

**PROVÁDĚCÍ ROZHODNUTÍ KOMISE (EU) 2023/1795****ze dne 10. července 2023****podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o odpovídající úrovni ochrany osobních údajů poskytované rámcem EU–USA pro ochranu údajů***(oznámeno pod číslem C(2023) 4745)***(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) <sup>(1)</sup>, a zejména na čl. 45 odst. 3 uvedeného nařízení,

vzhledem k těmto důvodům:

**1. ÚVOD**

- (1) Nařízení (EU) 2016/679 <sup>(2)</sup> stanoví pravidla pro předávání osobních údajů správci nebo zpracovateli v Unii do třetích zemí a mezinárodním organizacím, pokud toto předávání spadá do oblasti působnosti uvedeného nařízení. Pravidla pro mezinárodní předávání údajů stanoví kapitola V uvedeného nařízení. Jakkoli je tok osobních údajů do zemí a ze zemí mimo Evropskou unii nezbytný pro rozvoj přeshraničního obchodu a mezinárodní spolupráce, úroveň ochrany osobních údajů v Unii nesmí být předáváním těchto údajů do třetích zemí nebo mezinárodních organizací oslabena <sup>(3)</sup>.
- (2) Podle čl. 45 odst. 3 nařízení (EU) 2016/679 může Komise prostřednictvím prováděcího aktu rozhodnout, že určitá třetí země, určité území či jedno nebo více konkrétních odvětví v určité třetí zemi zajišťuje odpovídající úroveň ochrany. Za této podmínky se může předávání osobních údajů do třetí země bez nutnosti získat další povolení uskutečnit, jak stanoví čl. 45 odst. 1 a 103. bod odůvodnění nařízení (EU) 2016/679.
- (3) Podle čl. 45 odst. 2 nařízení (EU) 2016/679 musí přijetí rozhodnutí o odpovídající ochraně vycházet z komplexní analýzy právního řádu dané třetí země, a to jak z hlediska pravidel použitelných pro dovozce údajů, tak z hlediska omezení a záruk vztahujících se k přístupu orgánů veřejné moci k osobním údajům. V tomto posouzení 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). To, zda tomu tak je, musí být posouzeno podle právních předpisů Unie, a to zejména nařízení (EU) 2016/679, jakož i judikatury Soudního dvora Evropské unie (dále jen „Soudní dvůr“) <sup>(4)</sup>.

<sup>(1)</sup> Úř. věst. L 119, 4.5.2016, s. 1.

<sup>(2)</sup> Seznam zkratk použitých v tomto rozhodnutí je pro usnadnění uveden v příloze VIII.

<sup>(3)</sup> Viz 101. bod odůvodnění nařízení (EU) 2016/679.

<sup>(4)</sup> Nejnověji viz věc C-311/18, Facebook Ireland a Schrems (Schrems II), ECLI:EU:C:2020:559.

- (4) Jak Soudní dvůr objasnil ve svém rozsudku ze dne 6. října 2015 ve věci C-362/14, Maximilian Schrems v. Data Protection Commissioner <sup>(5)</sup> (dále jen „rozsudek ve věci Schrems“), nevyžaduje to zjištění stejné úrovně ochrany. Zejména prostředky, které dotyčná třetí země k ochraně osobních údajů využívá, se mohou lišit od prostředků zavedených v Unii, pokud se v praxi ukážou jako účinné k zajištění odpovídající úrovně ochrany <sup>(6)</sup>. Standard odpovídající ochrany tedy nevyžaduje opakování pravidel Unie slovo od slova. Kritériem je spíše to, zda zahraniční systém jako celek zajišťuje prostřednictvím podstaty práva na soukromí a jeho účinného uplatňování, dozoru a vymáhání požadovanou úroveň ochrany <sup>(7)</sup>. Podle tohoto rozsudku by Komise při uplatňování tohoto standardu měla 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 činit v případě, že sledují takové legitimní cíle, jako je bezpečnost státu, a zda poskytuje účinnou právní ochranu proti takovým zásahům <sup>(8)</sup>. Vodítko v tomto ohledu nabízí i „referenční rámec pro odpovídající ochranu“ stanovený Evropským sborem pro ochranu osobních údajů, který má tento standard dále vyjasnit <sup>(9)</sup>.
- (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, Data Protection Commissioner v. Facebook Ireland Limited a Maximilian Schrems (dále jen „rozsudek ve věci Schrems II“), kterým bylo zrušeno prováděcí rozhodnutí Komise (EU) 2016/1250 <sup>(10)</sup> o předchozím transatlantickém rámci pro tok údajů, štítu EU–USA na ochranu soukromí. Soudní dvůr měl za to, že omezení ochrany osobních údajů, která plynou z vnitrostátních právních předpisů Spojených států upravujících přístup k takovým údajům předávaným z Unie do Spojených států a jejich použití orgány veřejné moci USA pro účely národní bezpečnosti, nejsou upravena takovým způsobem, aby odpovídala požadavkům, které jsou v zásadě rovnocenné požadavkům vyžadovaným v unijním právu, pokud jde o nezbytnost a přiměřenost takových zásahů do práva na ochranu osobních údajů <sup>(11)</sup>. Soudní dvůr měl rovněž za to, že neexistuje žádný prostředek nápravy u orgánu, který by osobám, jejichž údaje jsou předány do Spojených států, poskytoval záruky v zásadě rovnocenné zárukám vyžadovaným v článku 47 Listiny týkajícím se práva na účinnou právní ochranu <sup>(12)</sup>.
- (6) V návaznosti na rozsudek ve věci Schrems II zahájila Komise jednání s vládou USA s cílem přijmout nové rozhodnutí o odpovídající ochraně, které by splňovalo požadavky čl. 45 odst. 2 nařízení (EU) 2016/679, jak je vyložil Soudní dvůr. V důsledku těchto jednání přijaly Spojené státy dne 7. října 2022 výkonný dekret č. 14086 „Posílení záruk pro činnosti USA v oblasti signálového zpravodajství“ (EO 14086), který je doplněn nařízením o Soudu pro přezkum ochrany údajů vydaným ministrem spravedlnosti USA (nařízení ministra spravedlnosti) <sup>(13)</sup>. Kromě toho byl aktualizován rámec vztahující se na obchodní subjekty, které zpracovávají údaje předávané z Unie podle tohoto rozhodnutí, – „rámec EU–USA pro ochranu údajů“ (EU–U.S. Data Privacy Framework, dále též „rámec pro ochranu údajů“).
- (7) Komise provedla pečlivou analýzu práva a praxe USA, včetně výkonného dekretu č. 14086 a nařízení ministra spravedlnosti. Na základě zjištění stanovených v 9. až 200. bodě odůvodnění Komise došla k závěru, že Spojené státy zajišťují odpovídající úroveň ochrany osobních údajů předávaných na základě rámce EU–USA pro ochranu údajů ze strany správce nebo zpracovatele v Unii <sup>(14)</sup> certifikovaným organizacím ve Spojených státech.

<sup>(5)</sup> Věc C-362/14, Maximilian Schrems v. Data Protection Commissioner (Schrems), ECLI:EU:C:2015:650, bod 73.

<sup>(6)</sup> Rozsudek ve věci Schrems, bod 74.

<sup>(7)</sup> Viz sdělení Komise Evropskému parlamentu a Radě, Výměna a ochrana osobních údajů v globalizovaném světě, COM(2017) 7 ze dne 10. ledna 2017, oddíl 3.1, s. 6–7.

<sup>(8)</sup> Rozsudek ve věci Schrems, body 88–89.

<sup>(9)</sup> Evropský sbor pro ochranu osobních údajů, Referenční rámec pro odpovídající ochranu, WP 254 rev. 01, k dispozici na této adrese: [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=614108](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108)

<sup>(10)</sup> Prováděcí rozhodnutí Komise (EU) 2016/1250 ze dne 12. července 2016 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí (Úř. věst. L 207, 1.8.2016, s. 1).

<sup>(11)</sup> Rozsudek ve věci Schrems II, bod 185.

<sup>(12)</sup> Rozsudek ve věci Schrems II, bod 197.

<sup>(13)</sup> 28 CFR část 302.

<sup>(14)</sup> Toto rozhodnutí má význam pro EHP. Dohoda o Evropském hospodářském prostoru (Dohoda o EHP) stanoví rozšíření vnitřního trhu Evropské unie o tři státy EHP, a to Island, Lichtenštejnsko a Norsko. Rozhodnutí Smíšeného výboru, kterým se do přílohy XI Dohody o EHP začleňuje nařízení (EU) 2016/679, přijal Smíšený výbor EHP dne 6. července 2018 a v platnost vstoupilo dne 20. července 2018. Uvedená dohoda se tedy na nařízení vztahuje. Pro účely tohoto rozhodnutí se tudíž odkazy na EU a členské státy EU vykládají jako odkazy zahrnující i státy EHP.

- (8) Toto rozhodnutí má účinek v tom smyslu, že předávání osobních údajů ze strany správců a zpracovatelů v Unii certifikovaným organizacím ve Spojených státech <sup>(15)</sup> může probíhat, aniž by bylo nutné získat další povolení. Tímto rozhodnutím není dotčeno přímé uplatňování nařízení (EU) 2016/679 na takové organizace, pokud jsou splněny podmínky týkající se místní působnosti uvedeného nařízení, stanovené v jeho článku 3.

## 2. RÁMEC EU–USA PRO OCHRANU ÚDAJŮ

### 2.1 Osobní a věcná působnost

#### 2.1.1 Certifikované organizace

- (9) Rámec EU–USA pro ochranu údajů je založen na systému certifikace, kterým se organizace USA zavazují k dodržování souboru zásad ochrany soukromí – „zásad rámce EU–USA pro ochranu údajů“, včetně doplňkových zásad (společně dále jen „zásady“), které vydalo Ministerstvo obchodu Spojených států a které jsou obsahem přílohy I tohoto rozhodnutí <sup>(16)</sup>. Aby bylo možné získat certifikaci podle rámce EU–USA pro ochranu údajů, musí organizace podléhat vyšetřovacím a donucovacím pravomocem Federální obchodní komise (Federal Trade Commission, FTC) nebo Ministerstva dopravy USA <sup>(17)</sup>. Zásady jsou použitelné bezprostředně po certifikaci. Jak je podrobněji vysvětleno ve 48. až 52. bodě odůvodnění, organizace rámce EU–USA pro ochranu údajů jsou povinny každoročně opětovně získat certifikaci o tom, že tyto zásady dodržují <sup>(18)</sup>.

#### 2.1.2 Definice osobních údajů a pojmy správce a „zprostředkovatel“

- (10) Ochrana poskytovaná na základě rámce EU–USA pro ochranu údajů se vztahuje na všechny osobní údaje předávané z Unie organizacím v USA, které u Ministerstva obchodu osvědčily 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 <sup>(19)</sup>. Tyto informace proto nelze předávat na základě rámce EU–USA pro ochranu údajů.
- (11) Zásady definují osobní údaje / osobní informace stejným způsobem jako nařízení (EU) 2016/679, tedy jako „údaje o identifikované nebo identifikovatelné fyzické osobě, které spadají do oblasti působnosti obecného nařízení o ochraně osobních údajů, jež organizace ve Spojených státech obdrží z EU a jež jsou zaznamenány v jakékoli formě“ <sup>(20)</sup>. V souladu s tím se vztahují také na pseudonymizované výzkumné údaje (nebo výzkumné údaje „kódované pomocí klíče“) (včetně případů, kdy klíč není sdílen s přijímající organizací v USA) <sup>(21)</sup>. Pojem zpracování je obdobně definován jako „jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenání, uspořádání, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění nebo šíření a výmaz nebo zničení“ <sup>(22)</sup>.
- (12) Rámec EU–USA pro ochranu údajů 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) <sup>(23)</sup> nebo zpracovatelé (tj. zprostředkovatelé jednající jménem správce) <sup>(24)</sup>. Zpracovatelé v USA musí být smluvně zavázáni

<sup>(15)</sup> Tímto rozhodnutím nejsou dotčeny požadavky nařízení (EU) 2016/679, které se vztahují na subjekty (správce a zpracovatele) v Unii předávající údaje, například na účelové omezení, minimalizaci údajů, transparentnost a zabezpečení údajů (viz také článek 44 nařízení (EU) 2016/679).

<sup>(16)</sup> V tomto ohledu viz rozsudek ve věci Schrems, bod 81, v němž Soudní dvůr potvrdil, že systém vlastního osvědčení může zajistit odpovídající úroveň ochrany.

<sup>(17)</sup> Příloha I oddíl I odst. 2. Federální obchodní komise má širokou pravomoc nad obchodními činnostmi až na některé výjimky, např. pokud jde o banky, letecké dopravce, pojišťovnictví a běžné přenosové činnosti poskytovatelů telekomunikačních služeb (ačkoli rozhodnutí Odvolacího soudu USA pro devátý obvod ze dne 26. února 2018 ve věci FTC v. AT&T potvrdilo, že Federální obchodní komise má pravomoc nad činnostmi těchto subjektů, které nejsou běžnými přenosovými činnostmi). Viz také příloha IV, poznámka pod čarou č. 2. Ministerstvo dopravy má pravomoc vymáhat dodržování předpisů od leteckých dopravců a prodejců letenek (pro leteckou dopravu), viz příloha V, oddíl A.

<sup>(18)</sup> Příloha I oddíl III odst. 6.

<sup>(19)</sup> Příloha I oddíl III odst. 2.

<sup>(20)</sup> Příloha I oddíl I odst. 8 písm. a.

<sup>(21)</sup> Příloha I oddíl III odst. 14 písm. g.

<sup>(22)</sup> Příloha I oddíl I odst. 8 písm. b.

<sup>(23)</sup> Příloha I oddíl I odst. 8 písm. c.

