude průběžně monitorovat účinné dodržování předpisů organizacemi EU a USA v oblasti DPF, aby zjistilo problémy, které mohou vyžadovat následná opatření. Ministerstvo bude z *moci úřední provádět zejména* běžné namátkové kontroly těchto

organizací

náhodně vybrané organizace DPF EU a USA, jakož i *ad hoc* namátkové kontroly konkrétních organizací EU a USA.
Organizace DPF USA při zjištění potenciálních nedostatků v dodržování předpisů (*např.* , potenciálních nedostatků v dodržování předpisů, na které ministerstvo upozornily třetí strany) ověřit:
a) že kontaktní místo (místa) odpovědné (odpovědná) za vyřizování stížností, žádostí o přístup a dalších záležitostí vyplývajících z dohody mezi EU a USA. b) případně, že veřejně přístupná politika ochrany osobních údajů organizace je snadno dostupná k nahlédnutí veřejnosti jak na veřejných internetových stránkách organizace, tak prostřednictvím hypertextového odkazu na seznamu rámce ochrany osobních údajů; c) že politika ochrany osobních údajů organizace nadále splňuje požadavky na vlastní certifikaci popsané v zásadách a d) že je k dispozici nezávislý mechanismus odvolání určený organizací pro řešení stížností podaných podle rámce ochrany osobních údajů EU a USA. Ministerstvo bude rovněž aktivně sledovat zprávy, které poskytují věrohodné důkazy o nedodržování pravidel ze strany organizací v rámci DPF EU a USA;

- V rámci kontroly dodržování předpisů bude ministerstvo požadovat, aby organizace EU-SA DPF vyplnila a předložila ministerstvu podrobný dotazník, když: (b) organizace uspokojivě neodpovídá na dotazy ministerstva týkající se informací o DPF EU-SA nebo c) existují věrohodné důkazy, že organizace neplní své závazky v rámci DPF EU-SA.
DPF V USA. Pokud ministerstvo zašle organizaci takový podrobný dotazník a organizace na dotazník uspokojivě neodpoví, ministerstvo organizaci informuje, že pokud ministerstvo neobdrží od organizace včasnou a uspokojivou odpověď, postoupí případně záležitost příslušné agentuře k případnému vymáhání práva. Odbor bude organizaci informovat prostřednictvím kontaktních prostředků, které organizace odboru poskytla, nebo v případě potřeby jiným vhodným způsobem. Pokud organizace neposkytne včasnou a uspokojivou odpověď, postoupí odbor z *moci úřední* záležitost FTC, ministerstvu dopravy nebo jinému příslušnému donucovacímu orgánu nebo přijme jiná vhodná opatření k zajištění souladu. V případě potřeby konzultuje ministerstvo tyto kontroly dodržování předpisů s příslušnými orgány pro ochranu údajů a
- Ministerstvo bude pravidelně posuzovat správu a dohled nad programem rámce ochrany osobních údajů, aby zajistilo, že jeho monitorovací úsilí, včetně veškerého takového úsilí vyvíjeného prostřednictvím vyhledávacích nástrojů (*např.* kontrola nefunkčních odkazů na zásady ochrany osobních údajů organizací EU a USA), je vhodné k řešení stávajících problémů a jakýchkoli nových problémů, které se objeví.

Přizpůsobení webových stránek rámce ochrany osobních údajů cílovému publiku

Ministerstvo přizpůsobí webové stránky rámce ochrany osobních údajů tak, aby se zaměřily na následující cílové skupiny: Fyzické osoby z EU, podniky z EU, podniky z USA a orgány pro ochranu údajů. Zahrnutí materiálů určených přímo fyzickým osobám z EU a podnikům z EU usnadní transparentnost několika způsoby. Pokud jde o fyzické osoby z EU, webové stránky budou jasně vysvětlovat: (1) práva, která Rámec pro ochranu osobních údajů mezi EU a USA poskytuje fyzickým osobám z EU; (2) mechanismy odvolání, které mají fyzické osoby z EU k dispozici, pokud se domnívají, že organizace porušila svůj závazek k ochraně osobních údajů.

dodržovat zásady a (3) jak najít informace týkající se organizace v EU.
Vlastní certifikace DPF v USA. Pokud jde o podniky v EU, usnadní to ověřování: (1) zda je organizace účastníkem DPF EU a USA; (2) typ informací, na které se vztahuje vlastní certifikace organizace v rámci DPF EU a USA; (3) zásady ochrany osobních údajů, které se vztahují na zahrnuté informace; a (4) metodu, kterou organizace používá k ověření dodržování zásad. Pokud jde o podniky v USA, bude jasně vysvětleno: (1) výhody účasti v DPF EU-U.S.; (2) jak se k DPF EU-U.S. připojit, jakož i jak se k DPF EU-U.S. znovu certifikovat a jak z něj vystoupit; a (3) jak Spojené státy spravují a prosazují DPF EU-U.S.. Zahrnutí materiálů určených přímo orgánům pro ochranu údajů (*např.* informace o specializovaném kontaktním místě ministerstva pro orgány pro ochranu údajů a hypertextový odkaz na obsah související se zásadami na internetových stránkách FTC) usnadní spolupráci i transparentnost. Oddělení bude rovněž *ad hoc spolupracovat* s Komisí a Evropským sborem pro ochranu osobních údajů.
(dále jen "EDPB"), aby vypracoval další aktuální materiály (*např.* odpovědi na často kladené otázky) pro použití na internetových stránkách rámce ochrany osobních údajů, pokud by takové informace usnadnily účinnou správu a dohled nad programem rámce ochrany osobních údajů.

Usnadnění spolupráce s orgány pro ochranu údajů

V zájmu rozšíření možností spolupráce s orgány pro ochranu údajů bude ministerstvo udržovat zvláštní kontaktní místo na ministerstvu, které bude působit jako styčný bod s orgány pro ochranu údajů. V případech, kdy se orgán pro ochranu údajů bude domnívat, že organizace EU a USA v oblasti DPF nedodržuje zásady, včetně případů, kdy si na něj stěžuje fyzická osoba z EU, bude se moci obrátit na specializované kontaktní místo na ministerstvu a předat organizaci k dalšímu přezkoumání. Ministerstvo vyvine maximální úsilí, aby usnadnilo vyřešení stížnosti s organizací DPF EU a USA. Do 90 dnů od obdržení stížnosti poskytne ministerstvo orgánu pro ochranu údajů aktuální informace. Vyhrazené kontaktní místo bude rovněž přijímat postoupení týkající se organizací, které nepravdivě tvrdí, že se účastní DPF EU-SA. Specializované kontaktní místo bude sledovat všechna postoupení od orgánů pro ochranu údajů, která ministerstvo obdrží, a ministerstvo poskytne v rámci níže popsaného společného přezkumu zprávu, v níž bude souhrnně analyzovat stížnosti, které každoročně obdrží. Specializované kontaktní místo bude pomáhat orgánům pro ochranu údajů, které hledají informace týkající se vlastní certifikace konkrétní organizace nebo její předchozí účasti v rámci DPF EU a USA, a specializované kontaktní místo bude odpovídat na dotazy orgánů pro ochranu údajů týkající se provádění konkrétních požadavků DPF EU a USA. Oddělení bude rovněž spolupracovat s Komisí a EDPB na procesních a administrativních aspektech panelu DPA, včetně stanovení vhodných postupů pro rozdělování finančních prostředků vybraných prostřednictvím poplatku panelu DPA. Chápeme, že Komise bude spolupracovat s oddělením, aby usnadnila řešení jakýchkoli problémů, které mohou v souvislosti s těmito postupy vzniknout. Kromě toho ministerstvo poskytne orgánům pro ochranu údajů materiály týkající se DPF EU a USA, které budou moci umístit na své vlastní internetové stránky, aby se zvýšila transparentnost pro fyzické osoby a podniky v EU. Větší informovanost o DPF EU a USA a o právech a povinnostech, které z něj vyplývají, by měla usnadnit identifikaci problémů, které se objeví, aby mohly být náležitě řešeny.

Plnit své závazky podle přílohy I Zásad

Ministerstvo bude plnit své závazky podle přílohy I zásad, včetně vedení seznamu rozhodců vybraných společně s Komisí na základě nezávislosti, bezúhonnosti a odbornosti, a bude případně podporovat třetí stranu vybranou ministerstvem ke správě rozhodčích řízení podle přílohy I zásad a ke správě rozhodčího fondu uvedeného v příloze I zásad.[3] Ministerstvo bude s třetí stranou spolupracovat mimo jiné na ověření, zda třetí strana spravuje internetové stránky s pokyny k rozhodčímu řízení, včetně: 1) způsobu zahájení řízení a předkládání dokumentů; 2) seznamu rozhodců vedeného ministerstvem a způsobu výběru rozhodců z tohoto seznamu; 3) rozhodčích postupů a kodexu chování rozhodců přijatých ministerstvem a Komisí;[4] a 4) výběru a placení poplatků za rozhodčí řízení. Kromě toho bude ministerstvo ve spolupráci s třetí stranou pravidelně přezkoumávat fungování rozhodčího fondu, včetně potřeby upravit výši příspěvků nebo stropy (*tj.* maximální částky) nákladů na rozhodčí řízení, a zváží mimo jiné počet rozhodčích řízení a náklady a načasování rozhodčích řízení s tím, že na organizace DPF EU a USA nebude uvalena nadměrná finanční zátěž. Ministerstvo oznámí Komisi výsledek těchto přezkumů s třetí stranou a poskytne Komisi předběžné oznámení o případných úpravách výše příspěvků.

Provádění společných přezkumů fungování DPF EU a USA

Ministerstvo a případně další agentury budou pravidelně pořádat schůzky s Komisí, zúčastněnými orgány pro ochranu údajů a příslušnými zástupci EDPB, na nichž bude ministerstvo poskytovat aktuální informace o DPF EU a USA. Součástí schůzek bude diskuse o aktuálních otázkách souvisejících s fungováním, prováděním, dohledem a prosazováním programu rámce ochrany osobních údajů. Schůzky mohou podle potřeby zahrnovat diskusi o souvisejících tématech, jako jsou jiné mechanismy předávání údajů, které využívají záruk v rámci DPF EU a USA.

Aktualizace zákonů

Ministerstvo vynaloží přiměřené úsilí, aby Komisi informovalo o podstatném vývoji práva ve Spojených státech, pokud je relevantní pro DPF mezi EU a USA, a to v následujících bodech

[3] Mezinárodní centrum pro řešení sporů (dále jen "ICDR"), mezinárodní divize Americké asociace rozhodců (dále jen "AAA") (dále jen "ICDR-AAA"), bylo ministerstvem vybráno, aby spravovalo rozhodčí řízení podle zásad a spravovalo rozhodčí fond uvedený v příloze I těchto zásad.

[4] Dne 15. září 2017 se ministerstvo a Komise dohodly na přijetí souboru rozhodčích pravidel, jimiž se řídí závazná rozhodčí řízení popsaná v příloze I Zásad, jakož i kodexu chování rozhodců, který je v souladu s obecně uznávanými etickými normami pro obchodní rozhodce a přílohou I Zásad. Ministerstvo a Komise se dohodly na úpravě pravidel rozhodčího řízení a kodexu chování tak, aby odrážely aktualizace v rámci DPF EU a USA, a ministerstvo bude na těchto aktualizacích spolupracovat s ICDR-AAA.

oblast ochrany soukromí a omezení a záruky, které se vztahují na přístup amerických orgánů k osobním údajům a jejich následné využití.