<sup>(24)</sup> Viz např. příloha I oddíl II odst. 2 písm. b, odst. 3 písm. b a odst. 7 písm. d, z nichž jasně vyplývá, že zprostředkovatelé jednají jménem správce podle jeho pokynů a na základě konkrétních smluvních povinností.

k tomu, že budou konat pouze na pokyny správce z EU a že mu budou nápomocni při odpovídání fyzickým osobám uplatňujícím svá práva podle zásad <sup>(25)</sup>. Jsou-li údaje navíc zpracovávány externě, musí zpracovatel uzavřít s externím zpracovatelem smlouvu, která zaručí stejnou úroveň ochrany, jakou poskytují zásady, a přijmout opatření k zajištění jejího řádného plnění <sup>(26)</sup>.

## 2.2 Zásady rámce EU–USA pro ochranu údajů

### 2.2.1 Účelové omezení a možnost volby

- (13) Osobní údaje by měly být zpracovávány zákonným a korektním způsobem. Měly by být shromažďovány za konkrétním účelem a následně používány, pouze pokud to není neslučitelné s účelem zpracování.
- (14) Podle rámce EU–USA pro ochranu údajů je toto zajištěno prostřednictvím různých zásad. Za prvé, podle *zásady integrity údajů a účelového omezení*, obdobně 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 subjektem údajů povoleny <sup>(27)</sup>.
- (15) Za druhé, dříve než organizace použije osobní údaje pro nový (změněný) účel, který je významně odlišný, ale stále slučitelný s původním účelem, nebo než je zpřístupní třetí straně, musí subjektům údajů poskytnout možnost vyslovit nesouhlas (opt-out) v souladu se *zásadou možnosti volby* <sup>(28)</sup> prostřednictvím jasného, srozumitelného a snadno dostupného mechanismu. Důležité je, že tato zásada nenahrazuje výslovný zákaz neslučitelného zpracování <sup>(29)</sup>.

<sup>(25)</sup> Příloha I oddíl III odst. 10 písm. a. Viz také pokyny, které pro účely štítu na ochranu soukromí připravilo Ministerstvo obchodu po konzultaci s Evropským sborem pro ochranu osobních údajů a které upřesnily povinnosti amerických zpracovatelů přijímajících na základě daného rámce osobní údaje z Unie. Vzhledem k tomu, že se tato pravidla nezměnila, zůstávají tyto pokyny / často kladené dotazy relevantní i pro účely rámce EU–USA pro ochranu údajů (<https://www.privacyshield.gov/article?id=Processing-FAQs>).

<sup>(26)</sup> Příloha I oddíl II odst. 3 písm. b.

<sup>(27)</sup> Příloha I oddíl II odst. 5 písm. a. Mezi slučitelné účely může patřit audit, prevence podvodů nebo jiné účely, které odpovídají přiměřenému očekávání vzhledem k souvislostem shromažďování (viz příloha I, poznámka pod čarou č. 6).

<sup>(28)</sup> Příloha I oddíl II odst. 2 písm. a. To neplatí, pokud organizace poskytuje osobní údaje zpracovateli, který jedná jejím jménem a podle jejích pokynů (příloha I oddíl II odst. 2 písm. b). V tomto případě však organizace musí mít uzavřenou smlouvu a zajistit soulad se zásadou *odpovědnosti za další předávání*, jak je podrobněji popsáno ve 43. bodě odůvodnění. Zásada *možnosti volby* může být kromě toho (stejně jako zásada *oznamovací povinnosti*) omezena, pokud jsou osobní údaje zpracovávány v souvislosti s hloubkovou kontrolou (jako součást potenciální fúze nebo převzetí) nebo auditu, 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 ohrozilo oprávněné zájmy organizace v konkrétní souvislosti s hloubkovou kontrolou nebo auditu (příloha I oddíl III odst. 4). Doplňková zásada č. 15 (příloha I oddíl III odst. 15 písm. a a b) rovněž stanoví výjimku ze zásady *možnosti volby* (jakož i ze zásad *oznamovací povinnosti* 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 ze záznamů, které jsou obecně přístupné veřejnosti (pokud nejsou kombinovány s informacemi z neveřejných záznamů a jsou dodrženy veškeré podmínky pro nahlížení). Podobně doplňková zásada č. 14 (příloha I oddíl III odst. 14 písm. f) stanoví výjimku ze *zásady možnosti volby* (jakož i ze zásad *oznamovací povinnosti* a *odpovědnosti za další předávání*) pro zpracování osobních údajů farmaceutickou společností nebo společností vyrábějící zdravotnické prostředky při činnostech v oblasti sledování bezpečnosti a účinnosti výrobků, pokud dodržování těchto zásad narušuje dodržování regulačních požadavků.

<sup>(29)</sup> To se vztahuje na veškeré předávání údajů na základě rámce EU–USA pro ochranu údajů, včetně případů, kdy se toto předávání týká údajů shromážděných v souvislosti se zaměstnaneckým vztahem. Certifikovaná organizace USA proto v zásadě může použít údaje v oblasti lidských zdrojů pro různé účely nesouvisějící se zaměstnáváním (např. pro některé druhy marketingové komunikace), musí však přitom respektovat zákaz neslučitelného zpracování, a navíc tak může činit jen v souladu se zásadou *oznamovací povinnosti* a zásadou *možnosti volby*. Organizace může výjimečně použít osobní údaje pro další slučitelný účel, aniž by dodržela zásadu *oznamovací povinnosti* a zásadu *možnosti volby*, ale pouze v rozsahu a po dobu nezbytnou k tomu, aby nebyla dotčena schopnost organizace povyšovat, jmenovat nebo přijímat podobná personální rozhodnutí (viz příloha I oddíl III odst. 9 písm. b bod iv)). Zákaz uplatňování sankcí ze strany organizace USA vůči zaměstnanci, který uplatňuje svou možnost volby, včetně omezení z hlediska zaměstnaneckých příležitostí, zajišťuje, že se zaměstnanec navzdory podřízenému vztahu a inherentní závislosti nebude cítit pod nátlakem, a může tak provést opravdu svobodnou volbu. Viz příloha I oddíl III odst. 9 písm. b bod i).

### 2.2.2 *Zpracování zvláštních kategorií osobních údajů*

- (16) Pokud se zpracovávají „zvláštní kategorie“ údajů, měly by existovat zvláštní záruky.
- (17) V souladu se zásadou možnosti volby se zvláštní záruky vztahují na zpracování „citlivých informací“, tj. osobních údajů vypovídajících o zdravotním stavu, rasovém nebo etnickém původu, politických postojích, náboženském nebo filozofickém přesvědčení, členství v odborových organizacích, informací o sexuální životě dané osoby nebo jakýchkoli jiných informací získaných od třetí strany, které tato strana označí a považuje za citlivé <sup>(30)</sup>. To znamená, že s jakýmkoliv údaji, které jsou považovány za citlivé podle právních předpisů Unie o ochraně údajů (včetně údajů o sexuální orientaci, genetických údajů a biometrických údajů), bude podle rámce EU–USA pro ochranu údajů certifikovanými organizacemi zacházeno jako s citlivými.
- (18) Obecně platí, že k použití citlivých informací pro jiné účely, než pro které byly původně shromážděny nebo následně fyzickou osobou schváleny (prostřednictvím opt-in), nebo k jejich zpřístupnění třetím stranám musí organizace od fyzických osob získat potvrzující výslovný souhlas (tj. opt-in) <sup>(31)</sup>.
- (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 k poskytnutí zdravotní péče nebo určení diagnózy <sup>(32)</sup>.

### 2.2.3 *Přesnost, minimalizace a zabezpečení údajů*

- (20) Údaje musí být přesné a v případě potřeby aktualizované. Měly by být také přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelům, pro které jsou zpracovávány, a v zásadě by se neměly uchovávat déle, než je nezbytné pro účely, k nimž jsou dané osobní údaje zpracovávány.
- (21) Podle zásady integrity údajů a účelového omezení <sup>(33)</sup> musí být osobní údaje omezeny na údaje relevantní k účelu zpracování. Organizace je kromě toho povinna v rozsahu nezbytném pro účely zpracování podniknout přiměřené kroky, aby zajistila spolehlivost osobních údajů pro zamýšlený účel, jejich přesnost, úplnost a aktuálnost.
- (22) Osobní informace lze nadto uchovávat v podobě ztotožňující fyzickou osobu nebo umožňující její ztotožnění (tedy v podobě osobních údajů) <sup>(34)</sup> jen potud, pokud tyto informace slouží účelu (účelům), pro který byly původně shromážděny nebo následně fyzickou osobou schváleny v souladu se zásadou možnosti volby. Tato povinnost organizacím nebrání v tom, aby nadále zpracovávaly osobní informace po delší období, mohou tak ale činit jen po dobu a v rozsahu, který přiměřeně slouží jednomu z následujících konkrétních účelů, podobně jako srovnatelné výjimky stanovené v právu Unie v oblasti ochrany údajů: archivace ve veřejném zájmu, žurnalistika, literatura a umění, vědecký a historický výzkum a statistická analýza <sup>(35)</sup>. Pokud jsou osobní údaje uchovávány pro jeden z těchto účelů, jejich zpracování podléhá zárukám stanovených v zásadách <sup>(36)</sup>.
- (23) Osobní údaje by také měly být zpracovávány způsobem, který zajišťuje jejich zabezpečení, včetně ochrany před neoprávněným nebo protiprávním 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 přihlédnutím ke stavu techniky, souvisejícím nákladům a k povaze, rozsahu, kontextu a účelům zpracování i k rizikům pro práva fyzických osob.

<sup>(30)</sup> Příloha I oddíl II odst. 2 písm. c.

<sup>(31)</sup> Příloha I oddíl II odst. 2 písm. c.

<sup>(32)</sup> Příloha I oddíl III odst. 1.

<sup>(33)</sup> Příloha I oddíl II odst. 5.

<sup>(34)</sup> 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 by bylo možné s přiměřenou pravděpodobností využít (mimo jiné s ohledem na náklady a množství času potřebné k identifikaci a na dostupnou technologii v době zpracování).

<sup>(35)</sup> Příloha I oddíl II odst. 5 písm. b.

<sup>(36)</sup> Tamtéž.

- (24) Na základě rámce EU–USA pro ochranu údajů to zajišťuje *zásada zabezpečení*, která podobně jako článek 32 nařízení (EU) 2016/679 vyžaduje přijetí přiměřených a vhodných bezpečnostních opatření s přihlédnutím k rizikům spojeným se zpracováním a povahou údajů <sup>(37)</sup>.

#### 2.2.4 Transparentnost

- (25) Subjekty údajů by měly být informovány o hlavních znacích zpracování jejich osobních údajů.
- (26) To je zajištěno prostřednictvím *zásady oznamovací povinnosti* <sup>(38)</sup>, která podobně jako požadavky na transparentnost podle nařízení (EU) 2016/679 vyžaduje, aby organizace informovaly subjekty údajů mimo jiné o i) účasti organizace v rámci pro ochranu údajů, ii) druhu shromažďovaných údajů, iii) účelu zpracování, iv) typu nebo totožnosti třetích stran, kterým mohou být osobní údaje zpřístupněny, a o účelech takového zpřístupnění, v) jejich individuálních právech, vi) způsobu kontaktování organizace a vii) dostupných možnostech nápravy.
- (27) Toto oznámení musí být učiněno jasně a zřetelně při první příležitosti, při které je fyzická osoba požádána, aby poskytla své osobní údaje, nebo co možná nejdříve poté, avšak v každém případě předtím, než jsou tyto údaje použity pro účel výrazně odlišný (ale slučitelný), než pro jaký byly původně shromážděny, nebo před tím, než jsou zpřístupněny třetí straně <sup>(39)</sup>.
- (28) Organizace musí kromě toho zveřejnit své politiky ochrany soukromí odrážející zásady (nebo je v případě údajů o lidských zdrojích snadno zpřístupnit dotčeným osobám) a poskytnout odkazy na internetové stránky Ministerstva obchodu (s dalšími podrobnostmi o certifikaci, právech subjektů údajů a dostupných odvolacích mechanismech), seznam organizací rámce pro ochranu údajů a internetové stránky příslušného poskytovatele alternativního řešení sporů <sup>(40)</sup>.

#### 2.2.5 Individuální práva

- (29) Subjekty údajů by měly mít určitá práva, která lze vůči správci nebo zpracovateli vymáhat, zejména právo na přístup k údajům, právo vznést námitku proti zpracování a právo na opravu a výmaz údajů.
- (30) Tato práva poskytuje jednotlivcům *zásada práva na přístup* <sup>(41)</sup> rámce EU–USA pro ochranu údajů. Subjekty údajů mají zejména právo na to, aby jim bez nutnosti zdůvodnění organizace potvrdila, zda tato organizace zpracovává osobní údaje, které se jich týkají; aby jim tyto údaje byly sděleny; a získat informace o účelu zpracování, kategoriích zpracovávaných osobních údajů a (kategoriích) příjemců, kterým jsou údaje zpřístupněny <sup>(42)</sup>. Organizace jsou povinny reagovat na žádosti o přístup v přiměřené lhůtě <sup>(43)</sup>. Organizace může přiměřeně omezit počet žádostí

<sup>(37)</sup> Příloha I oddíl II odst. 4 písm. a. Pokud jde o údaje v oblasti lidských zdrojů, rámec EU–USA pro ochranu údajů kromě toho požaduje, aby zaměstnavatelé vycházeli vstříc preferencím zaměstnanců z hlediska ochrany soukromí a omezovali přístup k osobním údajům, anonymizovali některé údaje nebo jim přidělovali kódy či pseudonymy (příloha I oddíl III odst. 9 písm. b. bod iii).

<sup>(38)</sup> Příloha I oddíl II odst. 1.