Přístup vlády USA k osobním údajům

Spojené státy vydaly exekutivní příkaz 14086 "Posílení záruk pro zpravodajské činnosti Spojených států" a 28 CFR část 201, kterým se mění předpisy ministerstva spravedlnosti za účelem zřízení Soudu pro přezkum ochrany údajů (dále jen "DPRC"), které poskytují silnou ochranu osobních údajů, pokud jde o přístup vlády k údajům pro účely národní bezpečnosti. Poskytovaná ochrana zahrnuje: posílení záruk ochrany soukromí a občanských svobod, aby se zajistilo, že činnosti amerického signálového zpravodajství jsou nezbytné a přiměřené při sledování stanovených cílů národní bezpečnosti; zřízení nového mechanismu nápravy s nezávislou a závaznou pravomocí; a posílení stávajícího přísného a vrstevnatého dohledu nad činnostmi amerického signálového zpravodajství. Prostřednictvím těchto ochranných opatření se mohou fyzické osoby z EU domáhat nápravy u nového víceúrovňového mechanismu nápravy, který zahrnuje nezávislý Výbor pro odškodnění, jenž by se skládal z osob vybraných mimo vládu USA, které by měly plnou pravomoc rozhodovat o stížnostech a v případě potřeby nařizovat nápravná opatření. Ministerstvo bude vést evidenci osob z EU, které podají kvalifikovanou stížnost podle výkonné vyhlášky 14086 a části 28 CFR 201. Pět let po datu tohoto dopisu a poté každých pět let bude ministerstvo kontaktovat příslušné agentury ohledně toho, zda byly informace týkající se přezkumu kvalifikovaných stížností nebo přezkumu jakýchkoli žádostí o přezkum předložených DPRC odtajněny. Pokud byly takové informace odtajněny, bude ministerstvo spolupracovat s příslušným orgánem pro ochranu údajů, aby informovalo jednotlivce z EU. Tato vylepšení potvrzují, že s osobními údaji EU předávanými do Spojených států bude nakládáno v souladu s právními požadavky EU, pokud jde o přístup vlády k údajům.

Na základě Zásad, výkonného nařízení 14086, 28 CFR část 201 a doprovodných dopisů a materiálů, včetně závazků ministerstva týkajících se správy a dohledu nad programem rámce ochrany osobních údajů, očekáváme, že Komise rozhodne, že rámec ochrany osobních údajů mezi EU a USA poskytuje odpovídající ochranu pro účely práva EU a že předávání údajů z Evropské unie bude pokračovat organizacím, které se účastní rámce ochrany osobních údajů mezi EU a USA. Očekáváme také, že předávání údajů organizacím v USA prováděné na základě standardních smluvních doložek EU nebo závazných podnikových pravidel EU bude dále usnadněno podmínkami těchto ujednání.

S

pozdravem,

Marisa Lago

PŘÍLOHA IV

Didier Reynders komisař pro
spravedlnost Evropská komise
Rue de la Loi / Wetstraat 200
1049 Brusel
Belgie

Vážený pane komisaři Reyndersi:

Federální obchodní komise Spojených států amerických (dále jen "FTC") si váží příležitosti zabývat se svou úlohou v oblasti prosazování práva v souvislosti se zásadami rámce EU a USA pro ochranu soukromí ("EU-U.S. DPF"). FTC se dlouhodobě zasazuje o ochranu spotřebitelů a soukromí napříč hranicemi a jsme odhodláni prosazovat aspekty tohoto rámce týkající se obchodního sektoru. FTC plní tuto úlohu od roku 2000 v souvislosti s rámcem USA-EU Safe Harbor a nejnověji od roku 2016 v souvislosti s rámcem EU-U.S. Privacy Shield.[1] Dne 16. července 2020 Soudní dvůr Evropské unie (dále jen "SDEU") zrušil rozhodnutí Evropské komise o přiměřenosti, které je základem rámce štítu EU-USA na ochranu soukromí, na základě jiných otázek než obchodních zásad, které FTC prosazovala. Spojené státy a Evropská komise od té doby jednaly o rámci EU-USA pro ochranu soukromí s cílem řešit toto rozhodnutí Soudního dvora EU.

Píši vám, abych potvrdil závazek FTC důsledně prosazovat zásady DPF mezi EU a USA. Zejména potvrzujeme náš závazek ve třech klíčových oblastech: (1) prioritizace postoupení a vyšetřování; (2) vyhledávání a monitorování příkazů; a (3) spolupráce při prosazování s orgány EU pro ochranu údajů (dále jen "orgány DPA").

I. Úvod

a. Práce FTC v oblasti prosazování ochrany soukromí a politiky

FTC má rozsáhlé občanskoprávní pravomoci k prosazování ochrany spotřebitele a hospodářské soutěže v obchodní sféře. V rámci svého mandátu v oblasti ochrany spotřebitele prosazuje FTC celou řadu zákonů na ochranu soukromí a bezpečnosti spotřebitelů a jejich údajů. Hlavní zákon, který FTC prosazuje, zákon FTC, zakazuje "nekalé" nebo "klamavé" jednání nebo praktiky v obchodě nebo při jeho ovlivňování.[2] FTC rovněž prosazuje cílené zákony, které chrání

[1] Dopis předsedkyně Edith Ramirezové Věře Jourové, komisařce Evropské komise pro spravedlnost, spotřebitele a rovnost pohlaví, Describing Federal Trade Commission Enforcement of the New EU-U.S. Privacy Shield Framework (29. února 2016), *k dispozici na* https://www.ftc.gov/legal-library/browse/cases- proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers- gender-equality-european. FTC se rovněž dříve zavázala prosazovat program "bezpečného přístavu" mezi USA a EU. Dopis Roberta Pitofského, předsedy FTC, Johnu Moggovi, řediteli GŘ pro vnitřní trh Evropské komise (14. července 2000), *k dispozici na adrese* https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor- principles-and-transmission-to-european-commission. Tento dopis nahrazuje tyto dřívější závazky.

[2] 15 U.S.C. § 45(a). FTC nemá pravomoc rozhodovat o prosazování trestního práva nebo o záležitostech národní bezpečnosti. FTC nemůže zasáhnout ani do většiny jiných vládních akcí. Kromě toho existují výjimky z pravomoci FTC ve vztahu k obchodním činnostem, včetně bank, leteckých společností, pojišťovnictví a běžného obchodního styku.

informace týkající se zdraví, úvěrů a dalších finančních záležitostí, jakož i informace o dětech online, a vydala prováděcí předpisy ke každému z těchto zákonů.[3]

FTC také v poslední době realizovala řadu iniciativ na posílení naší práce v oblasti ochrany soukromí.

V srpnu 2022 FTC oznámila, že zvažuje pravidla, která by potlačila škodlivé komerční sledování a nedostatečné zabezpečení dat.[4] Cílem projektu je vytvořit spolehlivý veřejný záznam, který by poskytl informace o tom, zda by FTC měla vydat pravidla pro řešení praktik komerčního dohledu a zabezpečení údajů a jak by tato pravidla měla případně vypadat. Uvítali jsme připomínky zúčastněných stran z EU k této a dalším iniciativám.

Na našich konferencích "PrivacyCon" se i nadále scházejí přední výzkumní pracovníci, aby diskutovali o nejnovějším výzkumu a trendech týkajících se ochrany soukromí a bezpečnosti dat spotřebitelů. Rovněž jsme zvýšili schopnost naší agentury držet krok s technologickým vývojem, který je v centru naší práce v oblasti ochrany soukromí, a vytvořili jsme rostoucí tým technologů a interdisciplinárních výzkumníků. Jak víte, oznámili jsme také společný dialog s vámi a vašimi kolegy z Evropské komise, jehož součástí je řešení takových témat souvisejících s ochranou soukromí, jako jsou temné vzory a obchodní modely vyznačující se všudypřítomným shromažďováním údajů.[5] Nedávno jsme také vydali zprávu pro Kongres, ve které jsme varovali před škodami spojenými s využíváním umělé inteligence ("AI") k řešení škod online identifikovaných Kongresem. Tato zpráva vyjádřila obavy týkající se nepřesnosti, zaujatosti, diskriminace a plíživého komerčního dohledu.[6]

b. Právní ochrana v USA ve prospěch spotřebitelů v EU

Rámec pro ochranu osobních údajů mezi EU a USA funguje v kontextu širšího prostředí ochrany osobních údajů v USA, které rovněž chrání spotřebitele v EU řadou způsobů. Zákaz nekalých nebo klamavých jednání nebo praktik stanovený zákonem o FTC se neomezuje pouze na ochranu spotřebitelů v USA před americkými společnostmi, neboť zahrnuje i ty praktiky, které (1) způsobují nebo mohou způsobit rozumně předvídatelnou újmu ve Spojených státech

činnosti poskytovatelů telekomunikačních služeb. FTC rovněž nemá pravomoc nad většinou neziskových organizací, ačkoli má pravomoc nad fiktivními charitativními organizacemi nebo jinými neziskovými organizacemi, které ve skutečnosti působí za účelem zisku. FTC má rovněž pravomoc nad neziskovými organizacemi, které působí za účelem zisku svých ziskových členů, včetně poskytování značných ekonomických výhod těmto členům. V některých případech je pravomoc FTC souběžná s pravomocí jiných orgánů činných v trestním řízení. S federálními a státními orgány jsme si vytvořili pevné pracovní vztahy a úzce s nimi spolupracujeme při koordinaci vyšetřování nebo v případě potřeby při postoupení případu.

[3] *Viz* Soukromí a bezpečnost, https://www.ftc.gov/business-guidance/privacy-security.

[4] *Viz* FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (11. srpna 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

[5] *Viz* společné tiskové prohlášení Didiera Reynderse, komisaře Evropské komise pro spravedlnost, a Liny Khan, předsedkyně Federální obchodní komise Spojených států (30. března 2022), *dostupné na adrese* https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

[6] *Viz* Zpráva FTC varuje před používáním umělé inteligence v boji proti problémům online (16. června 2022), *dostupná na adrese* https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial- intelligence-combat-online-problems.

nebo 2) zahrnují podstatné jednání ve Spojených státech. Dále může FTC při ochraně zahraničních spotřebitelů použít všechny opravné prostředky, které jsou k dispozici na ochranu domácích spotřebitelů.[7]

FTC prosazuje také další cílené zákony, jejichž ochrana se vztahuje i na spotřebitele mimo USA, jako je zákon o ochraně soukromí dětí na internetu (Children's Online Privacy Protection Act, COPPA). COPPA mimo jiné vyžaduje, aby provozovatelé webových stránek a online služeb zaměřených na děti nebo stránek pro širokou veřejnost, kteří vědomě shromažďují osobní údaje od dětí mladších 13 let, poskytli rodičům oznámení a získali ověřitelný souhlas rodičů. Webové stránky a služby se sídlem v USA, na které se vztahuje COPPA a které shromažďují osobní údaje od zahraničních dětí, jsou povinny dodržovat COPPA. Webové stránky a online služby se sídlem v zahraničí musí rovněž dodržovat COPPA, pokud jsou určeny dětem ve Spojených státech nebo pokud vědomě shromažďují osobní údaje od dětí ve Spojených státech. Kromě federálních zákonů USA, které prosazuje FTC, mohou navíc spotřebitelům v EU poskytovat další výhody i další federální a státní zákony na ochranu spotřebitele, porušení ochrany osobních údajů a soukromí.

c. Činnost FTC v oblasti vymáhání práva

FTC zahájila řízení jak v rámci "bezpečného přístavu" mezi USA a EU, tak v rámci štítu na ochranu soukromí mezi EU a USA a pokračovala v prosazování štítu na ochranu soukromí mezi EU a USA i poté, co Soudní dvůr EU zrušil rozhodnutí o přiměřenosti, na němž je založen rámec štítu na ochranu soukromí mezi EU a USA.[8] Několik nedávných stížností FTC obsahovalo body, v nichž se tvrdilo, že firmy porušily zásady EU a EU pro ochranu soukromí. ustanovení amerického štítu na ochranu soukromí, včetně řízení proti společnosti Twitter,[9] CafePress,[10] a Flo.[11] V řízení o vymáhání práva proti společnosti Twitter FTC zajistila, aby společnost Twitter zaplatila 150 milionů dolarů za porušení dřívějšího příkazu FTC, které se týkalo praktik ovlivňujících více než 140 milionů zákazníků, včetně porušení zásady 5 štítu na ochranu soukromí mezi EU a USA (integrita údajů a omezení účelu). Příkaz agentury dále vyžaduje, aby společnost Twitter umožnila uživatelům používat bezpečné vícefaktorové metody ověřování, které nevyžadují, aby uživatelé poskytovali svá telefonní čísla.