<sup>(39)</sup> Příloha I oddíl II odst. 1 písm. b. Doplnková zásada č. 14 (příloha I oddíl III odst. 14 písm. b a c) stanoví zvláštní ustanovení pro zpracování osobních údajů v souvislosti se zdravotnickým výzkumem a klinickým hodnocením. Tato zásada zejména umožňuje organizacím zpracovávat údaje z klinických hodnocení i poté, co osoba od hodnocení odstoupí, pokud to bylo jasně uvedeno v oznámení, které bylo poskytnuto při souhlasu s účastí. Stejně tak v případě, že organizace rámce EU–USA pro ochranu údajů obdrží osobní údaje pro účely zdravotnického výzkumu, může je použít pro novou výzkumnou činnost jediné v souladu se zásadou *oznamovací povinnosti* a zásadou *možnosti 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 použití pro účely výzkumu může vyplynout z nových poznatků nebo vývoje v oblasti lékařství/výzkumu), musí být zahrnuto vysvětlení, že údaje mohou být použity v rámci budoucích nepředvídaných lékařských a farmaceutických výzkumných činností. Pokud takové další použití neodpovídá obecným výzkumným účelům, pro které byly údaje shromážděny (tj. pokud jsou nové účely výrazně odlišné, ale stále slučitelné s původním účelem, viz 14.–15. bod odůvodnění), je třeba získat nový souhlas (tj. opt-in). Dále viz konkrétní omezení/výjimky ze zásady *oznamovací povinnosti* popsané v poznámce pod čarou č. 28.

<sup>(40)</sup> Příloha I oddíl III odst. 6 písm. d.

<sup>(41)</sup> Viz také doplnková zásada práva na přístup (příloha I oddíl III odst. 8).

<sup>(42)</sup> Příloha I oddíl III odst. 8 písm. a body i) až ii).

<sup>(43)</sup> Příloha I oddíl III odst. 8 písm. i.

o přístup od určité osoby, kterým v daném období vyhoví, a může účtovat poplatek, který není nepřiměřený, např. v případě, že žádosti jsou zjevně nepřiměřené, zvláště z toho důvodu, že se opakují <sup>(44)</sup>.

- (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 legitimní práva jiných osob; pokud by zátěž nebo náklady spojené s poskytnutím přístupu byly za daných okolností nepřiměřené rizikům pro soukromí jednotlivce (ačkoli náklady a zátěž nejsou rozhodujícími faktory při určování, zda je poskytnutí přístupu přiměřené); v rozsahu, v němž by zveřejnění pravděpodobně ohrozilo důležité veřejné zájmy, jako je např. bezpečnost státu, veřejná bezpečnost nebo obrana; informace obsahují důvěrné obchodní informace; nebo jsou informace zpracovávány výhradně pro účely výzkumu nebo statistiky <sup>(45)</sup>. Jakékoli odepření práva či jeho omezení musí být nezbytné a řádně odůvodněné, přičemž důkazní břemeno toho, že jsou tyto požadavky splněny, leží na organizaci <sup>(46)</sup>. Při tomto posuzování musí organizace přihlížet zejména k zájmům fyzické osoby <sup>(47)</sup>. Pokud je možné oddělit informace od ostatních údajů, na které se vztahuje omezení, musí organizace chráněné informace oddělit a ostatní informace zpřístupnit <sup>(48)</sup>.
- (32) Subjekty údajů mají kromě toho právo na opravu nebo změnu nepřesných údajů a na výmaz údajů, které byly zpracovány v rozporu se zásadami <sup>(49)</sup>. Podle vysvětlení v 15. bodě odůvodnění mají fyzické osoby nadto právo vznést námitku proti zpracování / vyslovit nesouhlas se zpracováním svých údajů pro významně odlišné (ale slučitelné) účely, než pro které byly údaje shromážděny, a proti zpřístupnění svých údajů třetím stranám. Pokud jsou osobní údaje používány pro účely přímého marketingu, mají fyzické osoby obecné právo vyslovit nesouhlas se zpracováním kdykoli <sup>(50)</sup>.
- (33) Zásady se výslovně nezabývají otázkou rozhodnutí, která se dotýkají subjektu údajů a která jsou založena výhradně na automatizovaném zpracování osobních údajů. Pokud však jde o osobní údaje, které byly shromážděny v Unii, jakékoli rozhodnutí založené na automatizovaném zpracování bude obvykle činit správce v Unii (který má přímý vztah s dotyčným subjektem údajů), a vztahuje se tedy na něj nařízení (EU) 2016/679 <sup>(51)</sup>. To zahrnuje situace předávání, kdy zpracování provádí zahraniční (např. americký) podnikatelský subjekt jednající jako zprostředkovatel (zpracovatel) jménem správce v Unii (nebo jako externí zpracovatel jednající jménem zpracovatele z Unie, jenž získal údaje od správce v Unii, který je shromáždil), který na tomto základě činí rozhodnutí.
- (34) To potvrdila studie, kterou si Komise nechala vypracovat v roce 2018 v souvislosti s druhým výročním přezkumem fungování štítu na ochranu soukromí <sup>(52)</sup> a 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.

<sup>(44)</sup> Příloha I oddíl III odst. 8 písm. f body i) až ii) a písm. g.

<sup>(45)</sup> Příloha I oddíl III odst. 4; odst. 8 písm. b, c, e; odst. 14 písm. e, f a odst. 15 písm. d.

<sup>(46)</sup> Příloha I oddíl III odst. 8 písm. e bod ii). Organizace musí fyzické osoby informovat o důvodech zamítnutí/omezení a poskytnout kontaktní údaje pro případné další dotazy, oddíl III odst. 8 písm. a bod iii).

<sup>(47)</sup> Příloha I oddíl III odst. 8 písm. a. body ii) až iii).

<sup>(48)</sup> Příloha I oddíl III odst. 8 písm. a bod i).

<sup>(49)</sup> Příloha I oddíl II odst. 6 a oddíl III odst. 8 písm. a bod i).

<sup>(50)</sup> Příloha I oddíl III odst. 8 a 12.

<sup>(51)</sup> Naproti tomu ve výjimečném případě, kdy má americká organizace přímý vztah se subjektem údajů z Unie, to obvykle bude důsledek cíleného zaměření na danou fyzickou osobu v Unii, které nabízí zboží nebo služby nebo monitoruje její chování. V tomto případě bude americká organizace sama spadat do oblasti působnosti nařízení (EU) 2016/679 (čl. 3 odst. 2), a musí tedy přímo dodržovat právní předpisy Unie na ochranu údajů.

<sup>(52)</sup> SWD(2018) 497 final, oddíl 4.1.5. Studie se zaměřila na i) rozsah, v jakém organizace štítu na ochranu soukromí v USA přijímají rozhodnutí mající dopad na fyzické osoby na základě automatizovaného zpracování osobních údajů předávaných ze společností v EU v rámci štítu na ochranu soukromí, a ii) záruky pro fyzické osoby, které pro tento druh situací stanoví federální právo USA, a podmínky pro uplatnění těchto záruk.

- (35) V každém případě v oblastech, kde společnosti nejčastěji využívají automatizovaného zpracování osobních údajů pro rozhodování, které má dopad na fyzickou osobu (např. úvěry a půjčky, nabídky hypoték, zaměstnání, bydlení a pojištění), poskytuje právo USA konkrétní ochranu proti negativním rozhodnutím<sup>(53)</sup>. Tyto předpisy obvykle stanoví, že fyzické osoby mají právo být informovány o konkrétních důvodech, které stály za rozhodnutím (např. zamítnutím úvěru), rozporovat neúplné nebo nepřesné informace (jakož i použití nezákonných faktorů) a požadovat nápravu. V oblasti spotřebitelských úvěrů obsahují zákon o spravedlivém informování o úvěrové spolehlivosti (Fair Credit Reporting Act) a zákon o rovné příležitosti k získání úvěru (Equal Credit Opportunity Act) záruky, které spotřebitelům poskytují určitou formu práva na vysvětlení a práva napadnout rozhodnutí. Tyto zákony mají význam v celé řadě oblastí, včetně úvěrů, zaměstnání, bydlení a pojištění. Některé antidiskriminační zákony, jako je hlava VII zákona o občanských právech a zákon o spravedlivém bydlení, poskytují kromě toho fyzickým osobám ochranu s ohledem na modely používané při automatizovaném rozhodování, které by mohlo vést k diskriminaci na základě určitých prvků, a přiznávají fyzickým osobám právo napadnout taková rozhodnutí, včetně automatizovaných rozhodnutí. Pokud jde o zdravotní informace, pravidlo o ochraně soukromí zákona o přenositelnosti zdravotního pojištění a o související odpovědnosti stanoví určitá práva, která jsou podobná právům uvedeným v nařízení (EU) 2016/679, pokud jde o přístup k osobním zdravotním informacím. Pokyny amerických orgánů navíc vyžadují, aby poskytovatelé zdravotní péče obdrželi informace, které jim umožní informovat fyzické osoby o systémech automatizovaného rozhodování používaných ve zdravotnictví<sup>(54)</sup>.
- (36) Proto tato pravidla poskytují ochranu podobnou ochraně poskytované podle práva Unie v oblasti ochrany údajů v nepravděpodobné situaci, kdy by organizace rámce EU–USA pro ochranu údajů samy přijímaly automatizovaná rozhodnutí.

#### 2.2.6 Omezení dalšího předávání

- (37) Úroveň ochrany poskytovaná osobním údajům předávaným z Unie organizacím ve Spojených státech nesmí být oslabena dalším předáváním těchto údajů příjemci ve Spojených státech nebo jiné třetí zemi.
- (38) Podle *zásady odpovědnosti za další předávání*<sup>(55)</sup> platí zvláštní pravidla pro tzv. „další předávání“, tj. předávání osobních údajů z organizace rámce EU–USA pro ochranu údajů třetí straně jednající jako správce nebo zpracovatel neohledně na to, zda se tato třetí strana nachází ve Spojených státech nebo ve třetí zemi mimo Spojené státy (a Unii). Jakékoli další předávání může probíhat pouze i) pro omezené a přesně stanovené účely, ii) na základě smlouvy mezi organizací rámce EU–USA pro ochranu údajů a třetí stranou<sup>(56)</sup> (nebo srovnatelného ujednání v rámci skupiny podniků<sup>(57)</sup>) a iii) pouze tehdy, pokud tato smlouva stanoví povinnost, 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 účelového omezení* 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 fyzickou osobou (v souladu se *zásadou možnosti volby*).

<sup>(53)</sup> Viz např. zákon o rovné příležitosti k získání úvěru (Equal Credit Opportunity Act, 15 U.S.C. 1691 a násl.), zákon o spravedlivém informování o úvěrové spolehlivosti (Fair Credit Reporting Act, 15 USC § 1681 a násl.) nebo zákon o spravedlivém bydlení (Fair Housing Act, 42 U.S.C. 3601 a násl.). Kromě toho se Spojené státy přihlasy k zásadám Organizace pro hospodářskou spolupráci a rozvoj v oblasti umělé inteligence, které mimo jiné zahrnují zásady transparentnosti, schopnosti vysvětlovat, bezpečnosti a odpovědnosti.

<sup>(54)</sup> Viz např. pokyny dostupné na adrese 2042-What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans? | HHS.gov.

<sup>(55)</sup> Viz příloha I oddíl II odst. 3 a doplňková zásada „povinné smlouvy pro účely dalšího předávání“ (příloha I oddíl III odst. 10).

<sup>(56)</sup> Na základě výjimky z této obecné zásady může organizace dále předávat osobní údaje malého počtu zaměstnanců bez uzavření smlouvy s příjemcem pro příležitostné provozní potřeby související se zaměstnáním, např. rezervace letu, hotelového pokoje nebo pojištění. I v tomto případě však musí organizace dodržovat zásadu *oznamovací povinnosti* a zásadu *možnosti volby* (viz příloha I oddíl III odst. 9 písm. e).

<sup>(57)</sup> Viz doplňková zásada „povinné smlouvy pro účely dalšího předávání“ (příloha I oddíl III odst. 10 písm. b). Přestože tato zásada umožňuje předávání založené také na nesmluvních nástrojích (např. vnitroskupinové programy dodržování předpisů a kontrolní programy), text jasně uvádí, že tyto nástroje musí vždy „zajistit kontinuitu ochrany osobních informací podle zásad“. Navíc to, že certifikované organizace USA zůstanou odpovědné za dodržování zásad, bude silným impulsem k použití nástrojů, které jsou v praxi opravdu účinné.

- (40) *Zásadu odpovědnosti za další předávání* je třeba vykládat rovněž ve spojení se *zásadou oznamovací povinnosti* a v případě dalšího předávání správci, který je třetí stranou <sup>(58)</sup>, se *zásadou možnosti volby*, podle níž musí být subjekty údajů informovány (mimo jiné) o druhu/totožnosti jakéhokoli příjemce, který je třetí stranou, o účelu dalšího předávání, a o nabízené možnosti volby a mohou vyslovit nesouhlas (opt-out), nebo v případě citlivých údajů musí vyslovit „potvrzující výslovný souhlas“ (opt-in) s dalším předáváním.
- (41) Povinnost poskytnout stejnou úroveň ochrany, jakou požadují zásady, se použije na všechny třetí strany, které jsou zapojeny do zpracování takto předávaných údajů neohledně na to, kde se nacházejí (v USA nebo v jiné třetí zemi), jakož i v případě, kdy původní příjemce, který je třetí stranou, sám předá tyto údaje jinému příjemci, který je třetí stranou, např. za účelem externího zpracování.
- (42) Ve všech případech musí být ve smlouvě s příjemcem, který je třetí stranou, stanoveno, že příjemce bude informovat organizaci rámce EU–USA pro ochranu údajů, pokud zjistí, že již nemůže plnit svůj závazek. Je-li takové zjištění učiněno, zpracování touto třetí stranou musí být ukončeno nebo musí být přijaty jiné přiměřené a vhodné kroky k nápravě situace <sup>(59)</sup>.
- (43) V případě dalšího předání zprostředkovateli, který je třetí stranou (tj. zpracovatel), platí doplňková ochrana. V tomto případě musí organizace USA zajistit, aby zprostředkovatel jednal pouze na základě jejích pokynů, a přijmout přiměřené a vhodné kroky, aby i) zajistila, že zprostředkovatel účinně zpracovává osobní informace předané způsobem, který je v souladu s povinnostmi organizace podle zásad, a ii) na základě oznámení ukončila a napravila nepovolené zpracovávání <sup>(60)</sup>. Ministerstvo obchodu může od organizace požadovat, aby poskytla shrnutí nebo reprezentativní kopii ustanovení smlouvy týkající se ochrany soukromí <sup>(61)</sup>. Pokud v řetězci (dílčích) zpracování vzniknou problémy s dodržováním předpisů, organizace jednající jako správce osobních údajů v zásadě ponese odpovědnost, jak je uvedeno v *zásadě odvolání, prosazování a odpovědnosti*, s výjimkou případů, kdy prokáže, že za událost, která vedla ke vzniku škody, není odpovědná <sup>(62)</sup>.