Ve věci *CafePress* FTC tvrdila, že společnost nezabezpečila citlivé informace spotřebitelů, zatajila závažné narušení bezpečnosti údajů a porušila zásady 2 (možnost volby), 4 (bezpečnost) a 6 (přístup) štítu EU-USA na ochranu soukromí. Příkaz FTC vyžaduje, aby společnost nahradila nedostatečná ověřovací opatření vícefaktorovým ověřováním, podstatně omezila množství údajů, které shromažďuje a uchovává, šifrovala čísla sociálního zabezpečení a nechala třetí stranu posoudit své programy zabezpečení informací a poskytla FTC kopii, kterou lze zveřejnit.

---

[7] 15 U.S.C. § 45(a)(4)(B). Dále "nekalé nebo klamavé jednání nebo praktiky" zahrnují takové jednání nebo praktiky týkající se zahraničního obchodu, které i) způsobují nebo mohou způsobit rozumně předvídatelnou újmu na území Spojených států; nebo ii) zahrnují podstatné jednání, k němuž dochází na území Spojených států. 15 U.S.C. § 45(a)(4)(A).

[8] Seznam záležitostí týkajících se bezpečného přístavu FTC a štítu na ochranu soukromí naleznete v příloze A. Tato donucovací opatření se týkala jak nepravdivých tvrzení o účasti na předchozích rámcích, tak porušení věcných požadavků.

[9] *Viz* FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads (25. května 2022), *k dispozici na adrese* https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using- account-security-data-sell-targeted-ads.

[10] *Viz* FTC Takes Action Against CafePress for Data Breach Cover Up (15. března 2022), *k dispozici na adrese* https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover. [11] *Viz* FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others (22. června 2021), *dostupné na* https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

Ve zprávě *Flo* FTC uvedla, že aplikace pro sledování plodnosti poskytla zdravotní údaje uživatelů třetím stranám, které se zavázaly tyto údaje uchovávat v tajnosti. Stížnost FTC konkrétně uvádí interakce společnosti se spotřebiteli v EU a to, že Flo porušila zásady štítu na ochranu soukromí mezi EU a USA č. 1 (oznámení), č. 2 (možnost volby), č. 3 (odpovědnost za další předávání) a č. 5 (integrita údajů a omezení účelu). Příkaz agentury mimo jiné vyžaduje, aby společnost Flo informovala dotčené uživatele o zveřejnění jejich osobních údajů a aby dala pokyn jakékoli třetí straně, která obdržela zdravotní údaje uživatelů, aby tyto údaje zničila. Důležité je, že příkazy FTC chrání všechny spotřebitele na celém světě, kteří přicházejí do styku s americkým podnikem, nejen ty spotřebitele, kteří podali stížnost.

Mnoho případů prosazování pravidel Safe Harbor mezi USA a EU a Štítu na ochranu soukromí se v minulosti týkalo organizací, které provedly počáteční vlastní certifikaci prostřednictvím ministerstva obchodu, ale neudržely svou roční vlastní certifikaci, zatímco se nadále prezentovaly jako stávající účastníci. Další případy se týkaly nepravdivých tvrzení o účasti organizací, které nikdy nedokončily počáteční vlastní certifikaci prostřednictvím ministerstva obchodu. V řadě případů FTC vydala správní předvolání adresovaná certifikovaným společnostem, aby zkontrolovala, zda nedošlo k podstatnému porušení povinností vyplývajících ze štítu na ochranu soukromí. Do budoucna očekáváme, že se naše úsilí v oblasti prosazování právních předpisů bude dále zaměřovat na typy podstatných porušení zásad DPF mezi EU a USA, které jsou uváděny v případech, jako jsou Twitter, CafePress a Flo. Ministerstvo obchodu bude mezitím spravovat a dohlížet na proces autocertifikace, vést autoritativní seznam účastníků DPF mezi EU a USA a řešit další otázky týkající se nároků na účast v programu.[12] Důležité je, že organizace, které si nárokují účast v DPF EU a USA, mohou podléhat hmotněprávnímu vymáhání zásad DPF EU a USA, i když neprovedou nebo neudrží vlastní certifikaci prostřednictvím ministerstva obchodu.

II. Prioritizace postoupení a vyšetřování

Stejně jako v rámci "bezpečného přístavu" mezi USA a EU a v rámci štítu na ochranu soukromí mezi EU a USA se FTC zavazuje přednostně posuzovat postoupení zásad DPF mezi EU a USA od ministerstva obchodu a členských států EU. Rovněž budeme přednostně zvažovat postoupení případů nedodržování zásad DPF EU a USA od samoregulačních organizací pro ochranu soukromí a dalších nezávislých orgánů pro řešení sporů.

Pro usnadnění postoupení v rámci DPF EU - USA z členských států EU vytvořila FTC standardizovaný postup postoupení a poskytla členským státům EU pokyny ohledně typu informací, které by FTC nejlépe pomohly při vyšetřování postoupení. V rámci tohoto úsilí FTC určila kontaktní místo agentury pro postoupení případů z členských států EU. Nejužitečnější je, pokud postupující orgán provedl předběžné šetření údajného porušení a může s FTC při šetření spolupracovat.

Po obdržení takového postoupení od ministerstva obchodu, členského státu EU nebo samoregulační organizace či jiných nezávislých orgánů pro řešení sporů může FTC přijmout řadu opatření k řešení vznesených problémů. Například může přezkoumat organizaci.

[12] Dopis Marisy Lagové, náměstkyně ministra obchodu pro mezinárodní obchod, ctihodnému Didieru Reyndersovi,

komisaři pro spravedlnost Evropské komise.

zásady ochrany osobních údajů, získat další informace přímo od organizace nebo od třetích stran, navázat kontakt s odkazujícím subjektem, posoudit, zda existuje vzorec porušování nebo významný počet dotčených spotřebitelů, určit, zda se postoupení týká otázek, které spadají do působnosti ministerstva obchodu, posoudit, zda by bylo užitečné vyvinout další úsilí, aby byli účastníci trhu upozorněni, a případně zahájit řízení o vymáhání práva.

Kromě upřednostňování zásad DPF EU a USA se na ně obracejí ministerstvo obchodu, členské státy EU a samoregulační organizace pro ochranu soukromí nebo jiné nezávislé orgány pro řešení sporů,[13] bude FTC v případě potřeby pokračovat ve vyšetřování významných porušení zásad DPF EU a USA z vlastní iniciativy, přičemž využije celou řadu nástrojů. V rámci programu FTC na vyšetřování otázek ochrany soukromí a bezpečnosti týkajících se obchodních organizací agentura běžně zkoumala, zda dotčený subjekt činil prohlášení o štítu EU-USA na ochranu soukromí. Pokud subjekt taková prohlášení učinil a šetření odhalilo zjevné porušení zásad štítu EU-USA na ochranu soukromí, zahrnula FTC obvinění z porušení štítu EU-USA na ochranu soukromí do svých donucovacích opatření. V tomto proaktivním přístupu budeme pokračovat, nyní s ohledem na zásady ochrany soukromí mezi EU a USA.

III. Vyhledávání a sledování příkazů

FTC rovněž potvrzuje svůj závazek usilovat o vydání exekučních příkazů a sledovat jejich dodržování, aby zajistila dodržování zásad DPF mezi EU a USA. Budeme vyžadovat dodržování zásad DPF EU a USA prostřednictvím různých vhodných ustanovení o soudních příkazech v budoucích příkazech FTC týkajících se zásad DPF EU a USA. Porušení správních příkazů FTC může vést k občanskoprávním sankcím až do výše 46 517 USD za každé porušení nebo 46 517 USD za každý den v případě pokračujícího porušování,[14] což v případě praktik, které se týkají mnoha spotřebitelů, může činit miliony dolarů. Každý souhlasný příkaz obsahuje také ustanovení o podávání zpráv a dodržování předpisů. Subjekty, na které se vztahuje příkaz, musí po určitý počet let uchovávat dokumenty prokazující dodržování předpisů. S příkazy musí být rovněž seznámeni zaměstnanci odpovědní za zajištění jejich dodržování.

FTC systematicky sleduje dodržování stávajících nařízení o zásadách štítu na ochranu soukromí mezi EU a USA, stejně jako u všech svých nařízení, a v případě potřeby podává žaloby na jejich vymáhání.[15] Důležité je, že příkazy FTC budou i nadále chránit všechny spotřebitele na celém světě, kteří s podnikem přicházejí do styku, nejen ty spotřebitele, kteří podali stížnost. Nakonec bude FTC vést online seznam společností, na které se vztahují příkazy získané v souvislosti s prosazováním zásad DPF EU a USA.[16]

---

[13] Ačkoli FTC neřeší ani nezprostředkovává individuální stížnosti spotřebitelů, potvrzuje, že bude upřednostňovat postoupení zásad DPF EU a USA od orgánů EU pro ochranu údajů. Kromě toho FTC využívá stížnosti ve své databázi Consumer Sentinel, která je přístupná mnoha dalším orgánům činným v trestním řízení, k identifikaci trendů, stanovení priorit v oblasti prosazování práva a určení potenciálních cílů vyšetřování. Fyzické osoby v EU mohou k podání stížnosti FTC využít stejný systém stížností, který je k dispozici spotřebitelům v USA, a to na adrese https://reportfraud.ftc.gov/. V případě individuálních stížností na zásady DPF mezi EU a USA však může být pro fyzické osoby z EU nejužitečnější podat stížnost orgánu pro ochranu údajů nebo nezávislému orgánu pro řešení sporů ve svém členském státě.

[14] 15 U.S.C. § 45(m); 16 C.F.R. § 1.98. Tato částka se pravidelně upravuje o inflaci.

[15] V loňském roce FTC odhlasovala zefektivnění procesu vyšetřování opakovaných přestupků. *Viz* FTC Authorizes Investigations into Key Enforcement Priorities (1. července 2021), *dostupné na adrese*

https://www.ftc.gov/news- events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities.

[16] *Srov.* https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

IV. Spolupráce s orgány EU pro ochranu údajů v oblasti vymáhání práva

FTC uznává důležitou roli, kterou mohou hrát orgány pro ochranu údajů v EU v souvislosti s dodržováním zásad DPF mezi EU a USA, a podporuje intenzivnější konzultace a spolupráci v oblasti prosazování práva. Koordinovaný přístup k výzvám, které přináší současný vývoj na digitálním trhu a obchodní modely náročné na údaje, je totiž stále důležitější. FTC si bude vyměňovat informace o postoupení s předávajícími donucovacími orgány, včetně stavu postoupení, s výhradou zákonů a omezení týkajících se důvěrnosti. V rozsahu, v jakém je to možné vzhledem k počtu a druhu obdržených postoupení, budou poskytnuté informace zahrnovat hodnocení postoupených záležitostí, včetně popisu významných vznesených otázek a veškerých opatření přijatých k řešení porušení zákona v rámci pravomoci FTC. FTC bude rovněž poskytovat zpětnou vazbu orgánu, který postoupil případ, o typech obdržených postoupení, aby se zvýšila účinnost úsilí o řešení protiprávního jednání. Pokud si postupující orgán pro vymáhání práva vyžádá informace o stavu konkrétního postoupení pro účely vedení vlastního řízení o vymáhání práva, FTC odpoví s ohledem na počet posuzovaných postoupení a s výhradou důvěrnosti a dalších právních požadavků.

FTC bude rovněž úzce spolupracovat s orgány EU pro ochranu údajů a poskytovat jim pomoc při prosazování práva. Ve vhodných případech by to mohlo zahrnovat sdílení informací a pomoc při vyšetřování podle amerického zákona SAFE WEB Act, který opravňuje FTC k pomoci zahraničním orgánům činným v trestním řízení, pokud zahraniční orgán prosazuje zákony zakazující praktiky, které jsou v podstatě podobné těm, jež jsou zakázány zákony, které prosazuje FTC.[17] V rámci této pomoci může FTC sdílet informace získané v souvislosti s vyšetřováním FTC, vydávat soudní příkazy jménem orgánu pro ochranu údajů EU, který provádí vlastní vyšetřování, a vyžadovat ústní svědectví od svědků nebo obžalovaných v souvislosti s řízením orgánu pro ochranu údajů o prosazování práva, s výhradou požadavků zákona U.S. SAFE WEB Act. FTC tuto pravomoc pravidelně využívá k pomoci jiným orgánům po celém světě v případech týkajících se ochrany soukromí a spotřebitelů.

Kromě konzultací s příslušnými orgány EU pro ochranu údajů o konkrétních případech se FTC bude účastnit pravidelných schůzek s určenými zástupci Evropského sboru pro ochranu osobních údajů (dále jen "EDPB"), na nichž se bude obecně diskutovat o tom, jak zlepšit spolupráci při prosazování práva. FTC se bude spolu s ministerstvem obchodu, Evropskou komisí a zástupci EDPB rovněž účastnit pravidelného přezkumu rámce pro ochranu osobních údajů mezi EU a USA s cílem projednat jeho provádění. FTC rovněž podporuje vývoj nástrojů, které posílí spolupráci při prosazování práva s orgány pro ochranu osobních údajů v EU, jakož i s dalšími orgány pro prosazování práva na ochranu soukromí na celém světě. FTC s potěšením potvrzuje svůj závazek prosazovat v komerčním sektoru

[17] Při rozhodování, zda uplatnit svou pravomoc podle zákona U.S. SAFE WEB Act, FTC mimo jiné zvažuje: "B) zda by vyhovění žádosti poškodilo veřejný zájem Spojených států a C) zda se vyšetřování nebo donucovací řízení dožadující agentury týká jednání nebo praktik, které způsobují nebo mohou způsobit újmu významnému počtu osob.". 15 U.S.C. § 46(j)(3). Tato pravomoc se nevztahuje na prosazování právních předpisů v oblasti hospodářské

soutěže.

aspekty DPF EU a USA. Naše partnerství s kolegy z EU považujeme za důležitou součást zajištění ochrany soukromí našich i vašich občanů.

S pozdravem,

Lina M. Khan

Předseda

Federální obchodní komise

Příloha A

Prosazování štítu na ochranu soukromí a bezpečného přístavu

	Spis/FTC č.	Případ	Odkaz
1	Spis FTC č. 2023062 Věc č. 3:22-cv-03070 (N.D. Cal.)	USA v. **Twitter, Inc.**	Twitter
2	Spis FTC č. 192 3209	Ve věci společnosti Residual Pumpkin Entity, LLC, dříve d/b/a **CafePress,** a PlanetArt, LLC, d/b/a **CafePress**	CafePress
3	Spis FTC č. 192 3133 Spis č. C-4747	Ve věci společnosti **Flo Health, Inc.**	Flo Health
4	Spis FTC č. 192 3050 Spis č. C-4723	Ve věci společnosti **Ortho-Clinical Diagnostics, Inc.**	Ortho-Clinical
5	Spis FTC č. 192 3092 Spis č. C-4709	Ve věci společnosti **T&M Protection, LLC**	Ochrana T&M
6	Spis FTC č. 192 3084 Spis č. C-4704	Ve věci společnosti **TDARX, Inc.**	TDARX
7	Spis FTC č. 192 3093 Spis č. C-4706	Ve věci společnosti **Global Data Vault, LLC**	Globální data
8	Spis FTC č. 192 3078 Spis č. C-4703	Ve věci společnosti **Incentive Services, Inc.**	Motivačn í služby
9	Spis FTC č. 192 3090 Spis č. C-4705	Ve věci společnosti **Click Labs, Inc.**	Click Labs
10	Spis FTC č. 182 3192 Spis č. C-4697	Ve věci společnosti **Medable, Inc.**	Medable
11	Spis FTC č. 182 3189 Spis č. 9386	Ve věci společnosti NTT Global Data Centers Americas, Inc., jako právního nástupce společnosti **RagingWire Data Centers, Inc.**	RagingWire
12	Spis FTC č. 182 3196 Spis č. C-4702	Ve věci společnosti **Thru, Inc.**	Přes
13	Spis FTC č. 182 3188 Spis č. C-4698	Ve věci společnosti **DCR Workforce, Inc.**	Pracovní síla DCR
14	Spis FTC č. 182 3194 Spis č. C-4700	Ve věci společnosti **LotaData, Inc.**	LotaData
15	Spis FTC č. 182 3195 Spis č. C-4701	Ve věci společnosti **EmpiriStat, Inc.**	EmpiriStat
16	Spis FTC č. 182 3193 Spis č. C-4699	Ve věci společnosti 214 Technologies, Inc., rovněž d/b/a **Trueface.ai**	Trueface.ai

17	Spis FTC č. 182 3107 Spis č. 9383	Ve věci společnosti **Cambridge Analytica, LLC**	Cambridge Analytica
18	Spis FTC č. 182 3152 Spis č. C-4685	Ve věci společnosti **SecureTest, Inc.**	SecurTest
19	Spis FTC č. 182 3144 Spis č. C-4664	Ve věci společnosti **VenPath, Inc.**	VenPath
20	Spis FTC č. 182 3154 Spis č. C-4666	Ve věci společnosti **SmartStart Employment Screening, Inc.**	SmartStart
21	Spis FTC č. 182 3143 Spis č. C-4663	Ve věci **společnosti mResourceLLC,** d/b/a Loop Works LLC	mResource
22	Spis FTC č. 182 3150 Spis č. C-4665	Ve věci společnosti **Idmission LLC**	IDmission
23	Spis FTC č. 182 3100 Spis č. C-4659	Ve věci společnosti **ReadyTech Corporation**	ReadyTech
24	Spis FTC č. 172 3173 Spis č. C-4630	Ve věci společnosti **Decusoft, LLC**	Decusoft
25	Spis FTC č. 172 3171 Spis č. C-4628	Ve věci společnosti **Tru Communication, Inc.**	Tru
26	Spis FTC č. 172 3172 Spis č. C-4629	Ve věci společnosti **Md7, LLC**	Md7
30	Spis FTC č. 152 3198 Spis č. C-4543	Ve věci **Jhayrmaine Daniels (d/b/a California Skate-Line)**	Jhayrmaine Daniels
31	Spis FTC č. 152 3190 Spis č. C-4545	Ve věci společnosti **Dale Jarrett Racing Adventure, Inc.**	Dale Jarrett
32	Spis FTC č. 152 3141 Spis č. C-4540	Ve věci společnosti **Golf Connect, LLC**	Golf Connect
33	Spis FTC č. 152 3202 Spis č. C-4546	Ve věci společnosti **Inbox Group, LLC**	Skupina Doručená pošta
34	Spis č. 152 3187 Spis č. C-4542	Ve věci společnosti **IOActive, Inc.**	IOActive
35	Spis FTC č. 152 3140 Spis č. C-4549	Ve věci společnosti **Jubilant Clinsys, Inc.**	Jubilant
36	Spis FTC č. 152 3199 Spis č. C-4547	Ve věci společnosti **Just Bagels Manufacturing, Inc.**	Jen bagety
37	Spis FTC č. 152 3138 Spis č. C-4548	Ve věci společnosti **NAICS Association, LLC**	NAICS
38	Spis FTC č. 152 3201 Spis č. C-4544	Ve věci **One Industries Corp.**	One Industries
39	Spis FTC č. 152 3137 Spis č. C-4550	Ve věci společnosti **Pinger, Inc.**	Pinger

40	Spis FTC č. 152 3193 Spis č. C-4552	Ve věci společnosti **SteriMed Medical Waste Solutions**	SteriMed
41	Spis FTC č. 152 3184 Spis č. C-4541	Ve věci společnosti **Contract Logix, LLC**	Smlouva Logix
42	Spis FTC č. 152 3185 Spis č. C-4551	Ve věci společnosti **Forensics Consulting Solutions, LLC**	Forenzní poradenství
43	Spis FTC č. 152 3051 Spis č. C-4526	Ve věci společnosti **American Int'l Mailing, Inc.**	AIM
44	Spis FTC č. 152 3015 Spis č. C-4525	Ve věci společnosti **TES Franchising, LLC**	TES
45	Spis FTC č. 142 3036 Spis č. C-4459	Ve věci společnosti **American Apparel, Inc.**	American Apparel
46	Spis FTC č. 142 3026 Spis č. C-4469	Ve věci společnosti **Fantage.com, Inc.**	Fantage
47	Spis FTC č. 142 3017 Spis č. C-4461	Ve věci společnosti **Apperian, Inc.**	Apperian
48	Spis FTC č. 142 3018 Spis č. C-4462	Ve věci společnosti **Atlanta Falcons Football Club, LLC**	Atlanta Falcons
49	Spis FTC č. 142 3019 Spis č. C-4463	Ve věci společnosti **Baker Tilly Virchow Krause, LLP**	Baker Tilly
50	Spis FTC č. 142 3020 Spis č. C-4464	Ve věci společnosti **BitTorrent, Inc.**	BitTorrent
51	Spis FTC č. 142 3022 Spis č. C-4465	Ve věci **Charles River Laboratories, Int'l**	Charles River
52	Spis FTC č. 142 3023 Spis č. C-4466	Ve věci společnosti **DataMotion, Inc.**	DataMotion
53	Spis FTC č. 142 3024 Spis č. C-4467	Ve věci společnosti **DDC Laboratories, Inc.** d/b/a DNA Diagnostics Center	DDC
54	Spis FTC č. 142 3028 Spis č. C-4470	Ve věci společnosti **Level 3 Communications, LLC**	Úroveň 3
55	Spis FTC č. 142 3025 Spis č. C-4468	Ve věci **PDB Sports, Ltd.** d/b/a Denver Broncos Football Club, LLP	Broncos
56	Spis FTC č. 142 3030 Spis č. C-4471	Ve věci společnosti **Reynolds Consumer Products, Inc.**	Reynolds
57	Spis FTC č. 142 3031 Spis č. C-4472	Ve věci společnosti **Receivable Management Services Corporation**	Správa pohledávek
58	Spis FTC č. 142 3032 Spis č. C-4473	Ve věci společnosti **Tennessee Football, Inc.**	Fotbal v Tennessee
59	Spis FTC č. 102 3058 Spis č. C-4369	Ve věci **Myspace LLC**	Myspace