### 2.2.7 Odpovědnost

- (44) Podle zásady odpovědnosti se od subjektů zpracovávajících údaje vyžaduje zavedení vhodných technických a organizačních opatření, aby mohly účinně plnit své povinnosti v oblasti ochrany údajů a jejich plnění byly schopny prokázat, zejména příslušnému dozorovému úřadu.
- (45) Jakmile se organizace dobrovolně rozhodne pro certifikaci <sup>(63)</sup> podle rámce EU–USA pro ochranu údajů, je účinné dodržování zásad z její strany povinné a vymahatelné. Podle *zásady odvolání, prosazování a odpovědnosti* <sup>(64)</sup> musí organizace rámce EU–USA pro ochranu údajů poskytnout účinné mechanismy k zajištění dodržování zásad. Organizace musí také přijmout opatření k ověření toho <sup>(65)</sup>, zda jejich politika ochrany soukromí vyhovuje zásadám a je v praxi dodržována. Toto lze provádět buď systémem sebehodnocení, jehož součástí musí být interní postupy, kterými se zajistí, aby zaměstnanci obdrželi školení k provádění politiky ochrany soukromí organizace a aby dodržování této politiky bylo pravidelně a objektivně kontrolováno, anebo externími přezkumy jejího dodržování, které mohou mít podobu auditu, namátkových kontrol nebo použití technologických nástrojů.

<sup>(58)</sup> Fyzické osoby nebudou mít právo vyslovit nesouhlas, jsou-li osobní údaje předávány třetí straně, která jedná jako zprostředkovatel a vykonává úkoly jménem organizace USA a podle jejích pokynů. To však vyžaduje smlouvu se zprostředkovatelem a organizace USA ponese odpovědnost za zaručení ochrany poskytované podle zásad tím, že vykonává svou pravomoc udělovat pokyny.

<sup>(59)</sup> Situace se různí v závislosti na tom, zda je třetí strana správcem, nebo zpracovatelem (zprostředkovatelem). V prvním případě musí smlouva s třetí stranou stanovit, že tato třetí strana přestane údaje zpracovávat nebo přijme jiné přiměřené a vhodné kroky k nápravě situace. Ve druhém případě pak tato opatření přijímá organizace rámce EU–USA pro ochranu údajů, která spravuje zpracování a jejímiž pokyny se řídí zprostředkovatel. Viz příloha I oddíl II odst. 3.

<sup>(60)</sup> Příloha I oddíl II odst. 3 písm. b.

<sup>(61)</sup> *Tamtéž*.

<sup>(62)</sup> Příloha I oddíl II odst. 7 písm. d.

<sup>(63)</sup> Viz také doplňková zásada „autocertifikace“ (příloha I oddíl III odst. 6).

<sup>(64)</sup> Viz také doplňková zásada „řešení sporů a prosazování“ (příloha I oddíl III odst. 11).

<sup>(65)</sup> Viz také doplňková zásada „ověřování“ (příloha I oddíl III odst. 7).

- (46) Organizace musí kromě toho uchovávat záznamy o uplatňování svých postupů podle rámce EU–USA pro ochranu údajů a zpřístupnit je na požádání v souvislosti s vyšetřováním nebo stížností na nedodržování předpisů nezávislému subjektu pro řešení sporů nebo příslušnému orgánu pro prosazování práva <sup>(66)</sup>.

### 2.3 Správa, dohled a prosazování

- (47) Rámec EU–USA pro ochranu údajů bude spravován a monitorován Ministerstvem obchodu. Tento rámec stanoví mechanismy pro dohled a prosazování, aby se ověřilo a zajistilo, že organizace rámce EU–USA pro ochranu údajů dodržují zásady a že veškeré případy nesouladu jsou řešeny. Tyto mechanismy jsou popsány v zásadách (příloha I) a závazcích přijatých Ministerstvem obchodu (příloha III), Federální obchodní komisí (příloha IV) a Ministerstvem dopravy (příloha V).

#### 2.3.1 (Opětovná) certifikace

- (48) Pro certifikaci podle rámce EU–USA pro ochranu údajů (nebo každoroční opětovnou certifikaci) jsou organizace povinny veřejně deklarovat svůj závazek dodržovat zásady, zpřístupnit své politiky ochrany soukromí a plně je uplatňovat <sup>(67)</sup>. V rámci své žádosti o (opětovnou) certifikaci musí organizace Ministerstvu obchodu předložit informace, které mimo jiné zahrnují název příslušné organizace, popis účelů, pro které bude organizace zpracovávat osobní údaje, osobní údaje, na které se certifikace bude vztahovat, a také zvolenou metodu ověřování, příslušný nezávislý odvolací mechanismus a orgán zřízený zákonem, který má pravomoc vymáhat dodržování zásad <sup>(68)</sup>.
- (49) Organizace mohou přijímat osobní údaje na základě rámce EU–USA pro ochranu údajů ode dne, kdy je Ministerstvo obchodu zařadí na seznam organizací rámce pro ochranu údajů. Aby byla zajištěna právní jistota a zabránilo se „nepravdivým tvrzením“, nesmí organizace, které se certifikují poprvé, veřejně odkazovat na své dodržování zásad dříve, než Ministerstvo obchodu rozhodne, že předložení certifikace organizace je úplné, a zařadí organizaci na seznam organizací rámce pro ochranu údajů <sup>(69)</sup>. Aby tato organizace mohla na základě rámce EU–USA pro ochranu údajů dále přijímat osobní údaje z Unie, musí každý rok svou účast v rámci opětovně certifikovat. Pokud organizace rámec EU–USA pro ochranu údajů z jakéhokoli důvodu opustí, musí odstranit všechna prohlášení, která naznačují, že se organizace nadále rámce účastní <sup>(70)</sup>.
- (50) Jak je zakotveno v závazcích stanovených v příloze III, Ministerstvo obchodu ověří, zda organizace splňují všechny požadavky na certifikaci a zda zavedly (veřejnou) politiku ochrany soukromí obsahující informace požadované podle *zásady oznamovací povinnosti* <sup>(71)</sup>. Na základě zkušeností s postupem (opětovně) certifikace v rámci štítu na ochranu soukromí bude Ministerstvo obchodu provádět řadu kontrol, mimo jiné za účelem ověření, zda politiky ochrany soukromí organizací obsahují hypertextový odkaz na správný formulář stížnosti na internetových stránkách příslušného mechanismu řešení sporů, a pokud je do žádosti o certifikaci zahrnuto několik subjektů a dceřiných společností jedné organizace, zda politiky ochrany soukromí každého z těchto subjektů splňují požadavky na certifikaci a jsou snadno dostupné subjektům údajů <sup>(72)</sup>. Ministerstvo obchodu bude kromě toho v případě potřeby provádět křížové kontroly s Federální obchodní komisí a Ministerstvem dopravy, aby ověřilo, zda organizace podléhají orgánu dohledu uvedenému v jejich žádostech o (opětovnou) certifikaci, a bude spolupracovat se subjekty pro alternativní řešení sporů, aby ověřilo, zda jsou organizace registrovány k nezávislému odvolacímu mechanismu uvedenému v jejich podáních týkajících se (opětovně) certifikace <sup>(73)</sup>.

<sup>(66)</sup> Příloha I oddíl III odst. 7.

<sup>(67)</sup> Příloha I oddíl I. odst. 2.

<sup>(68)</sup> Příloha I oddíl III odst. 6 písm. b a příloha III, viz oddíl „Ověřování požadavků na autocertifikaci“.

<sup>(69)</sup> Poznámka pod čarou č. 12 v příloze I.

<sup>(70)</sup> Příloha I oddíl III odst. 6 písm. h.

<sup>(71)</sup> Příloha I oddíl III odst. 6 písm. a poznámka pod čarou č. 12, jakož i příloha III, viz oddíl „Ověřování požadavků na autocertifikaci“.

<sup>(72)</sup> Příloha III oddíl „Ověřování požadavků na autocertifikaci“.

<sup>(73)</sup> Obdobně bude Ministerstvo obchodu spolupracovat s třetí stranou, která bude sloužit jako správce finančních prostředků vybraných prostřednictvím poplatku za panel úřadů pro ochranu osobních údajů (viz 73. bod odůvodnění), za účelem ověření, zda organizace, které si zvolí úřady pro ochranu osobních údajů jako svůj nezávislý odvolací mechanismus, zaplatily poplatek za příslušný rok. Viz příloha III oddíl „Ověřování požadavků na autocertifikaci“.

- (51) Ministerstvo obchodu bude organizace informovat, že pro dokončení (opětovné) certifikace musí vyřešit všechny problémy zjištěné během jejího přezkumu. V případě, že organizace nereaguje ve lhůtě stanovené Ministerstvem obchodu (například pokud jde o opětovnou certifikaci, očekává se, že proces bude dokončen do 45 dnů) <sup>(74)</sup> nebo jiným způsobem nedokončí svou certifikaci, bude podání považováno za zrušené. V takovém případě může jakékoli nepravdivé tvrzení ohledně účasti v rámci EU–USA pro ochranu údajů nebo jeho dodržování být předmětem donucovacího opatření ze strany Federální obchodní komise nebo Ministerstva dopravy <sup>(75)</sup>.
- (52) Pro zajištění řádného uplatňování rámce EU–USA pro ochranu údajů musí být zúčastněné strany, jako jsou subjekty údajů, vývozci údajů a vnitrostátní úřady pro ochranu údajů, schopny identifikovat organizace, které zásady přijaly. Za účelem zajištění takové transparentnosti v rámci „místa vstupu“ se Ministerstvo obchodu zavázalo vést a veřejně zpřístupnit seznam organizací, které certifikovaly přijetí zásad a podléhají pravomoci alespoň jednoho z donucovacích orgánů uvedených v přílohách IV a V tohoto rozhodnutí <sup>(76)</sup>. Ministerstvo obchodu bude tento seznam aktualizovat na základě každoročních podáních organizací týkajících se opětovné certifikace a pokaždé, když některá organizace rámec EU–USA pro ochranu údajů opustí nebo z něj bude odstraněna. Aby byla rovněž zajištěna transparentnost u „místa výstupu“, Ministerstvo obchodu povede a veřejnosti zpřístupní evidenci organizací, které byly ze seznamu odstraněny, v každém jednotlivém případě s uvedením důvodu pro toto odstranění <sup>(77)</sup>. V neposlední řadě poskytne odkaz na internetové stránky Federální obchodní komise ohledně rámce EU–USA pro ochranu údajů, kde bude uveden seznam donucovacích opatření Federální obchodní komise na základě tohoto rámce <sup>(78)</sup>.

### 2.3.2 Sledování dodržování zásad

- (53) Ministerstvo obchodu bude průběžně sledovat účinné dodržování zásad ze strany organizací rámce EU–USA pro ochranu údajů prostřednictvím různých mechanismů <sup>(79)</sup>. Zejména bude provádět „kontroly na místě“ náhodně vybraných organizací, jakož i *ad hoc* kontroly na místě konkrétních organizací, pokud budou zjištěny potenciální problémy s dodržováním zásad (např. nahlášené Ministerstvu obchodu třetími stranami), s cílem ověřit, zda i) jsou k dispozici kontaktní místa pro vyřizování stížností a žádostí subjektů údajů a zda tato kontaktní místa pohotově reagují; ii) je politika ochrany soukromí organizace snadno dostupná jak na jejích internetových stránkách, tak prostřednictvím hypertextového odkazu na internetových stránkách Ministerstva obchodu; iii) je politika ochrany soukromí organizace nadále v souladu s požadavky na certifikaci a iv) zda je pro vyřizování stížností k dispozici organizací zvolený nezávislý mechanismus řešení sporů <sup>(80)</sup>.
- (54) Pokud existují věrohodné důkazy o tom, že organizace nedodržuje své závazky vyplývající z rámce EU–USA pro ochranu údajů (včetně případů, kdy Ministerstvo obchodu obdrží stížnosti nebo organizace uspokojivě nereaguje na dotazy Ministerstva obchodu), bude Ministerstvo obchodu požadovat, aby organizace vyplnila a předložila podrobný dotazník <sup>(81)</sup>. Organizace, která na dotazník uspokojivě a včas neodpoví, bude postoupena příslušnému orgánu (Federální obchodní komisi nebo Ministerstvu dopravy) k případnému uplatnění donucovacího opatření <sup>(82)</sup>. V rámci svých činností sledování dodržování zásad štitu na ochranu soukromí Ministerstvo obchodu pravidelně

<sup>(74)</sup> Poznámka pod čarou č. 2 v příloze III.

<sup>(75)</sup> Viz příloha III oddíl „Ověřování požadavků na autocertifikaci“.

<sup>(76)</sup> Informace o správě seznamu organizací rámce pro ochranu údajů lze nalézt v příloze III (viz úvod k oddílu „Správa programu rámce pro ochranu údajů a dohled nad ním ze strany Ministerstva obchodu“) a příloze I (oddíl I odst. 3, oddíl I odst. 4, oddíl III odst. 6 písm. d a oddíl III odst. 11 písm. g).