60	Spis FTC č. 092 3184 Spis č. C-4365	Ve věci společnosti **Facebook, Inc.**	Facebook
61	Spis FTC č. 092 3081 Občanskoprávní žaloba č. 09-CV- 5276 (C.D. Cal.)	FTC v. Javian Karnani a **Balls of Kryptonite, LLC**, d/b/a Bite Size Deals, LLC, a Best Priced Brands, LLC	Kryptonitové koule
62	Spis FTC č. 102 3136 Spis č. C-4336	Ve věci společnosti **Google, Inc.**	Google
63	Spis FTC č. 092 3137 Spis č. C-4282	Ve věci společnosti **World Innovators, Inc.**	Světoví inovátoři
64	Spis FTC č. 092 3141 Spis č. C-4271	Ve věci společnosti **Progressive Gaitways LLC**	Progresivní chodníky
65	Spis FTC č. 092 3139 Spis č. C-4270	Ve věci společnosti **Onyx Graphics, Inc.**	Onyx Graphics
66	Spis FTC č. 092 3138 Spis č. C-4269	Ve věci společnosti **ExpatEdge Partners, LLC**	ExpatEdge
67	Spis FTC č. 092 3140 Spis č. C-4281	Ve věci společnosti **Directors Desk LLC**	Stůl ředitele
68	Spis FTC č. 092 3142 Spis č. C-4272	Ve věci společnosti **Collectify LLC**	Collectify

PŘÍLOHA V

Komisař Didier Reynders
Evropská komise
Rue de la Loi / Wetstraat 200
1049 1049 Brusel
Belgie

Re:Rámec pro ochranu osobních údajů mezi EU a USA

Vážený pane komisaři Reyndersi:

Ministerstvo dopravy Spojených států amerických (dále jen "ministerstvo" nebo "ministerstvo") si váží příležitosti popsat svou úlohu při prosazování zásad rámce EU a USA pro ochranu osobních údajů (dále jen "rámec EU a USA pro ochranu osobních údajů"). Zásady ochrany osobních údajů mezi EU a USA budou hrát zásadní roli při ochraně osobních údajů poskytovaných během obchodních transakcí ve stále více propojeném světě. Umožní podnikům provádět důležité operace v globální ekonomice a zároveň zajistí, aby si spotřebitelé v EU zachovali důležitou ochranu soukromí.

Ministerstvo dopravy poprvé veřejně vyjádřilo svůj závazek k prosazování rámce "bezpečného přístavu" mezi USA a EU v dopise zaslaném Evropské komisi před více než 22 lety, který byl zopakován a rozšířen v dopise z roku 2016 týkajícím se rámce štítu na ochranu soukromí mezi EU a USA. Ministerstvo dopravy se v těchto dopisech zavázalo důsledně prosazovat zásady ochrany soukromí mezi USA a EU v rámci "bezpečného přístavu" a poté zásady štítu na ochranu soukromí mezi EU a USA. Ministerstvo dopravy tento závazek rozšiřuje i na EU
Zásady DPF USA a tento dopis tento závazek připomíná.

Ministerstvo dopravy zejména potvrzuje svůj závazek v následujících klíčových oblastech: 1) stanovení priorit při vyšetřování údajných porušení zásad DPF EU a USA; 2) vhodná donucovací opatření proti subjektům, které uvádějí nepravdivá nebo klamavá tvrzení o účasti na DPF EU a USA; a 3) monitorování a zveřejňování donucovacích příkazů týkajících se porušení zásad DPF EU a USA. Uvádíme informace o každém z těchto závazků a pro nezbytný kontext i příslušné informace o úloze ministerstva dopravy při ochraně soukromí spotřebitelů a prosazování zásad DPF EU a USA.

1. Pozadí

A. Úřad ministerstva dopravy pro ochranu osobních údajů

Ministerstvo je pevně odhodláno zajistit ochranu soukromí informací, které spotřebitelé poskytují leteckým společnostem a zprostředkovatelům letenek. Pravomoc ministerstva dopravy přijímat opatření v této oblasti je obsažena v zákoně 49 U.S.C. 41712, který zakazuje dopravci nebo zprostředkovateli letenek "nekalé nebo klamavé praktiky" v letecké dopravě nebo při prodeji letecké dopravy. Článek 41712 je vytvořen podle vzoru článku 5 zákona o Federální obchodní komisi (FTC) (15 U.S.C. 45). Ministerstvo dopravy nedávno vydalo předpisy

definující nekalé a klamavé praktiky, které jsou v souladu s precedenty ministerstva dopravy i FTC. Konkrétně je praktika "nekalá", pokud způsobuje nebo může způsobit značnou újmu, které se nelze rozumně vyhnout, a újma není vyvážena výhodami pro spotřebitele nebo hospodářskou soutěž. A

praktika je "klamavá" vůči spotřebitelům, pokud může spotřebitele jednajícího rozumně za daných okolností uvést v omyl ohledně podstatné skutečnosti. Záležitost je podstatná, pokud je pravděpodobné, že ovlivnila chování nebo rozhodnutí spotřebitele ohledně výrobku nebo služby. Kromě těchto obecných zásad ministerstvo dopravy konkrétně vykládá § 41712 tak, že zakazuje dopravcům a zprostředkovatelům letenek: (1) porušovat podmínky své politiky ochrany soukromí; (2) porušovat jakékoli pravidlo vydané ministerstvem, které označuje konkrétní praktiky ochrany soukromí za nekalé nebo klamavé; nebo (3) porušovat zákon o ochraně soukromí dětí na internetu (Children's Online Privacy Protection Act - COPPA) nebo pravidla FTC, která COPPA provádějí; nebo (4) nedodržovat jako účastník DPF EU a USA zásady DPF EU a USA.[1]

Podle federálních zákonů má ministerstvo dopravy výhradní pravomoc regulovat postupy leteckých společností v oblasti ochrany soukromí a sdílí pravomoc s FTC, pokud jde o postupy zprostředkovatelů prodeje letenek při ochraně soukromí v letecké dopravě.

Jakmile se tedy dopravce nebo prodejce letecké dopravy veřejně zaváže k dodržování zásad DPF EU a USA, může ministerstvo využít zákonné pravomoci podle § 41712 k zajištění dodržování těchto zásad. Jakmile tedy cestující poskytne informace dopravci nebo prodejci letenek, který se zavázal dodržovat zásady DPF EU a USA, bude jakékoli nedodržení těchto zásad ze strany dopravce nebo prodejce letenek porušením oddílu 41712.

B. Postupy vymáhání práva

Úřad pro ochranu spotřebitelů v letectví ("OACP")[2] vyšetřuje a stíhá případy podle 49 U.S.C. 41712. Prosazuje zákonný zákaz nekalých a klamavých praktik uvedený v § 41712 především prostřednictvím jednání, přípravy příkazů k zastavení činnosti a vypracovávání příkazů k vyměření občanskoprávních sankcí. Úřad se o možných porušeních dozvídá převážně ze stížností, které dostává od jednotlivců, cestovních kanceláří, leteckých společností a amerických i zahraničních vládních agentur. Spotřebitelé mohou na internetových stránkách ministerstva dopravy podávat stížnosti na ochranu soukromí leteckých společností a zprostředkovatelů letenek.[3]

Pokud se nepodaří dosáhnout přiměřeného a vhodného urovnání případu, má úřad OACP pravomoc zahájit řízení o vymáhání práva zahrnující důkazní řízení před správním soudcem ministerstva dopravy (dále jen "ALJ"). ALJ je oprávněn vydávat příkazy k zastavení činnosti a občanskoprávní sankce. Porušení § 41712 může vést k vydání příkazu k zastavení činnosti a k uložení občanskoprávních sankcí až do výše 37 377 USD za každé porušení § 41712.

Odbor nemá pravomoc přiznávat jednotlivým stěžovatelům náhradu škody nebo poskytovat peněžitou pomoc. Ministerstvo však má pravomoc schvalovat narovnání vyplývající z vyšetřování vedených jeho OACP, která přímo zvýhodňují spotřebitele (např. hotovost, poukázky) jako kompenzaci peněžitých sankcí, které by jinak byly splatné vládě USA. K tomu již v minulosti došlo a může k tomu dojít i v souvislosti se zásadami DPF mezi EU a USA, pokud to okolnosti vyžadují. Opakované porušení oddílu 41712 ze strany letecké společnosti by rovněž vyvolalo

[1] https://www.transportation.gov/individuals/aviation-consumer-protection/privacy.

[2] Dříve známý jako Úřad pro prosazování práva a řízení v letectví.

[3] http://www.transportation.gov/airconsumer/privacy-complaints.

otázky týkající se dodržování předpisů ze strany letecké společnosti, které by v závažných situacích mohly vést k tomu, že by letecká společnost byla shledána nezpůsobilou k provozu, a tudíž by ztratila své oprávnění k hospodářské činnosti.

Ministerstvo dopravy dosud obdrželo poměrně málo stížností týkajících se údajného porušení ochrany osobních údajů ze strany zprostředkovatelů letenek nebo leteckých společností. Pokud se vyskytnou, jsou prošetřovány podle výše uvedených zásad.

C. Právní ochrana ministerstva dopravy ve prospěch spotřebitelů v EU

Podle § 41712 se zákaz nekalých nebo klamavých praktik v letecké dopravě nebo při prodeji letecké dopravy vztahuje na americké a zahraniční letecké dopravce i na prodejce letenek. Ministerstvo dopravy často podává žaloby proti americkým a zahraničním leteckým společnostem za praktiky, které se dotýkají jak zahraničních, tak amerických spotřebitelů, a to na základě toho, že k praktikám letecké společnosti došlo při poskytování přepravy do Spojených států nebo z nich. Ministerstvo dopravy využívá a bude i nadále využívat všechny dostupné opravné prostředky na ochranu zahraničních i amerických spotřebitelů před nekalými nebo klamavými praktikami regulovaných subjektů v letecké dopravě.

Ministerstvo dopravy prosazuje v souvislosti s leteckými společnostmi také další cílené zákony, jejichž ochrana se vztahuje i na spotřebitele mimo USA, jako je zákon o ochraně soukromí dětí na internetu ("COPPA"). COPPA mimo jiné vyžaduje, aby provozovatelé webových stránek a online služeb zaměřených na děti nebo stránek pro širokou veřejnost, kteří vědomě shromažďují osobní údaje dětí mladších 13 let, informovali rodiče a získali jejich ověřitelný souhlas. Webové stránky a služby se sídlem v USA, na které se vztahuje COPPA a které shromažďují osobní údaje od zahraničních dětí, jsou povinny dodržovat COPPA. Webové stránky a online služby se sídlem v zahraničí musí rovněž dodržovat COPPA, pokud jsou určeny dětem ve Spojených státech nebo pokud vědomě shromažďují osobní údaje od dětí ve Spojených státech. Pokud by americké nebo zahraniční letecké společnosti podnikající ve Spojených státech porušily ustanovení COPPA, mělo by ministerstvo dopravy pravomoc přijmout opatření k prosazování práva.

II. Prosazování zásad DPF v EU a USA

Pokud se letecká společnost nebo zprostředkovatel letenek rozhodne účastnit se DPF EU a USA a ministerstvo obdrží stížnost, že tato letecká společnost nebo zprostředkovatel letenek údajně porušil zásady DPF EU a USA, ministerstvo podnikne následující kroky k důslednému prosazování zásad DPF EU a USA.

A. Stanovení priorit při vyšetřování údajných porušení předpisů

Oddělení OACP ministerstva prošetří každou stížnost týkající se údajného porušení zásad DPF mezi EU a USA, včetně stížností obdržených od orgánů EU pro ochranu údajů (dále jen "OPA"), a v případě důkazů o porušení přijme donucovací opatření. Dále bude OACP spolupracovat s FTC a ministerstvem obchodu a bude se prioritně zabývat tvrzeními, že regulované subjekty nedodržují závazky v oblasti ochrany osobních údajů přijaté v rámci DPF EU a USA.