<sup>(77)</sup> Příloha III, viz úvod k oddílu „Správa programu rámce pro ochranu údajů a dohled nad ním ze strany Ministerstva obchodu“.

<sup>(78)</sup> Viz příloha III oddíl „Uzpůsobení internetových stránek rámce pro ochranu údajů cílovým adresátům“.

<sup>(79)</sup> Viz příloha III oddíl „Provádění pravidelných úředních přezkumů dodržování zásad a hodnocení programu rámce pro ochranu údajů“.

<sup>(80)</sup> V rámci svých monitorovacích činností může Ministerstvo obchodu používat různé nástroje, mimo jiné za účelem kontroly nefunkčních odkazů na politiky ochrany soukromí nebo aktivního sledování zpráv, které poskytují věrohodné důkazy o nedodržování zásad.

<sup>(81)</sup> Viz příloha III oddíl „Provádění pravidelných úředních přezkumů dodržování zásad a hodnocení programu rámce pro ochranu údajů“.

<sup>(82)</sup> Viz příloha III oddíl „Provádění pravidelných úředních přezkumů dodržování zásad a hodnocení programu rámce pro ochranu údajů“.

provádělo kontroly na místě uvedené v 53. bodě odůvodnění a průběžně sledovalo veřejné zprávy, což mu umožnilo identifikovat, řešit a vyřešit problémy s dodržováním zásad<sup>(83)</sup>. Organizace, které soustavně nedodržují zásady, budou odstraněny ze seznamu organizací rámce pro ochranu údajů a musí vrátit nebo vymazat osobní údaje, které na základě tohoto rámce obdržely<sup>(84)</sup>.

- (55) V jiných případech odstranění, například pokud organizace dobrovolně ukončí účast v rámci nebo pokud se opětovně necertifikuje, musí organizace údaje vymazat či vrátit, nebo si je může ponechat, pokud Ministerstvo obchodu každoročně ujistí o svém závazku řídit se i nadále zásadami nebo pokud osobním údajům zajistí odpovídající ochranu jiným povoleným způsobem (např. smlouvou, která plně vyhovuje požadavkům příslušných standardních smluvních doložek schválených Komisí)<sup>(85)</sup>. V tomto případě musí organizace rovněž určit kontaktní místo uvnitř organizace pro veškeré otázky související s rámcem EU–USA pro ochranu údajů.

### 2.3.3 Identifikace a řešení nepravdivých tvrzení o účasti

- (56) Ministerstvo obchodu bude sledovat případná nepravdivá tvrzení o účasti v rámci EU–USA pro ochranu údajů nebo nesprávné použití certifikační značky rámce EU–USA pro ochranu údajů, a to jak z moci úřední, tak na základě stížností (např. přijatých od úřadů pro ochranu osobních údajů)<sup>(86)</sup>. Ministerstvo obchodu bude zejména průběžně ověřovat, zda organizace, které i) vystoupí z rámce EU–USA pro ochranu údajů, ii) nedokončí roční opětovnou certifikaci (tj. buď proces roční opětovné certifikace zahájily, ale nedokončily včas, nebo proces roční opětovné certifikace vůbec nezahájily), iii) jsou jako účastníci odstraněny, zejména pro „soustavné nedodržování předpisů“, nebo iv) nedokončí počáteční certifikaci (tj. proces počáteční certifikace zahájily, ale nedokončily včas), odstraní ze všech příslušných zveřejněných politik ochrany soukromí odkazy na rámec EU–USA pro ochranu údajů, které naznačují, že organizace se rámce aktivně účastní<sup>(87)</sup>. Ministerstvo obchodu bude rovněž provádět vyhledávání na internetu s cílem identifikovat odkazy na rámec EU–USA pro ochranu údajů v politikách ochrany soukromí organizací, mimo jiné za účelem identifikace nepravdivých tvrzení organizací, které se rámce EU–USA pro ochranu údajů nikdy neúčastnily<sup>(88)</sup>.
- (57) V případě, že Ministerstvo obchodu zjistí, že odkazy na rámec EU–USA pro ochranu údajů nebyly odstraněny nebo jsou nesprávně používány, bude organizaci informovat o možném postoupení případu Federální obchodní komisi / Ministerstvu dopravy<sup>(89)</sup>. Pokud organizace nereaguje uspokojivě, Ministerstvo obchodu předá záležitost příslušné agentuře k případnému uplatnění donucovacího opatření<sup>(90)</sup>. Jakékoli uvedení široké veřejnosti v omyl zavádějícími prohlášeními nebo postupy organizace ohledně přijetí zásad je postižitelné Federální obchodní komisí, Ministerstvem dopravy nebo jinými příslušnými donucovacími orgány USA. Uvedení Ministerstva obchodu v omyl je postižitelné podle zákona o nepravdivých tvrzeních (False Statements Act, 18 U.S.C. § 1001).

<sup>(83)</sup> Během druhého výročního přezkumu štitu na ochranu soukromí informovalo Ministerstvo obchodu, že provedlo kontroly na místě u 100 organizací a v 21 případech zaslalo dotazníky o dodržování zásad (poté byly zjištěné problémy odstraněny), viz pracovní dokument útvarů Komise SWD(2018) 497 final, s. 9. Podobně Ministerstvo obchodu během třetího výročního přezkumu štitu na ochranu soukromí informovalo, že prostřednictvím monitorování veřejných zpráv zjistilo tři incidenty a zahájilo praxi provádění kontrol na místě u 30 společností každý měsíc, což vedlo k následným opatřením s předložením dotazníků o dodržování zásad ve 28 % případů (po nichž byly zjištěné problémy okamžitě napraveny, nebo ve třech případech vyřešeny po zaslání varovného dopisu), viz pracovní dokument útvarů Komise SWD(2019) 495 final, s. 8.

<sup>(84)</sup> Příloha I oddíl III odst. 11 písm. g. K soustavnému nedodržování dochází zejména tehdy, pokud organizace odmítá vyhovět konečnému rozhodnutí jakéhokoli samoregulačního orgánu na ochranu soukromí, nezávislého subjektu pro řešení sporů nebo donucovacího orgánu.

<sup>(85)</sup> Příloha I oddíl III odst. 6 písm. f.

<sup>(86)</sup> Příloha III oddíl „Vyhledávání a řešení nepravdivých tvrzení o účasti“.

<sup>(87)</sup> *Tamtéž*.

<sup>(88)</sup> *Tamtéž*.

<sup>(89)</sup> *Tamtéž*.

<sup>(90)</sup> V rámci štitu na ochranu soukromí Ministerstvo obchodu během třetího výročního přezkumu rámce oznámilo, že zjistilo 669 případů nepravdivých tvrzení o účasti (mezi říjnem 2018 a říjnem 2019), z nichž většina byla vyřešena po varovném dopise Ministerstva obchodu, přičemž 143 případů bylo postoupeno Federální obchodní komisi (viz 62. bod odůvodnění níže). Viz pracovní dokument útvarů Komise SWD(2019) 495 final, s. 10.

### 2.3.4 Prosazování

- (58) Aby se zajistilo, že odpovídající úroveň ochrany údajů je zaručena v praxi, měl by být zřízen nezávislý dozorový úřad oprávněný monitorovat a vymáhat dodržování pravidel v oblasti ochrany údajů.
- (59) Organizace rámce EU–USA pro ochranu údajů musí podléhat pravomoci příslušných orgánů USA – Federální obchodní komise a Ministerstva dopravy –, které mají nezbytné vyšetřovací a donucovací pravomoci, aby účinně zajistily dodržování zásad <sup>(91)</sup>.
- (60) Federální obchodní komise je nezávislý orgán složený z pěti komisařů, kteří jsou jmenováni prezidentem s doporučením a souhlasem senátu <sup>(92)</sup>. Komisaři jsou jmenováni na sedmileté funkční období a mohou být odvoláni prezidentem pouze z důvodu neefektivní, zanedbání povinností nebo nesprávného výkonu funkce. Federální obchodní komise může mít nejvýše tři komisaře z téže politické strany a komisaři nesmějí po dobu svého jmenování vykonávat žádné jiné podnikání, povolání nebo zaměstnání.
- (61) Federální obchodní komise může vyšetřovat dodržování zásad, jakož i nepravdivá tvrzení o dodržování zásad nebo o účasti v rámci EU–USA pro ochranu údajů ze strany organizací, které již nejsou na seznamu organizací rámce pro ochranu údajů nebo se nikdy necertifikovaly <sup>(93)</sup>. Federální obchodní komise může prosazovat dodržování zásad správními příkazy nebo příkazy federálního soudu (včetně soudních smírů, kterých bylo dosaženo dohodou, tzv. consent orders) <sup>(94)</sup> s cílem uložit předběžné nebo trvalé soudní zákazy nebo jiná nápravná opatření a bude systematicky sledovat dodržování těchto příkazů <sup>(95)</sup>. Pokud organizace takové příkazy neplní, smí Federální obchodní komise usilovat o uložení občanskoprávních sankcí a jiných nápravných opatření, včetně těch za újmu způsobenou nezákonným jednáním. Každý soudní smír vydaný vůči organizaci rámce EU–USA pro ochranu údajů bude obsahovat ustanovení o podávání zpráv <sup>(96)</sup> a organizace budou povinny zveřejnit veškeré relevantní, rámce EU–USA pro ochranu údajů se týkající části každé hodnotící zprávy nebo zprávy o dodržování zásad předložené Federální obchodní komisi. A konečně Federální obchodní komise povede online seznam organizací, jimž byl vydán příkaz Federální obchodní komise nebo soudní příkaz v případech týkajících se rámce EU–USA pro ochranu údajů <sup>(97)</sup>.
- (62) Pokud jde o štít na ochranu soukromí, Federální obchodní komise přijala donucovací opatření přibližně ve 22 případech, a to jak v souvislosti s porušením konkrétních požadavků rámce (např. nepotvrzení Ministerstvu obchodu, že organizace pokračuje v uplatňování ochrany štítu na ochranu soukromí i poté, co rámec opustila, neověření prostřednictvím sebehodnocení nebo externího přezkumu souladu, že organizace rámec dodržuje) <sup>(98)</sup>, tak v souvislosti s nepravdivými tvrzeními o účasti v tomto rámci (např. ze strany organizací, které nedokončily kroky nezbytné k získání certifikace nebo nechaly vypršet platnost své certifikace, ale nepravdivě uvedly, že se rámce nadále účastní) <sup>(99)</sup>. 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 <sup>(100)</sup>.

<sup>(91)</sup> Organizace rámce EU–USA pro ochranu údajů musí veřejně deklarovat závazek dodržovat zásady, zpřístupnit své politiky ochrany soukromí v souladu s těmito zásadami a plně je provádět. Nedodržení těchto zásad je postižitelné podle § 5 zákona o Federální obchodní komisi, který zakazuje nekalé a klamavé praktiky při obchodování nebo nekalé a klamavé praktiky, které na obchodování dopadají (15 U.S.C. § 45), a 49 U.S.C. § 41712, který zakazuje dopravní nebo zprostředkovateli letenek, aby se v letecké dopravě nebo prodeji letecké dopravy dopouštěli nekalé nebo klamavé praktiky.

<sup>(92)</sup> 15 U.S.C. § 41.

<sup>(93)</sup> Příloha IV.

<sup>(94)</sup> Podle informací od Federální obchodní komise tato komise nemá pravomoc vykonávat kontroly na místě v oblasti ochrany soukromí. Má však pravomoc přikázat organizacím, aby předložily dokumenty a poskytlly svědecké výpovědi (viz § 20 zákona o Federální obchodní komisi) a k vymození takových příkazů v případě jejich nesplnění smí použít systém soudů.

<sup>(95)</sup> Viz příloha IV oddíl „Užívání a vydávání příkazů a sledování jejich dodržování“.

<sup>(96)</sup> Soudní příkazy nebo příkazy Federální obchodní komise mohou společněm přikazovat, aby prováděly programy na ochranu soukromí a aby Federální obchodní komisi pravidelně předkládaly zprávy o dodržování těchto programů nebo nezávislá hodnocení těchto programů vypracovaná třetími stranami.

<sup>(97)</sup> Viz příloha IV oddíl „Užívání a vydávání příkazů a sledování jejich dodržování“.

<sup>(98)</sup> Pracovní dokument útvarů Komise SWD(2019) 495 final, s. 11.

<sup>(99)</sup> Viz případy uvedené na internetových stránkách Federální obchodní komise, dostupné na adrese <https://www.ftc.gov/business-guidance/privacy-security/privacy-shield>. Viz také pracovní dokument útvarů Komise SWD(2017) 344 final, s. 17; pracovní dokument útvarů Komise SWD(2018) 497 final, s. 12 a pracovní dokument útvarů Komise SWD(2019) 495 final, s. 11.

<sup>(100)</sup> Viz např. Prepared Remarks of Chairman Joseph Simons at the Second Privacy Shield Annual Review (ftc.gov).

- (63) Obecněji řečeno, Federální obchodní komise v minulých letech přijala donucovací opatření v řadě případů týkajících se dodržování konkrétních požadavků na ochranu údajů, které jsou rovněž stanoveny podle rámce EU–USA pro ochranu údajů, např. pokud jde o zásady účelového omezení a uchovávání údajů <sup>(101)</sup>, minimalizace údajů <sup>(102)</sup>, zabezpečení údajů <sup>(103)</sup> a přesnosti údajů <sup>(104)</sup>.
- (64) Ministerstvo dopravy má výlučnou pravomoc regulovat postupy leteckých dopravců v oblasti ochrany soukromí a pravomoc sdílenou s Federální obchodní komisí nad postupy prodejců letenek v oblasti ochrany soukromí. Úředníci Ministerstva dopravy se nejprve snaží dosáhnout dohody, a pokud to není možné, mohou zahájit vykonávací řízení, jehož obsahem je i důkazní řízení před správním soudcem Ministerstva dopravy, který je oprávněn vydávat příkazy ke zdržení se konání a ukládat občanskoprávní sankce <sup>(105)</sup>. 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 vážných důvodů; jsou přidělováni k případům na základě rotace; nemohou vykonávat povinnosti, které jsou neslučitelné s jejich povinnostmi a odpovědnostmi jako soudců ve správním soudnictví; nepodléhají doзору vyšetřovacího týmu orgánu, u něhož jsou zaměstnáni (v tomto případě Ministerstva dopravy), a musí vykonávat svou rozhodovací/vykonávací funkci nestranně <sup>(106)</sup>. Ministerstvo dopravy se zavázalo sledovat příkazy k výkonu rozhodnutí a zajistit, aby příkazy vyplývající z případů rámce EU–USA pro ochranu údajů byly k dispozici na jeho internetových stránkách <sup>(107)</sup>.