Po obdržení obvinění z porušení zásad DPF EU a USA může OACP v rámci svého šetření přijmout řadu opatření. Může například přezkoumat zásady ochrany osobních údajů zprostředkovatele letenek nebo letecké společnosti, získat další informace od zprostředkovatele letenek nebo letecké společnosti nebo od třetích stran,

navázat kontakt s odkazujícím subjektem a posoudit, zda se jedná o porušení nebo zda je postižen značný počet spotřebitelů. Dále by určil, zda se problém týká záležitostí, které spadají do působnosti ministerstva obchodu nebo FTC, posoudil by, zda by bylo užitečné vzdělávání spotřebitelů a podnikatelů, a případně by zahájil řízení o vymáhání práva.

Pokud se ministerstvo dozví o možném porušení zásad DPF EU a USA ze strany zprostředkovatelů prodeje letenek, bude tuto záležitost koordinovat s FTC. Rovněž budeme informovat FTC a ministerstvo obchodu o výsledku jakéhokoli opatření k prosazení zásad DPF mezi EU a USA.

B. Řešení falešných nebo klamavých tvrzení o účasti

Ministerstvo je i nadále odhodláno vyšetřovat porušování zásad DPF EU a USA, včetně nepravdivých nebo klamavých tvrzení o účasti na DPF EU a USA. Budeme přednostně zvažovat postoupení od ministerstva obchodu týkající se organizací, které se podle jeho zjištění neoprávněně vydávají za účastníky DPF EU a USA nebo neoprávněně používají certifikační značku DPF EU a USA.

Kromě toho upozorňujeme, že pokud organizace v zásadách ochrany osobních údajů slibuje, že dodržuje předpisy EU.
Zásady DPF USA, její neúspěch při provádění nebo udržování vlastní certifikace prostřednictvím ministerstva obchodu pravděpodobně sám o sobě nezbaví organizaci povinnosti prosazovat tyto závazky ze strany ministerstva dopravy.

C. Monitorování a zveřejňování exekučních příkazů týkajících se porušování DPF v EU a USA

Oddělení OACP ministerstva je rovněž odhodláno podle potřeby sledovat příkazy k výkonu rozhodnutí, aby bylo zajištěno dodržování zásad DPF mezi EU a USA. Konkrétně, pokud úřad vydá příkaz, kterým letecké společnosti nebo zprostředkovateli letenek nařídí, aby v budoucnu přestali porušovat zásady DPF EU a USA a § 41712, bude sledovat, zda subjekt dodržuje ustanovení o zastavení porušování v příkazu. Kromě toho úřad zajistí, aby příkazy vyplývající z případů týkajících se zásad DPF EU a USA byly k dispozici na jeho internetových stránkách.

Těšíme se na další spolupráci s našimi federálními partnery a zúčastněnými stranami z EU v otázkách DPF mezi EU a USA.

Doufám, že vám tyto informace pomohou. Pokud máte jakékoli dotazy nebo potřebujete další informace, neváhejte mě kontaktovat.

S pozdravem,

Pete Buttigieg
Ministr dopravy

PŘÍLOHA
VI

Trestní oddělení Ministerstva

spravedlnosti USA

Kancelář asistenta generálního prokurátoraWashington , D.C. 20530

prosinec , 2022

Ana Gallego Torres
Generální ředitel pro spravedlnost a spotřebitele
Evropské komise
Rue Montoyer/Montoyerstraat 59
1049 Brusel
Belgie

Vážená paní generální ředitelko Gallego Torresová:

Tento dopis poskytuje stručný přehled hlavních vyšetřovacích nástrojů používaných k získávání obchodních údajů a dalších informací ze záznamů společností ve Spojených státech pro účely vymáhání trestního práva nebo veřejného zájmu (občanskoprávní a regulační), včetně omezení přístupu stanovených v těchto orgánech.[1] Všechny právní postupy popsané v tomto dopise jsou nediskriminační v tom smyslu, že se používají k získávání informací od korporací ve Spojených státech, včetně společností, které se samy certifikují prostřednictvím rámce USA-EU pro ochranu osobních údajů, bez ohledu na státní příslušnost nebo místo bydliště subjektu údajů. Dále mohou korporace, které obdrží právní proces ve Spojených státech, tento proces napadnout u soudu, jak je uvedeno níže.[2]

V souvislosti se zabavováním údajů orgány veřejné moci je třeba zmínit zejména čtvrtý dodatek Ústavy Spojených států, který stanoví, že "právo lidu na osobní bezpečnost, ochranu obydlí, listin a majetku před neoprávněnými prohlídkami a zabavováním nesmí být porušováno a soudní příkaz nesmí být vydán jinak než na základě pravděpodobného důvodu, podloženého důkazy".

[1] Tento přehled nepopisuje nástroje vyšetřování národní bezpečnosti, které používají donucovací orgány při vyšetřování terorismu a jiných případů národní bezpečnosti, včetně dopisů národní bezpečnosti (National Security Letters, NSL) pro určité informace v úvěrových zprávách, finančních záznamech a elektronických záznamech o účastnících a transakcích, 12 U.S.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, 50 U.S.C. § 3162, a pro elektronické sledování, příkazy k prohlídce, obchodní záznamy a další shromažďování informací podle zákona o dohledu nad zahraničním zpravodajstvím, 50 U.S.C. § 3162.
U.S.C. § 1801 a následující.

[2] Tento dopis se zabývá federálními donucovacími a regulačními orgány. Porušení státních zákonů vyšetřují státní donucovací orgány a projednávají je státní soudy. Státní orgány činné v trestním řízení používají příkazy k prohlídce a předvolání vydané podle státního práva v podstatě stejným způsobem, jaký je popsán v tomto dokumentu, avšak s tím, že státní soudní řízení může podléhat dodatečné ochraně poskytované státními ústavami nebo zákony, které přesahují ochranu stanovenou ústavou USA. Ochrana podle státního práva musí být přinejmenším stejná jako ochrana podle Ústavy USA, mimo jiné včetně čtvrtého dodatku.

přísahou nebo místopřísežným prohlášením, a to zejména s popisem místa, které má být prohledáno, a osob nebo věcí, které mají být zajištěny." Ústava Spojených států amerických, pozn. překl. IV. Jak uvedl Nejvyšší soud Spojených států ve věci Berger v. State of New York, "[z]ákladním účelem tohoto dodatku, jak bylo uznáno v nesčetných rozhodnutích tohoto soudu, je chránit soukromí a bezpečnost jednotlivců před svévolnými zásahy vládních úředníků.". 388 U.S. 41, 53 (1967) (citace rozsudku Camara v. Mun. Court of San Francisco, 387 U.S. 523, 528 (1967)). Při vyšetřování vnitrostátních trestných činů čtvrtý dodatek obecně vyžaduje, aby policisté před provedením prohlídky získali soudní příkaz. Viz Katz v. Spojené státy, 389 U.S. 347, 357 (1967). Standardy pro vydání soudního příkazu, jako jsou požadavky na pravděpodobnou příčinu a konkrétnost, se vztahují na příkazy k fyzickým prohlídkám a zabavení, jakož i na příkazy k prohlídce uloženého obsahu elektronických komunikací vydané podle zákona o uložených komunikacích, jak je uvedeno níže.
Pokud se požadavek na soudní příkaz neuplatní, vládní činnost stále podléhá "přiměřenosti" podle čtvrtého dodatku. Samotná ústava tedy zajišťuje, že vláda USA nemá neomezenou nebo svévolnou pravomoc zabavovat soukromé informace.[3]

Orgány činné v trestním řízení:

Federální státní zástupci, kteří jsou úředníky ministerstva spravedlnosti (DOJ), a federální vyšetřovací agenti, včetně agentů Federálního úřadu pro vyšetřování (FBI), což je donucovací orgán ministerstva spravedlnosti, mohou pro účely trestního vyšetřování vynutit předložení dokumentů a dalších záznamů od společností ve Spojených státech prostřednictvím několika typů povinných právních postupů, včetně předvolání před velkou porotu, správních předvolání a příkazů k prohlídce, a mohou získávat další komunikaci na základě federálních trestních odposlechů a registrů.

Předvolání před velkou porotu nebo soud: Předvolání k trestnímu soudu se používají k podpoře cílených vyšetřování orgánů činných v trestním řízení. Předvolání před velkou porotu je oficiální žádost vydaná velkou porotou (obvykle na žádost federálního státního zástupce) na podporu vyšetřování velké poroty v souvislosti s konkrétním podezřením na porušení trestního zákona. Velké poroty jsou vyšetřovací složkou soudu a jsou jmenovány soudcem nebo soudcem. Předvolání může vyžadovat, aby někdo vypovídal při řízení nebo aby předložil či zpřístupnil obchodní záznamy, elektronicky uložené informace nebo jiné hmotné předměty. Tyto informace musí být relevantní pro vyšetřování a předvolání nesmí být nepřiměřené, protože je příliš široké nebo protože je obtěžující či zatěžující. A
příjemce může podat návrh na zpochybnění předvolání na základě těchto důvodů. Viz Fed. R. Crim.
P. 17. Za omezených okolností lze předvolání k soudu pro dokumenty použít i poté, co byla věc obžalována velkou porotou.

Správní orgán pro předvolání: Správní předvolání lze uplatnit v rámci trestního nebo občanskoprávního vyšetřování. V souvislosti s vymáháním trestního práva povoluje několik federálních zákonů používat správní předvolání k předložení nebo zpřístupnění obchodních záznamů, elektronicky uložených informací nebo jiných hmotných věcí důležitých pro vyšetřování.

[3] Pokud jde o výše uvedené zásady čtvrtého dodatku o ochraně soukromí a bezpečnostních zájmů, americké soudy tyto zásady pravidelně uplatňují na nové typy vyšetřovacích nástrojů orgánů činných v trestním řízení, které jsou umožněny vývojem technologií. Například v roce 2018 Nejvyšší soud rozhodl, že získání historických informací o poloze mobilního telefonu vládou v rámci vyšetřování v oblasti prosazování práva z mobilního telefonu společnosti po delší dobu je "prohlídkou", na kterou se vztahuje čtvrtý dodatek zákona. Carpenter v. Spojené státy, 138 S. Ct. 2206 (2018).

vyšetřování týkající se podvodů v oblasti zdravotní péče, zneužívání dětí, ochrany tajných služeb, případů týkajících se kontrolovaných látek a vyšetřování generálního inspektora, do nichž jsou zapojeny vládní agentury. Pokud vláda usiluje o vymáhání správního předvolání u soudu, může příjemce správního předvolání, stejně jako příjemce předvolání před velkou porotu, namítat, že předvolání je nepřiměřené, protože je příliš široké nebo protože je obtížné či zatěžující.

Soudní příkazy pro Pen Register a Trap and Traces: Na základě ustanovení o trestních registrech a sledování stop mohou orgány činné v trestním řízení získat soudní příkaz k získání informací o vytáčení, směrování, adresování a signalizaci telefonního čísla nebo e-mailu v reálném čase, bez ohledu na obsah, po potvrzení, že poskytnuté informace jsou relevantní pro probíhající trestní vyšetřování. Viz 18 U.S.C. §§ 3121-3127. Použití nebo instalace takového zařízení mimo rámec zákona je federálním trestným činem.