## 2.4 Nápravná opatření

- (65) Aby se zajistila odpovídající ochrana a zejména vymáhání individuálních práv, měla by být subjektu údajů poskytnuta účinná správní a soudní náprava.
- (66) Rámec EU–USA pro ochranu údajů prostřednictvím *zásady odvolání, prosazování a odpovědnosti* vyžaduje, aby organizace poskytly možnost odvolání fyzickým osobám, které jsou postiženy nedodržováním zásad, a tedy možnost, aby subjekty údajů v Unii podávaly stížnosti týkající se nedodržování zásad ze strany organizací rámce EU–USA pro ochranu údajů a aby tyto stížnosti byly vyřešeny, a to v případě potřeby formou rozhodnutí poskytujícího účinnou nápravu <sup>(108)</sup>. V rámci certifikace musí organizace vyhovět požadavkům této zásady, a to tím, že zajistí účinné a snadno dostupné nezávislé odvolací mechanismy, pomocí kterých lze stížnosti fyzických osob a spory vyšetřit a promptně vyřešit, aniž by fyzické osobě vznikly náklady <sup>(109)</sup>.

<sup>(101)</sup> Viz např. příkaz Federální obchodní komise ve věci Drizly, LLC., ve kterém mimo jiné stanoví povinnost, aby společnost 1) zničila veškeré osobní údaje, které shromažďovala a které nejsou nezbytné pro poskytování výrobků nebo služeb spotřebitelům, 2) neshromažďovala nebo neuchovávala osobní údaje, pokud nejsou nezbytné pro konkrétní účely uvedené v plánu uchovávání.

<sup>(102)</sup> Viz např. příkaz Federální obchodní komise ve věci CafePress (24. března 2022), který mimo jiné stanoví povinnost minimalizovat množství shromažďovaných údajů.

<sup>(103)</sup> Viz např. donucovací opatření Federální obchodní komise ve věcech Drizly, LLC a CafePress, kde požadovala, aby příslušné společnosti zavedly specializovaný bezpečnostní program nebo konkrétní bezpečnostní opatření. Kromě toho, pokud jde o porušení zabezpečení údajů, viz také příkaz Federální obchodní komise ze dne 27. ledna 2023 ve věci Chegg, narovnání dosažené se společností Equifax v roce 2019 (<https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach>)

<sup>(104)</sup> Viz např. věc RealPage, Inc (16. října 2018), kdy Federální obchodní komise přijala donucovací opatření podle zákona o spravedlivém informování o úvěrové spolehlivosti proti společnosti prověřující nájemníky, která poskytovala majitelům nemovitostí a společnostem spravujícím nemovitosti podkladové zprávy o fyzických osobách na základě informací týkajících se historie nájmu, informací z veřejných rejstříků (včetně záznamů v rejstříku trestů a rejstříku vykazání) a informací o úvěrech, které byly použity jako kritérium při určování způsobilosti k získání bydlení. Federální obchodní komise zjistila, že společnost neprijala přiměřená opatření k zajištění přesnosti informací, které poskytovala na základě svého nástroje pro automatické rozhodování.

<sup>(105)</sup> Viz příloha V oddíl „Postupy prosazování předpisů“.

<sup>(106)</sup> Viz 5 U.S.C. § 3105, 7521 písm. a), 554 písm. d) a 556 písm. b) odst. 3.

<sup>(107)</sup> Příloha V, viz oddíl „Sledování a zveřejňování příkazů k výkonu rozhodnutí týkajících se porušování rámce EU–USA pro ochranu údajů“.

<sup>(108)</sup> Příloha I oddíl II odst. 7.

<sup>(109)</sup> Příloha I oddíl III odst. 11.

- (67) Organizace si mohou zvolit nezávislé odvolací mechanismy buď v Unii nebo ve Spojených státech. Jak je podrobněji vysvětleno v 73. bodě odůvodnění, patří sem možnost dobrovolného závazku ke spolupráci s úřady EU pro ochranu osobních údajů. Pokud organizace zpracovávají údaje v oblasti lidských zdrojů, je tento závazek spolupráce s úřady EU pro ochranu osobních údajů povinný. K dalším alternativám patří nezávislé alternativní řešení sporů nebo soukromým sektorem vyvinuté programy na ochranu soukromí, které do svých pravidel začleňují zásady. Programy na ochranu soukromí musí obsahovat účinné donucovací mechanismy v souladu s požadavky *zásady odvolání, prosazování a odpovědnosti*.
- (68) V důsledku toho poskytuje rámec EU–USA pro ochranu údajů subjektům údajů řadu možností, jak uplatnit svá práva, podávat stížnosti týkající se nedodržování zásad ze strany organizací rámce mezi EU a USA a dosáhnout vyřešení těchto stížností, a to v případě potřeby formou rozhodnutí poskytujícího účinnou nápravu. Fyzické osoby mohou stížnost předložit přímo organizaci, nezávislému subjektu pro řešení sporů určeného organizací, vnitrostátním úřadům pro ochranu osobních údajů, Ministerstvu obchodu nebo Federální obchodní komisi. V případech, kdy jejich stížnosti nebyly vyřešeny ani jedním z odvolacích či donucovacích mechanismů, mají fyzické osoby také právo využít závazného rozhodčího řízení (příloha I přílohy I tohoto rozhodnutí). Kromě rozhodčího panelu, jehož využití vyžaduje, aby předtím byly vyčerpány určité opravné prostředky, mohou fyzické osoby využít kterýkoli nebo všechny nápravné mechanismy dle vlastní volby a nejsou povinny zvolit si jeden mechanismus na úkor jiného ani postupovat podle jakési určené posloupnosti.
- (69) Za prvé, subjekty údajů z Unie mohou případy nedodržení zásad řešit přímým kontaktováním organizací rámce EU–USA pro ochranu údajů <sup>(110)</sup>. Pro usnadnění řešení musí organizace zavést účinný nápravný mechanismus. Organizace tedy musí fyzické osoby ve své politice ochrany soukromí jasně informovat o kontaktním místě uvnitř organizace nebo mimo ni, které bude vyřizovat stížnosti (včetně jakéhokoli relevantního zařízení v Unii, které může odpovídat na dotazy nebo stížnosti), jakož i o určených nezávislých subjektech pro řešení sporů (viz 70. bod odůvodnění). Po přijetí stížnosti fyzické osoby buď přímo od ní nebo prostřednictvím Ministerstva obchodu v návaznosti na postoupení úřadem pro ochranu osobních údajů musí organizace subjektu údajů z Unie odpovědět do 45 dní <sup>(111)</sup>. Organizace jsou taktéž povinny promptně odpovídat na dotazy a jiné žádosti o informace ze strany Ministerstva obchodu nebo úřadu pro ochranu osobních údajů <sup>(112)</sup> (pokud se organizace zavázala s úřadem pro ochranu osobních údajů spolupracovat) týkající se toho, zda dodržují zásady.
- (70) Za druhé, fyzické osoby mohou stížnost podat přímo u nezávislého subjektu pro řešení sporů (buď ve Spojených státech, nebo v Unii), který je organizací pověřen k tomu, aby šetřil a řešil stížnosti fyzických osob (nejsou-li zjevně nepodložené nebo bezdůvodné) a zdarma fyzickým osobám poskytoval odpovídající právní ochranu <sup>(113)</sup>. Sankce a opravné prostředky uložené takovým subjektem musí být natolik přísné, aby bylo zaručeno dodržení zásad ze strany organizací, a měly by zajistit, aby organizace účinky nedodržování zásad zvrátily nebo napravily, a v závislosti na okolnostech by měly zajistit ukončení dalšího zpracovávání dotčených osobních údajů a/nebo jejich výmaz, jakož i propagaci zjištění o nedodržení zásad <sup>(114)</sup>. Nezávislé subjekty pro řešení sporů ustanovené organizací jsou povinny na svých veřejných internetových stránkách uvádět příslušné informace týkající se rámce EU–USA pro ochranu údajů a služeb, které v jeho rámci poskytují <sup>(115)</sup>. Každý rok musí zveřejnit výroční zprávu s uvedením souhrnných statistik ohledně těchto služeb <sup>(116)</sup>.

<sup>(110)</sup> Příloha I oddíl III odst. 11 písm. d bod i).

<sup>(111)</sup> Příloha I oddíl III odst. 11 písm. d bod i).

<sup>(112)</sup> Jde o vyřizující orgán pověřený panelem úřadů pro ochranu osobních údajů stanovený v doplňkové zásadě „úloha úřadů pro ochranu osobních údajů“ (příloha I oddíl III odst. 5).

<sup>(113)</sup> Příloha I oddíl III odst. 11 písm. d.

<sup>(114)</sup> Příloha I oddíl II odst. 7 a oddíl III odst. 11 písm. e.

<sup>(115)</sup> Příloha I oddíl III odst. 11 písm. d bod ii).

<sup>(116)</sup> Výroční zpráva musí obsahovat: 1) celkový počet stížností týkajících se rámce EU–USA pro ochranu údajů přijatých během vykazovaného roku; 2) druhy přijatých stížností; 3) opatření pro zajištění kvality řešení sporů, jako je doba potřebná k vyřízení stížností, a 4) výsledky přijatých stížností, zejména počet a druh uložených opravných prostředků nebo sankcí.

- (71) V rámci svého přezkumu dodržování zásad může Ministerstvo obchodu ověřovat, zda se organizace rámce EU–USA pro ochranu údajů skutečně zaregistrovaly u nezávislých odvolacích mechanismů, u nichž jsou dle vlastního tvrzení registrovány <sup>(117)</sup>. Jak organizace, tak odpovědné nezávislé odvolací mechanismy jsou povinny promptně odpovídat na dotazy a žádosti Ministerstva obchodu o informace týkající se rámce EU–USA pro ochranu údajů. Ministerstvo obchodu bude spolupracovat s nezávislými odvolacími mechanismy, aby ověřilo, zda na svých internetových stránkách uvádějí informace o zásadách a službách, které poskytují na základě rámce EU–USA pro ochranu údajů, a zda zveřejňují výroční zprávy <sup>(118)</sup>.
- (72) V případě, že organizace nedodrží usnesení subjektu pro řešení sporů nebo samoregulačního subjektu, musí tento subjekt takové nedodržení oznámit Ministerstvu obchodu a Federální obchodní komisi (nebo jinému orgánu USA příslušnému vyšetřovat nedodržování zásad organizacemi) nebo příslušnému soudu <sup>(119)</sup>. Odmítne-li se organizace podřídit konečnému rozhodnutí vydanému jakýmkoli samoregulačním subjektem pro otázky ochrany soukromí, nezávislým subjektem pro řešení sporů nebo vládním subjektem, nebo pokud takový subjekt zjistí, že organizace nedodrжуje zásady často, může to být chápáno jako soustavné nedodržování zásad s tím výsledkem, že Ministerstvo obchodu poté, co nejprve v třicetidenní lhůtě poskytne organizaci, která nedodrжала zásady, možnost vyjádřit se, vyškrtne organizaci ze seznamu organizací rámce pro ochranu údajů <sup>(120)</sup>. Pokud po odstranění ze seznamu organizace nadále tvrdí, že je certifikována v rámci EU–USA pro ochranu údajů, postoupí Ministerstvo obchodu věc Federální obchodní komisi či jinému donucovacímu orgánu <sup>(121)</sup>.
- (73) Za třetí, fyzické osoby mohou podávat stížnosti také u vnitrostátního úřadu pro ochranu osobních údajů v Unii, který může využít svých vyšetřovacích a nápravných pravomocí podle nařízení (EU) 2016/679. Organizace jsou povinny spolupracovat s úřadem pro ochranu osobních údajů na šetření a vyřešení stížnosti, buď pokud se týká zpracování údajů v oblasti lidských zdrojů shromážděných v kontextu zaměstnaneckého vztahu, nebo pokud se příslušná organizace dobrovolně podřídila dohledu úřadů pro ochranu osobních údajů <sup>(122)</sup>. Konkrétně musí organizace odpovídat na dotazy, řídit se doporučeními úřadů pro ochranu osobních údajů, pokud jde mimo jiné o nápravné nebo odškodňující opatření, a předkládat úřadu pro ochranu osobních údajů písemná potvrzení o tom, že bylo přijato příslušné opatření <sup>(123)</sup>. V případě nedodržení doporučení úřadu pro ochranu osobních údajů předá úřad pro ochranu osobních údajů tyto případy Ministerstvu obchodu (které může organizace vyřadit ze seznamu rámce EU–USA pro ochranu údajů) nebo v případě možných donucovacích opatření Federální obchodní komisi nebo Ministerstvu dopravy (nespolupráce s úřady pro ochranu osobních údajů nebo nedodržení zásad je podle amerického práva postižitelné) <sup>(124)</sup>.
- (74) Pro usnadnění spolupráce v zájmu účinného vyřizování stížností zřídily Ministerstvo obchodu i Federální obchodní komise specializované kontaktní místo, které je odpovědné za přímý styk s úřady pro ochranu osobních údajů <sup>(125)</sup>. Tato kontaktní místa pomáhají s dotazy úřadů pro ochranu osobních údajů ohledně dodržování zásad ze strany organizací.
- (75) Doporučení poskytnuté úřady pro ochranu osobních údajů <sup>(126)</sup> se vydá poté, co byla oběma stranám sporu poskytnuta dostatečná příležitost vyjádřit stanovisko a předložit jakékoli důkazy. Panel může vydat doporučení v co nejkratší době v souladu s požadavkem na spravedlivé řízení a obecně do 60 dní po obdržení stížnosti <sup>(127)</sup>. Jestliže se organizace nepodrobí doporučení do 25 dnů od jeho doručení a zpoždění uspokojivě nevysvětlí, může panel vydat oznámení v tom smyslu, že hodlá buď věc předložit Federální obchodní komisi (či jinému příslušnému donucovacímu orgánu USA), nebo dospět k závěru, že závazek ke spolupráci byl závažným způsobem porušen. V prvním případě to může vést k postihu na základě § 5 zákona o Federální obchodní komisi (nebo jiného

<sup>(117)</sup> Příloha I oddíl „Ověřování požadavků na autocertifikaci“.