Zákon o ochraně soukromí v elektronických komunikacích (ECPA): Další pravidla upravují přístup vlády k informacím o účastnících, provozním údajům a uloženému obsahu komunikace, které mají k dispozici poskytovatelé internetových služeb (známí také jako "ISP"), telefonní společnosti a další poskytovatelé služeb třetích stran podle hlavy II zákona ECPA, nazývaného také zákon o uložených komunikacích (Stored Communications Act, SCA), 18 U.S.C. §§ 2701-2712. SCA stanoví systém zákonných práv na ochranu soukromí, která omezují přístup orgánů činných v trestním řízení k údajům nad rámec toho, co od zákazníků a účastníků poskytovatelů internetových služeb vyžaduje ústavní právo. SCA stanoví rostoucí úroveň ochrany soukromí v závislosti na intenzitě shromažďování údajů. V případě registračních informací o účastnících, adres internetového protokolu (IP) a souvisejících časových razítek a fakturačních informací musí orgány činné v trestním řízení získat soudní obsílku. U většiny ostatních uložených informací, které nejsou obsahem, jako jsou hlavičky e-mailů bez předmětu, musí orgány činné v trestním řízení předložit soudci konkrétní skutečnosti, které prokazují, že požadované informace jsou relevantní a podstatné pro probíhající trestní vyšetřování. K získání uloženého obsahu elektronické komunikace musí obecně orgány činné v trestním řízení získat soudní příkaz na základě pravděpodobného důvodu domnívat se, že daný účet obsahuje důkazy o trestném činu.
ZZVZ rovněž stanoví občanskoprávní odpovědnost a trestněprávní sankce.[4]

Soudní příkazy ke sledování podle federálního zákona o odposlechu: Kromě toho mohou orgány činné v trestním řízení v reálném čase zachycovat odposlechy, ústní nebo elektronickou komunikaci pro účely vyšetřování trestné činnosti podle federálního zákona o odposlechu. Viz 18 U.S.C. §§ 2510-2523. Toto oprávnění je k dispozici pouze na základě soudního příkazu, v němž soudce mimo jiné zjistí, že existuje pravděpodobný důvod se domnívat, že odposlech nebo elektronický odposlech přinese důkazy o federálním trestném činu nebo o místě pobytu uprchlého pachatele, který se skrývá před trestním stíháním. Zákon stanoví občanskoprávní odpovědnost a trestní sankce za porušení ustanovení o odposlechu.

Příkaz k prohlídce -Fed. R. Crim. P. Rule 41: Orgány činné v trestním řízení mohou fyzicky prohledávat prostory ve Spojených státech, pokud je k tomu oprávněn soudce. Orgány činné v trestním řízení musí

[4] Kromě toho čl. 2705 písm. b) SCA opravňuje vládu, aby na základě prokázané potřeby ochrany před zveřejněním získala soudní příkaz zakazující poskytovateli komunikačních služeb dobrovolně informovat své uživatele o přijetí soudního procesu SCA. V říjnu 2017 vydal náměstek generálního prokurátora Rod Rosenstein memorandum pro právníky a agenty ministerstva spravedlnosti, v němž stanovil pokyny k zajištění toho, aby žádosti o takové ochranné příkazy byly přizpůsobeny konkrétním skutečnostem a obavám vyšetřování, a stanovil obecný roční strop pro to, jak dlouho může žádost o odložení oznámení trvat. V květnu 2022 vydala náměstkyně generálního prokurátora Lisa Monaco k tomuto tématu doplňující pokyny, které mimo jiné stanovily interní požadavky na schvalování žádostí o prodloužení ochranného příkazu po uplynutí původní jednoleté lhůty a požadovaly ukončení ochranných příkazů po ukončení vyšetřování.

prokázat soudci na základě prokázání pravděpodobného důvodu, že byl spáchán trestný čin nebo že má být spáchán a že na místě uvedeném v příkazu k prohlídce se pravděpodobně nacházejí věci související s trestným činem. Toto oprávnění se často používá v případech, kdy je nutné provést fyzickou prohlídku prostor policií z důvodu nebezpečí zničení důkazů, pokud je společnosti doručeno předvolání k soudu nebo jiný příkaz k předložení důkazů. Osoba, která je předmětem prohlídky nebo jejíž majetek je předmětem prohlídky, může podat návrh na potlačení důkazů získaných nebo získaných na základě nezákonné prohlídky, pokud jsou tyto důkazy předloženy proti této osobě během trestního řízení. Viz Mapp v. Ohio, 367 U.S. 643 (1961). Pokud je držitel údajů povinen poskytnout údaje na základě soudního příkazu, může nucená strana požadavek na poskytnutí údajů napadnout jako nepřiměřeně zatěžující. Viz In re Application of United States, 610 F.2d 1148, 1157 (3. obvod 1979) (rozhodl, že "řádný proces vyžaduje slyšení v otázce zatížení před tím, než donutí telefonní společnost poskytnout" pomoc s příkazem k prohlídce); In re Application of United States, 616 F.2d 1122 (9. obvod 1980) (dospěl ke stejnému závěru na základě dozorové pravomoci soudu).

Pokyny a zásady ministerstva spravedlnosti: Kromě těchto ústavních, zákonných a pravidlových omezení přístupu vlády k údajům vydal generální prokurátor pokyny, které stanoví další omezení přístupu orgánů činných v trestním řízení k údajům a které rovněž obsahují ochranu soukromí a občanských svobod. Například Pokyny generálního prokurátora pro vnitrostátní operace FBI (září 2008) (dále jen "pokyny AG FBI"), které jsou k dispozici na adrese http://www.justice.gov/archive/opa/docs/guidelines.pdf, stanoví omezení pro používání vyšetřovacích prostředků k vyhledávání informací souvisejících s vyšetřováním, které se týká federálních trestných činů. Tyto pokyny vyžadují, aby FBI používala co nejméně invazivní vyšetřovací metody s ohledem na dopad na soukromí a občanské svobody a na možné poškození pověsti. Dále se v nich uvádí
že "je samozřejmé, že FBI musí provádět svá vyšetřování a další činnosti zákonným a rozumným způsobem, který respektuje svobodu a soukromí a vyhýbá se zbytečným zásahům do života lidí, kteří dodržují zákony." AG FBI Guidelines (Směrnice FBI), 5. FBI tyto směrnice zavedla prostřednictvím Příručky FBI pro domácí vyšetřování a operace (DIOG), která je k dispozici na adrese https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20.%28DIOG%29, komplexní příručku, která obsahuje podrobná omezení pro používání vyšetřovacích nástrojů a pokyny, jak zajistit, aby byly při každém vyšetřování chráněny občanské svobody a soukromí. Další pravidla a zásady, které předepisují omezení vyšetřovacích činností federálních státních zástupců, jsou uvedeny v justiční příručce, která je rovněž k dispozici online na adrese https://www.justice.gov/jm/justice-manual.

Občanské a regulační orgány (veřejný zájem):

Ve Spojených státech také existují významná omezení občanského nebo regulačního (tj. "veřejného zájmu") přístupu k údajům v držení společností. Orgány s občanskoprávními a regulačními pravomocemi mohou vydávat korporacím předvolání k soudnímu jednání o obchodních záznamech, elektronicky uložených informacích nebo jiných hmotných věcech. Tyto agentury jsou při výkonu správních nebo občanskoprávních předvolání omezeny nejen svými organickými zákony, ale také nezávislým soudním přezkumem předvolání před případným soudním výkonem. Viz např.
R. Civ. P. 45. Agentury mohou žádat o přístup pouze k údajům, které se týkají záležitostí spadajících do jejich regulační pravomoci. Dále může příjemce správního předvolání napadnout výkon tohoto předvolání u soudu předložením důkazů, že agentura nejednala v souladu se základními standardy přiměřenosti, jak bylo uvedeno výše.

Existují i další právní základy, na jejichž základě mohou společnosti napadnout žádosti správních orgánů o poskytnutí údajů, a to v závislosti na konkrétním odvětví a typu údajů, které mají k dispozici. Například finanční instituce mohou napadnout správní předvolání požadující určité typy informací jako porušení zákona o bankovním tajemství a jeho prováděcích předpisů. 31 U.S.C.
§ 5318; 31 C.F.R. kapitola X. Ostatní podniky se mohou spolehnout na zákon o spravedlivém úvěrovém zpravodajství, 15
U.S.C. § 1681b nebo řada dalších odvětvových zákonů. Zneužití pravomoci agentury k předvolání může mít za následek odpovědnost agentury nebo osobní odpovědnost jejích úředníků. Viz např. zákon o právu na finanční soukromí, 12 U.S.C. §§ 3401-3423. Soudy ve Spojených státech tak vystupují jako strážci proti nevhodným žádostem o regulaci a zajišťují nezávislý dohled nad činností federálních agentur.

A konečně, jakákoli zákonná pravomoc správních orgánů fyzicky zabavit záznamy společnosti ve Spojených státech na základě správní prohlídky musí splňovat požadavky založené na čtvrtém dodatku. Viz rozsudek ve věci Seattle, 387 U.S. 541 (1967).

Závěr:

Veškeré činnosti v oblasti prosazování práva a regulace ve Spojených státech musí být v souladu s platnými zákony, včetně Ústavy USA, zákonů, pravidel a předpisů. Tyto činnosti musí být rovněž v souladu s platnými zásadami, včetně všech pokynů generálního prokurátora upravujících federální činnosti v oblasti prosazování práva. Výše popsaný právní rámec omezuje možnost amerických orgánů činných v trestním řízení a regulačních orgánů získávat informace od společností ve Spojených státech - bez ohledu na to, zda se informace týkají amerických osob nebo občanů cizích zemí - a navíc umožňuje soudní přezkum všech vládních žádostí o údaje na základě těchto pravomocí.

_____
Bruce C. Swartz
Zástupce náměstka generálního prokurátora a
poradce pro mezinárodní záležitosti

PŘÍLOHA VII

ÚŘAD ŘEDITELE NÁRODNÍHO ZPRAVODAJSTVÍ ÚŘAD
GENERÁLNÍHO PORADCE
WASHINGTON, DC 20511

9. prosince 2022

Leslie B. Kiernan Hlavní
právní poradce
Ministerstvo obchodu USA 1401
Constitution Ave., NW
Washington, DC 20230

Vážená paní Kiernanová,

Dne 7. října 2022 podepsal prezident Biden exekutivní příkaz 14086, *Enhancing Sqfeguards for United Stales Signals Intelligence Aclivilies,* který posiluje přísnou řadu záruk ochrany soukromí a občanských svobod, jež se vztahují na činnosti amerického signálového zpravodajství. Tato ochranná opatření zahrnují: vyžadují, aby činnosti signálového zpravodajství plnily vyjmenované legitimní cíle; výslovně zakazují tyto činnosti za účelem dosažení konkrétních zakázaných cílů; zavádějí nové postupy, které zajistí, aby činnosti signálového zpravodajství podporovaly tyto legitimní cíle a nepodporovaly zakázané cíle; požadavek, aby činnosti v oblasti signálového zpravodajství byly prováděny pouze na z á k l a d ě rozhodnutí založeného na přiměřeném posouzení všech relevantních faktorů, že tyto činnosti jsou nezbytné pro dosažení schválené zpravodajské priority, a to pouze v rozsahu a způsobem, který je přiměřený schválené zpravodajské prioritě, pro niž byly povoleny; a pokyn, aby složky zpravodajské služby (IC) aktualizovaly své politiky a postupy tak, aby odrážely ochranná opatření požadovaná výkonným nařízením v oblasti signálového zpravodajství. Nejdůležitější je, že prováděcí nařízení rovněž zavádí nezávislý a závazný mechanismus, který umožňuje jednotlivcům z "kvalifikovaných států", jak jsou určeny podle prováděcího nařízení, domáhat se nápravy, pokud se domnívají, že byli vystaveni nezákonným činnostem amerického signálového zpravodajství, včetně činností porušujících ochranu stanovenou v prováděcím nařízení.