<sup>(118)</sup> Viz příloha III oddíl „Usnadnění spolupráce se subjekty pro alternativní řešení sporů, které poskytují služby související se zásadami“. Viz příloha I oddíl III odst. 11 písm. d body ii) až iii).

<sup>(119)</sup> Viz příloha I oddíl III odst. 11 písm. e.

<sup>(120)</sup> Viz příloha I oddíl III odst. 11 písm. g, zejména body ii) a iii).

<sup>(121)</sup> Viz příloha III oddíl „Vyhledávání a řešení nepravdivých tvrzení o účasti“.

<sup>(122)</sup> Příloha I oddíl II odst. 7 písm. b.

<sup>(123)</sup> Příloha I oddíl III odst. 5.

<sup>(124)</sup> Příloha I oddíl III odst. 5 písm. c bod ii).

<sup>(125)</sup> Příloha III (viz oddíl „Usnadnění spolupráce s úřady pro ochranu osobních údajů“) a příloha IV (viz oddíly „Upřednostňování a vyšetřování věcí předložených k přezkoumání“ a „Spolupráce v oblasti prosazování práva s úřady EU pro ochranu osobních údajů“).

<sup>(126)</sup> Jednací řád neformálního panelu úřadů pro ochranu osobních údajů by měly úřady pro ochranu osobních údajů sestavit podle toho, jak jsou schopny zorganizovat svou činnost a vzájemnou spolupráci.

<sup>(127)</sup> Příloha I oddíl III odst. 5 písm. c bod i).

právního předpisu) <sup>(128)</sup>. V druhém případě panel informuje Ministerstvo obchodu, které toto odmítnutí organizace podrobit se doporučení panelu úřadů pro ochranu osobních údajů posoudí jako soustavné nedodržování zásad, což povede k odstranění organizace ze seznamu organizací rámce pro ochranu údajů.

- (76) Pokud úřad pro ochranu osobních údajů, jemuž byla stížnost adresována, nepřijme žádná opatření nebo přijme nedostatečná opatření k vyřešení stížnosti, má stěžovatel možnost napadnout tato opatření (nebo jejich absenci) u vnitrostátního soudu příslušného členského státu EU.
- (77) Fyzické osoby mohou stížnosti u úřadů pro ochranu osobních údajů podávat i v případě, kdy panel úřadů pro ochranu osobních údajů nebyl organizací určen jako její subjekt pro řešení sporů. V těchto případech může úřad pro ochranu osobních údajů takové stížnosti postupovat buď Ministerstvu obchodu nebo Federální obchodní komisi. Pro usnadnění a prohloubení spolupráce ve věcech týkajících se stížností fyzických osob a nedodržování zásad ze strany organizací rámce EU–USA pro ochranu údajů zřídí Ministerstvo obchodu specializované kontaktní místo, které bude fungovat jako styčný bod a které bude pomáhat s dotazy úřadů pro ochranu osobních údajů ohledně dodržování zásad ze strany organizací <sup>(129)</sup>. Federální obchodní komise se obdobně zavázala zřídit specializované kontaktní místo <sup>(130)</sup>.
- (78) Za čtvrté, Ministerstvo obchodu se zavázalo přijímat a posuzovat stížnosti na nedodržování zásad ze strany organizace a vynaložit veškeré rozumné úsilí k jejich vyřešení <sup>(131)</sup>. K tomuto účelu poskytuje Ministerstvo obchodu úřadům pro ochranu osobních údajů zvláštní postupy pro postupování stížností specializovanému kontaktnímu místu, jejich sledování a dořešení s organizacemi <sup>(132)</sup>. Aby bylo zpracování jednotlivých stížností co nejrychlejší, kontaktní místo jedná ve věcech dodržování zásad v přímé součinnosti s příslušným úřadem pro ochranu osobních údajů a zejména jej během nejvýše 90 dní od postoupení informuje o stavu stížností <sup>(133)</sup>. To umožňuje subjektům údajů podávat stížnosti na nedodržování zásad ze strany organizací rámce EU–USA pro ochranu údajů přímo svému vnitrostátnímu úřadu pro ochranu osobních údajů a jejich předání Ministerstvu obchodu jako orgánu USA spravujícímu rámec EU–USA pro ochranu údajů.
- (79) Pokud Ministerstvo obchodu na základě vlastních ověření z moci úřední, stížností nebo jiných informací dospěje k závěru, že organizace soustavně zásady nedodržuje, může takovou organizaci odstranit ze seznamu organizací rámce pro ochranu údajů <sup>(134)</sup>. Odmítnutí podřídit se konečnému rozhodnutí vydanému jakýmkoli samoregulačním subjektem pro otázky ochrany soukromí, nezávislým subjektem pro řešení sporů nebo vládním subjektem, včetně úřadu pro ochranu osobních údajů, bude chápáno jako soustavné nedodržování zásad <sup>(135)</sup>.
- (80) Za páté, organizace rámce EU–USA pro ochranu údajů musí podléhat pravomoci orgánů USA, zejména Federální obchodní komisi <sup>(136)</sup>, které mají nezbytné vyšetřovací a donucovací pravomoci, aby účinně zajistily dodržování zásad. Federální obchodní komise prioritně řeší případy nedodržení zásad postoupené nezávislými subjekty pro řešení sporů nebo samoregulačními orgány, Ministerstvem obchodu a úřady pro ochranu osobních údajů (jednajícími z vlastní iniciativy nebo na základě stížnosti) za účelem stanovení, zda byl porušen § 5 zákona o Federální obchodní komisi <sup>(137)</sup>. Federální obchodní komise se zavázala vytvořit standardizovaný postup postupování případů, ustanovit kontaktní místo uvnitř komise pro případy postoupené úřady pro ochranu osobních údajů a sdílet informace o postupovaných případech. Kromě toho může přijímat stížnosti přímo od fyzických osob a z vlastní iniciativy provádět šetření případů souvisejících s rámcem EU–USA pro ochranu údajů, zejména jako součást svých vlastních širších šetření případů porušení soukromí.

<sup>(128)</sup> Příloha I oddíl III odst. 5 písm. c bod ii).

<sup>(129)</sup> Viz příloha III oddíl „Usnadnění spolupráce s úřady pro ochranu osobních údajů“.

<sup>(130)</sup> Viz příloha IV oddíl „Upřednostňování a vyšetřování věcí předložených k přezkoumání“ a „Spolupráce v oblasti prosazování práva s úřady EU pro ochranu osobních údajů“.

<sup>(131)</sup> Příloha III, viz např. oddíl „Usnadnění spolupráce s úřady pro ochranu osobních údajů“.

<sup>(132)</sup> Příloha I oddíl II odst. 7 písm. e a příloha III oddíl „Usnadnění spolupráce s úřady pro ochranu osobních údajů“.

<sup>(133)</sup> *Tamtéž*.

<sup>(134)</sup> Příloha I oddíl III odst. 11 písm. g.

<sup>(135)</sup> Příloha I oddíl III odst. 11 písm. g.

<sup>(136)</sup> Organizace rámce EU–USA pro ochranu údajů musí veřejně deklarovat závazek dodržovat zásady, veřejně zpřístupnit své politiky ochrany soukromí v souladu s těmito zásadami a plně je provádět. Nedodržení těchto zásad je postižitelné podle § 5 zákona o Federální obchodní komisi, který zakazuje nekalé a klamavé praktiky při obchodování nebo nekalé a klamavé praktiky, které na obchodování dopadají.

<sup>(137)</sup> Viz rovněž obdobné závazky přijaté Ministerstvem dopravy, příloha V.

- (81) Za šesté, v případě, že žádnou z ostatních dostupných možností nápravy nebyla stížnost fyzické osoby uspokojivě vyřešena, smí subjekt údajů z Unie jako nápravný mechanismus „poslední možnosti“ využít závazné rozhodčí řízení u „panelu rámce EU–USA pro ochranu údajů“<sup>(138)</sup>. Organizace musí fyzické osoby informovat o tom, že mají možnost využít závazného rozhodčího řízení, a jsou povinny reagovat, jakmile fyzická osoba tuto možnost využila zasláním oznámení dotčené organizaci<sup>(139)</sup>.
- (82) Tento panel rámce EU–USA pro ochranu údajů sestává ze skupiny nejméně deseti rozhodců jmenovaných Ministerstvem obchodu a Komisí na základě jejich nezávislosti, bezúhonnosti a zkušeností v oblasti práva USA o ochraně soukromí i v oblasti práva EU o ochraně údajů. Pro každý jednotlivý spor vyberou strany z této skupiny panel jednoho nebo tří<sup>(140)</sup> rozhodců.
- (83) Ministerstvo obchodu vybralo k řízení rozhodčích řízení Mezinárodní středisko pro řešení sporů (ICDR), mezinárodní divizi Americké arbitrážní asociace (AAA). Řízení před panelem rámce EU–USA pro ochranu údajů se bude řídit souborem dohodnutých rozhodčích pravidel a kodexem chování jmenovaných rozhodců. Internetové stránky střediska ICDR-AAA poskytují fyzickým osobám jasné a stručné informace o rozhodčím mechanismu a postupu podání rozhodčí žaloby.
- (84) Rozhodčí pravidla dohodnutá mezi Ministerstvem obchodu a Komisí doplňují rámec EU–USA pro ochranu údajů, obsahující několik prvků, jež zlepšují přístupnost tohoto mechanismu pro subjekty údajů v Unii: i) při přípravě podnětů pro panel může subjekt údajů pomáhat jeho vnitrostátní úřad pro ochranu osobních údajů; ii) přestože se řízení bude konat ve Spojených státech, mají subjekty údajů v Unii možnost se jej zúčastnit pomocí videokonferenční nebo telekonferenční služby, která jim bude poskytnuta zdarma; iii) přestože jazykem rozhodčího řízení bude zásadně angličtina, na odůvodněnou žádost bude subjekt údajů během rozhodčího jednání v zásadě a zdarma poskytnuto tlumočení; iv) a konečně poněvadž každá ze stran musí hradit odměnu svého právního zástupce, je-li jím před panelem zastupována, zřídí Ministerstvo obchodu fond financovaný z ročních příspěvků organizací rámce EU–USA pro ochranu údajů, z nějž budou hrazeny náklady rozhodčího řízení až do maximální částky, kterou stanoví orgány USA v konzultaci s Komisí<sup>(141)</sup>.
- (85) Panel rámce EU–USA pro ochranu údajů má pravomoc ukládat individuální, nepeněžitě přiměřené opatření<sup>(142)</sup>, které je nezbytné k nápravě nedodržení zásad. Panel sice ve svém rozhodování zohlední jiné opravné prostředky získané prostřednictvím jiných mechanismů rámce EU–USA pro ochranu údajů, pokud však mají fyzické osoby za to, že tyto jiné opravné prostředky jsou nepostačující, mohou využít rozhodčího řízení. To subjektům údajů z Unie umožní, aby využívali rozhodčího řízení ve všech případech, kdy opatření organizací rámce EU–USA pro ochranu údajů, nezávislých odvolacích mechanismů nebo příslušných orgánů USA (například Federální obchodní komise) nebo absence takových opatření jejich stížnost nevyřešila uspokojivým způsobem. Rozhodčího řízení nelze využít, je-li předmětný nárok vůči organizaci rámce EU–USA pro ochranu údajů ze zákona oprávněn řešit úřad pro ochranu osobních údajů, zejména v případech, kdy je organizace buď povinna spolupracovat a řídit se doporučením úřadu pro ochranu osobních údajů, pokud jde o zpracování údajů v oblasti lidských zdrojů shromážděných v souvislosti se zaměstnáváním, nebo se k tomu dobrovolně zavázala sama. Fyzické osoby mohou rozhodnutí rozhodčího řízení vykonávat prostřednictvím soudů USA v souladu s federálním zákonem o rozhodčím řízení (Federal Arbitration Act), a zajistit si tak procesní prostředek pro případ, kdy organizace nedodrží zásady ochrany údajů.

<sup>(138)</sup> Viz příloha I „Rozhodčí model“ přílohy I.

<sup>(139)</sup> Viz příloha I oddíl II odst. 1 písm. a bod xi) a oddíl II odst. 7 písm. c.

<sup>(140)</sup> Na počtu rozhodců v panelu se strany budou muset dohodnout.

<sup>(141)</sup> Příloha I přílohy I, oddíl G odst. 6.

<sup>(142)</sup> Fyzické osoby se sice v rozhodčím řízení nemohou domáhat náhrady škody, využití rozhodčího řízení ovšem nevylučuje možnost domáhat se náhrady škody u obecných soudů USA.