Vydáním exekutivního příkazu č. 14086 prezidentem Bidenem vyvrcholila více než rok trvající podrobná jednání mezi zástupci Evropské komise (EK) a Spojených států a byly jím stanoveny kroky, které Spojené státy podniknou k provedení svých závazků v rámci dohody mezi EU a USA. USA v oblasti ochrany osobních údajů. V souladu s duchem spolupráce, který vedl k vytvoření rámce, jsem pochopil, že jste od EK obdrželi dvě sady otázek ohledně způsobu, jakým bude IC prováděcí nařízení provádět. Jsem rád, že se na tyto otázky mohu tímto dopisem vyjádřit.

Článek 702 zákona o dohledu nad zahraničním zpravodajstvím z roku 1978 (FJSA Section 702)

První skupina otázek se týká článku 702 zákona FISA, který umožňuje shromažďovat zahraniční zpravodajské informace prostřednictvím zaměřování se na osoby, o nichž se lze důvodně domnívat, že se nacházejí mimo území Spojených států, a to za nucené asistence poskytovatelů služeb elektronických komunikací. Otázky se konkrétně týkají vzájemného vztahu mezi tímto ustanovením a výkonným nařízením 14086, jakož i dalších záruk, které se vztahují na činnosti prováděné podle oddílu 702 zákona FISA.

Pro začátek můžeme potvrdit, že IC bude na činnosti prováděné podle oddílu 702 zákona FISA uplatňovat záruky stanovené ve výkonném nařízení 14086.

Kromě toho se na vládní použití článku 702 zákona FISA vztahuje řada dalších záruk. Například všechna osvědčení podle oddílu 702 zákona FISA musí být podepsána generálním prokurátorem a ředitelem národního zpravodajství (DNI) a vláda musí všechna tato osvědčení předložit ke schválení soudu pro dohled nad zahraničním zpravodajstvím (FISC), který se skládá z nezávislých soudců s doživotním mandátem, jejichž funkční období je sedmileté a nelze je obnovit. Tato osvědčení určují kategorie zahraničních zpravodajských informací, které mají být shromažďovány a které musí splňovat zákonnou definici zahraničních zpravodajských informací, a to prostřednictvím zaměření na jiné než zahraniční zpravodajské služby. osoby z USA, o nichž se lze důvodně domnívat, že se nacházejí mimo Spojené státy. Osvědčení zahrnovala informace týkající se mezinárodního terorismu a dalších témat, jako je získávání informací o zbraních hromadného ničení. Každé roční osvědčení musí být předloženo FISC ke schválení v balíčku žádosti o osvědčení, který obsahuje osvědčení generálního prokurátora a DNI, čestná prohlášení některých vedoucích zpravodajských agentur a postupy zaměřování, postupy minimalizace a postupy dotazování, které jsou pro vládu závazné. Postupy zaměřování mimo jiné vyžadují, aby IC na základě všech okolností důvodně vyhodnotil, že zaměření pravděpodobně povede ke shromažďování zahraničních zpravodajských informací uvedených v osvědčení podle článku 702 PISA.

Kromě toho musí IC při shromažďování informací podle oddílu 702 FISA: poskytnout písemné vysvětlení, na základě čeho v době zaměření vyhodnotil, že cíl pravděpodobně vlastní, obdrží nebo sdělí zahraniční zpravodajské informace uvedené v osvědčení podle oddílu 702 PISA; potvrdit, že standard zaměření stanovený v postupech zaměření podle oddílu 702 PISA je i nadále splněn; a ukončit shromažďování, pokud standard již není splněn. *Viz* Podání vlády USA Soudu pro dohled nad zahraničním zpravodajstvím, *2015 Summcuy ofNotable Section 702 Requirements,* na str. 2-3 (15. července 2015).

Požadavek, aby IC písemně zaznamenával a pravidelně potvrzoval platnost svého hodnocení, že cíle podle článku 702 zákona FISA splňují příslušné normy pro cílení, usnadňuje dohled FISC nad cílenými činnostmi IC. Každé zaznamenané posouzení a zdůvodnění zaměření je jednou za dva měsíce přezkoumáno právníky pro dohled nad zpravodajskými službami na ministerstvu spravedlnosti (DOJ), kteří tuto funkci dohledu vykonávají nezávisle na zahraničních zpravodajských operacích. Sekce ministerstva spravedlnosti, která tuto funkci vykonává, je pak podle dlouhodobě zavedeného pravidla FISC odpovědná za to, že bude FISC hlásit jakékoli porušení platných postupů. Toto podávání zpráv spolu s pravidelnými schůzkami mezi FISC a touto sekcí ministerstva spravedlnosti týkajícími se dohledu nad cílenými činnostmi podle oddílu 702 zákona FISA umožňuje FISC prosazovat dodržování cílených činností podle oddílu 702 zákona FISA a dalších postupů a jinak zajišťovat zákonnost vládních činností. FISC tak může činit zejména řadou způsobů, včetně vydávání závazných nápravných rozhodnutí o ukončení oprávnění vlády shromažďovat údaje proti určitému cíli nebo o změně či odložení shromažďování údajů podle oddílu 702 zákona FISA. FISC může rovněž požadovat, aby vláda podávala další zprávy nebo informace o dodržování postupů zaměřování a dalších postupů, nebo požadovat změny těchto postupů.

Hromadné shromažďování zpravodajských informací o signálech

Druhý soubor otázek se týká "hromadného" sběru zpravodajských informací, který je definován ve vládním nařízení 14086 jako "povolený sběr velkého množství zpravodajských informací, které jsou z technických nebo operativních důvodů získávány bez použití rozlišovacích prvků (například bez použití specifických identifikátorů nebo selekčních podmínek)".

V souvislosti s těmito otázkami nejprve poznamenáváme, že ani FISA, ani dopisy o národní bezpečnosti nepovolují hromadné shromažďování. Pokud jde o FISA:

- Hlavy I a III zákona FISA, které povolují elektronické sledování a fyzické prohlídky, vyžadují soudní příkaz (s omezenými výjimkami, jako jsou mimořádné okolnosti) a vždy vyžadují pravděpodobný důvod domnívat se, že cílem je cizí mocnost nebo agent cizí mocnosti. *Viz* 50 U.S.C. §§ 1805, 1824.

- Zákonem USA FREEDOM Act z roku 2015 byla změněna hlava IV zákona FISA, která povoluje používání záznamových zařízení a zařízení pro sledování a vyhledávání na základě soudního příkazu (s výjimkou mimořádných okolností), a to tak, aby vláda musela své žádosti opírat o "konkrétní termín výběru". *Viz* 50 U.S.C. § 1842(c)(3).

- Hlava V zákona FISA, která Federálnímu úřadu pro vyšetřování (FBI) umožňuje získávat určité typy obchodních záznamů, vyžaduje soudní příkaz na základě žádosti, v níž je uvedeno, že "existují konkrétní a zřetelné skutečnosti, které dávají důvod se domnívat, že osoba, jíž se záznamy týkají, je cizí mocností nebo agentem cizí mocnosti". *Viz* 50 U.S.C. § 1862(b)(2)(B).[1]

- A konečně článek 702 zákona FISA povoluje "zaměřit se na osoby, o nichž se důvodně předpokládá, že se nacházejí mimo území Spojených států, za účelem získání zahraničních zpravodajských informací". *Viz* 50 U.S.C. § 188la(a). Jak tedy uvedl Výbor pro dohled nad soukromím a občanskými svobodami, vládní shromažďování údajů podle článku 702 zákona FISA "spočívá výhradně v zaměření na jednotlivé osoby a získávání komunikace spojené s těmito osobami, od nichž vláda důvodně očekává, že získá určité druhy zahraničních zpravodajských informací", takže "program nepracuje na základě hromadného shromažďování komunikace". Rada pro dohled nad soukromím a občanskými svobodami, *Zpráva o programu "*Privacy and Civil Liberties Oversight Board".

[1] Od roku 2001 do roku 2020 umožňovala hlava V zákona FISA FBI žádat FISC o povolení k získání "hmotných věcí", které jsou důležité pro určitá povolená vyšetřování. *Viz* USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, § 215 (2001). Toto znění, které pozbylo platnosti, a tudíž již není zákonem, poskytovalo oprávnění, na jehož základě vláda svého času hromadně shromažďovala telefonní metadata. Ještě předtím, než toto ustanovení pozbylo platnosti, jej však zákon USA FREEDOM Act změnil tak, že vyžaduje, aby vláda založila žádost podanou FISC na "konkrétním termínu výběru". *Viz* USA FREEDOM Act, Pub. L. č. 114-23, 129 Stat.

268, § I 03 (2015).

Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, na 103 (2. července 2014).[2]

Co se týče dopisů o národní bezpečnosti, zákon USA FREEDOM Act z roku 2015 ukládá požadavek na "konkrétní termín výběru" pro používání těchto dopisů. *Viz* 12 U.S.C. § 3414(a)(2); 15 U.S.C.
§ 1681u; 15 U.S.C. § 1681v(a); 18 U.S.C. § 2709(b).

Výkonný příkaz č. 14086 dále stanoví, že "[c]ílený sběr je prioritní" a že pokud IC provádí hromadný sběr, "[h]loubkový sběr zpravodajských informací o signálech je povolen pouze na základě zjištění, ... že informace nezbytné k dosažení potvrzené zpravodajské priority nelze rozumně získat cíleným sběrem." *Viz* výkonný příkaz 14086, § 2 písm. c) bod ii) část A.

Pokud navíc IC rozhodne, že hromadné shromažďování splňuje tyto standardy, výkonný příkaz 14086 stanoví další záruky. Konkrétně výkonný příkaz vyžaduje, aby IC při hromadném shromažďování "použil přiměřené metody a technická opatření s cílem omezit shromažďované údaje pouze na ty, které jsou nezbytné k dosažení potvrzené zpravodajské priority, a zároveň minimalizovat shromažďování informací, které nejsou relevantní". *Viz id.* V nařízení se rovněž uvádí, že "činnosti v oblasti signálového zpravodajství", mezi něž patří dotazování na zpravodajské informace získané hromadným sběrem, - "se provádějí pouze na základě rozhodnutí založeného na přiměřeném posouzení všech relevantních faktorů, že tyto činnosti jsou nezbytné k dosažení potvrzené zpravodajské priority". *Viz id.* § 2 písm. a) bod ii) část A. Vyhláška tuto zásadu dále provádí tím, že uvádí, že IC smí provádět pouze hromadné dotazování na neomezené zpravodajské informace o signálech získané za účelem dosažení šesti přípustných cílů a že takové dotazování musí být prováděno v souladu se zásadami a postupy, které "náležitě zohledňují dopad [dotazování] na soukromí a občanské svobody všech osob bez ohledu na jejich státní příslušnost nebo místo jejich pobytu". *Viz id.* § 2 písm. c) bod iii) písm. d). Nakonec příkaz stanoví nakládání se shromážděnými údaji, jejich zabezpečení a kontrolu přístupu k nim. *Viz id.* § 2 písm. c) bod iii) část A a § 2 písm. c) bod iii) část B.

* * * * *

Doufáme, že vám tato vysvětlení pomohou. Pokud máte další otázky ohledně toho, jak IC USA plánuje implementovat exekutivní příkaz 14086, neváhejte se na nás obrátit.

Sincerely,

Christopher C. Fonzone Hlavní právní zástupce

[2] Oddíly 703 a 704, které opravňují IC zaměřit se na americké osoby nacházející se v zahraničí, vyžadují soudní příkaz (s výjimkou mimořádných okolností) a vždy vyžadují pravděpodobný důvod domnívat se, že cíl je cizí mocností, agentem cizí mocnosti nebo důstojníkem či zaměstnancem cizí mocnosti. *Viz50U.S.C.§§* 1881b, 1881c.