- (86) Za sedmé, pokud organizace poruší svůj závazek dodržovat zásady a politiku ochrany soukromí, kterou zveřejnila, jsou podle práva USA k dispozici dodatečné možnosti soudní nápravy, a to i za účelem získání náhrady škody. Fyzické osoby mohou například za určitých podmínek získat soudní nápravu (včetně náhrady škody) podle spotřebitelského práva jednotlivých států v případech podvodného uvedení v omyl, nekalého nebo klamavého jednání či praktik <sup>(143)</sup> a podle deliktního práva (zejména podle deliktů narušení soukromí <sup>(144)</sup>, přivlastnění jména nebo podoby <sup>(145)</sup> a zveřejnění soukromých skutečností <sup>(146)</sup>).
- (87) Různé výše popsané možnosti nápravy společně zajišťují, že každá stížnost týkající se nedodržování rámce EU–USA pro ochranu údajů ze strany certifikovaných organizací bude účinně posouzena a napravena.

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

- (88) Komise také posuzovala omezení a záruky, včetně dohledu a jednotlivých nápravných mechanismů dostupných v právu USA, pokud jde o shromažďování a následné používání osobních údajů předávaných správcům a zpracovatelům v USA ze strany orgánů veřejné moci USA pro účely veřejného zájmu, zejména pro účely prosazování trestního práva a národní bezpečnosti (dále jen „přístup vlády“) <sup>(147)</sup>. Při posuzování toho, zda podmínky přístupu vlády k údajům předávaným do Spojených států podle tohoto rozhodnutí splňují test „zásadní rovnocennosti“ podle čl. 45 odst. 1 nařízení (EU) 2016/679, jak je vykládán Soudním dvorem ve světle Listiny základních práv, Komise zohlednila několik kritérií.
- (89) Zejména musí být jakékoli omezení práva na ochranu osobních údajů stanoveno zákonem a samotný právní základ, který umožňuje zásah do takového práva, musí vymezovat rozsah omezení výkonu dotčeného práva <sup>(148)</sup>. Za účelem splnění požadavku přiměřenosti, podle kterého musí být výjimky z ochrany osobních údajů a její omezení činěny v mezích toho, co je v demokratické společnosti nezbytně nutné pro splnění konkrétních cílů obecného zájmu rovnocenných cílům uznaným Unií, musí nadto tento právní základ stanovit jasná a přesná pravidla pro rozsah a použití předmětných opatření a stanovit minimální požadavky, tak aby osoby, jejichž údaje byly předány, měly dostatečné záruky umožňující účinně chránit své osobní údaje proti riziku zneužití <sup>(149)</sup>. Kromě toho musí být tato

<sup>(143)</sup> Viz např. státní zákony na ochranu spotřebitele v Kalifornii (Kalifornský občanský zákoník § 1750 – § 1785 (západní) zákon o opravných prostředcích pro spotřebitele (Consumers Legal Remedies Act)); v District of Columbia (D.C. zákoník § 28-3901); na Floridě (Fla. Stat. § 501.201 – 501.213, zákon o klamavých a nekalých obchodních praktikách (Deceptive and Unfair Trade Practices Act)); v Illinois (815 Ill. Comp. Stat. 505/1 – 505/12, zákon o podvodech na spotřebitele a klamavých obchodních praktikách (Consumer Fraud and Deceptive Business Practices Act)); v Pensylvánii (73 Pa. Stat. Ann. § 201-1 – 201-9.3, (západní) zákon o nekalých obchodních praktikách a o ochraně spotřebitele (Unfair Trade Practices and Consumer Protection Law)).

<sup>(144)</sup> Tj. v případě úmyslného zásahu do soukromých záležitostí nebo zájmů jednotlivce, a to způsobem, který by byl pro osobu schopnou správného úsudku vysoce urážlivý (Restatement (2nd) of Torts, § 652(b)).

<sup>(145)</sup> Tento delikt se běžně uplatňuje v případě přivlastnění a použití jména nebo podobizny jednotlivce k reklamě podniku nebo výrobku nebo k podobnému komerčnímu účelu (viz Restatement (2nd) of Torts, § 652C).

<sup>(146)</sup> Tj. když jsou zveřejněny informace týkající se soukromého života fyzické osoby, pokud je to pro osobu schopnou správného úsudku vysoce urážlivé a tyto informace nejsou předmětem oprávněného zájmu veřejnosti (Restatement (2nd) of Torts, § 652D).

<sup>(147)</sup> To je důležité i s ohledem na oddíl I.5 přílohy I. Podle tohoto oddílu a podobně jako v nařízení GDPR může být dodržování požadavků na ochranu údajů a práv, které jsou součástí zásad ochrany soukromí, omezeno. Tato omezení však nejsou absolutní, ale lze se na ně odvolat pouze za několika podmínek, například v rozsahu nezbytném pro splnění soudního příkazu nebo splnění požadavků veřejného zájmu, prosazování práva nebo národní bezpečnosti. V této souvislosti a v zájmu jasnosti tento oddíl odkazuje také na podmínky stanovené ve výkonném dekretu č. 14086, které jsou posuzovány mimo jiné ve 127.–141. bodě odůvodnění.

<sup>(148)</sup> Viz rozsudek ve věci Schrems II, body 174–175 a citovaná judikatura. Pokud jde o přístup orgánů veřejné moci členských států, viz také věc C-623/17 Privacy International, ECLI:EU:C:2020:790, bod 65 a spojené věci C-511/18, C-512/18 a C-520/18 La Quadrature du Net a další, ECLI:EU:C:2020:791, bod 175.

<sup>(149)</sup> Viz rozsudek ve věci Schrems II, body 176 a 181, jakož i citovaná judikatura. Pokud jde o přístup orgánů veřejné moci členských států, viz také věc Privacy International, bod 68 a La Quadrature du Net a další, bod 132.

pravidla a záruky právně závazné a vymahatelné pro jednotlivce<sup>(150)</sup>. Subjektům údajů musí být zejména dána možnost využít právních prostředků před nezávislým a nestranným soudem s cílem získat přístup k osobním údajům, které se jich týkají, nebo dosáhnout opravy či výmazu těchto údajů<sup>(151)</sup>.

### 3.1 Přístup orgánů veřejné moci USA k osobním údajům a jejich použití těmito orgány pro účely prosazování trestního práva

- (90) Pokud jde o zásahy do osobních údajů předávaných na základě rámce EU–USA pro ochranu údajů pro účely prosazování trestního práva, právo Spojených států ukládá řadu omezení přístupu k osobním údajům a použití těchto údajů a stanoví v této oblasti dohledové a nápravné mechanismy, které jsou v souladu s požadavky uvedenými v 89. bodě odůvodnění tohoto rozhodnutí. Podmínky, za kterých lze takový přístup uskutečnit, a záruky týkající se využívání těchto pravomocí jsou podrobně posouzeny v následujících oddílech. V tomto ohledu vláda USA (prostřednictvím Ministerstva spravedlnosti) rovněž 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 prosazování trestního práva

- (91) K osobním údajům zpracovávaným certifikovanými organizacemi USA, které by byly předávány z Unie na základě rámce EU–USA pro ochranu údajů, mohou mít přístup pro účely prosazování trestního práva federální státní zástupci a federální vyšetřovací agenti USA na základě různých postupů, jak je podrobněji vysvětleno v 92.–99. bodě odůvodnění. Tyto postupy platí stejným způsobem při získávání informací od jakékoli organizace v USA bez ohledu na státní příslušnost nebo místo pobytu dotčených subjektů údajů<sup>(152)</sup>.
- (92) Za prvé, na žádost příslušníka federálního donucovacího orgánu nebo vládního zmocněnce může soudce vydat příkaz k prohlídce nebo zajištění (včetně elektronicky uložených informací)<sup>(153)</sup>. Takový příkaz může být vydán pouze tehdy, pokud existuje „důvodné podezření“<sup>(154)</sup>, že na místě uvedeném v příkazu budou pravděpodobně nalezeny „zajistitelné věci“ (důkazy o trestném činu, nezákonně držené věci nebo majetek určený k použití nebo použitý při spáchání trestného činu). V příkazu musí být uveden majetek nebo předmět, který má být zajištěn, a soudce, kterému musí být příkaz vrácen. Osoba, která je předmětem prohlídky nebo jejíž majetek je předmětem prohlídky, může usilovat o to, aby byly prohlášeny za neplatné důkazy získané při nezákonné prohlídce nebo z této

<sup>(150)</sup> Viz rozsudek ve věci Schrems II, body 181–182.

<sup>(151)</sup> Viz rozsudek ve věci Schrems I, bod 95 a rozsudek ve věci Schrems II, bod 194. V tomto ohledu SDEU zejména zdůraznil, že dodržování článku 47 Listiny základních práv Evropské unie, který zaručuje právo na účinnou ochranu nezávislým a nestranným soudem nebo tribunálem, „spoluplošně úroveň ochrany vyžadovanou v Unii a [jeho] dodržení musí Komise konstatovat ještě před přijetím rozhodnutí o odpovídající ochraně na základě čl. 45 odst. 1 [nařízení (EU) 2016/679]“ (rozsudek ve věci Schrems II, bod 186).

<sup>(152)</sup> Viz příloha VI. Viz například, pokud jde o zákon o odposleších (Wiretap Act), zákon o uchovávaných komunikacích (Stored Communications Act) a zákon o elektronickém registru odchozí komunikace (Pen Register Act) (podrobněji uvedený v 95.–98. bodě odůvodnění), věc *Suzlon Energy Ltd v. Microsoft Corp.*, 671 F.3d 726, 729 (9th Cir. 2011).

<sup>(153)</sup> Pravidlo 41 Federálního trestního řádu (Federal Rules of Criminal Procedure). V rozsudku z roku 2018 Nejvyšší soud potvrdil, že příkaz k prohlídce nebo výjimka z příkazu se vyžaduje rovněž pro přístup donucovacích orgánů k historickým záznamům o poloze mobilních telefonů, které poskytují ucelený přehled o pohybu uživatele, a že uživatel může mít ve vztahu k těmto informacím přiměřené očekávání soukromí (věc *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 založeného na přiměřených důvodech k domněnce, že tyto informace jsou relevantní a závažné pro probíhající trestní vyšetřování, ale vyžaduje se prokázání existence důvodného podezření při použití příkazu.

<sup>(154)</sup> Podle Nejvyššího soudu je „důvodné podezření“ „praktickým, nikoliv technickým“ standardem, který se odvolává na „faktické a praktické úvahy každodenního života, na jejichž základě jednají rozumní a obezřetní lidé [...]“ (věc *Illinois v. Gates*, 462 U.S. 213, 232 (1983)). Pokud jde o příkaz k prohlídce, důvodné podezření existuje tehdy, pokud existuje přiměřená pravděpodobnost, že prohlídka povede k nalezení důkazů o trestném činu (tamtéž).

prohlídky odvozené, pokud jsou tyto důkazy použity proti této osobě během trestního řízení<sup>(155)</sup>. Je-li držitel údajů (např. společnost) povinen zpřístupnit údaje na základě příkazu, může požadavek na zpřístupnění napadnout zejména jako nepřiměřeně zatěžující<sup>(156)</sup>.

- (93) Za druhé, v souvislosti s vyšetřováním určitých závažných trestných činů může velká porota (vyšetřovací složka soudu sestavená soudcem nebo magistrátním soudcem) vydat předvolání (subpoena)<sup>(157)</sup>, obvykle na žádost federálního státního zástupce, aby od někoho požadovala předložení nebo zpřístupnění obchodních záznamů, elektronicky uložených informací nebo jiných hmotných předmětů. Kromě toho různé zákony povolují využití správního předvolání k předložení nebo zpřístupnění obchodních záznamů, elektronicky uložených informací či jiných hmotných předmětů ve vyšetřováních týkajících se podvodů v oblasti zdravotní péče, zneužívání dětí, ochrany tajné služby, případů kontrolovaných látek a ve vyšetřováních generálního inspektora<sup>(158)</sup>. V obou případech musí být informace podstatná pro vyšetřování a předvolání nesmí být nepřiměřené z důvodu přílišné šíře, represivnosti nebo tíže břemene (a příjemce předvolání je může z těchto důvodů napadnout)<sup>(159)</sup>.
- (94) Velmi podobné podmínky se vztahují na správní předvolání vydávaná za účelem získání přístupu k údajům drženým společnostmi v USA pro občanskoprávní nebo regulační účely (z důvodu „veřejného zájmu“). Pravomoc agentur s občanskoprávními a regulačními povinnostmi vydávat taková správní předvolání musí být stanovena v zákoně. Použití správního předvolání podléhá „zkoušce přiměřenosti“, která vyžaduje, aby šetření bylo prováděno na základě legitimního účelu, informace požadované na základě předvolání byly pro tento účel relevantní, agentura již neměla informace, které požaduje na základě předvolání, a byly provedeny nezbytné administrativní kroky k vydání předvolání<sup>(160)</sup>. Judikatura Nejvyššího soudu rovněž objasnila potřebu vyvážit význam veřejného zájmu na požadovaných informacích s významem zájmů na ochranu soukromí osob a organizací<sup>(161)</sup>. Zatímco použití správního předvolání nepodléhá předchozímu soudnímu schválení, stává se předmětem soudního přezkumu v případech, že je příjemce napadne z výše uvedených důvodů, nebo pokud se vydávající agentura snaží předvolání vymáhat u soudu<sup>(162)</sup>. Kromě těchto obecných zastřešujících omezení mohou z jednotlivých zákonů vyplývat zvláštní (přísnější) požadavky<sup>(163)</sup>.

<sup>(155)</sup> Věc *Mapp v. Ohio*, 367 U.S. 643 (1961).

<sup>(156)</sup> Viz věc *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir. 1979) (soud rozhodl, že „řádný proces vyžaduje slyšení o otázce zátěže před tím, než bude telefonní společnost nucena poskytnout“ pomoc s příkazem k prohlídce) a věc *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980).

<sup>(157)</sup> Pátý dodatek Ústavy USA vyžaduje obžalobu velkou porotou pro jakýkoli „hrdelní nebo jinak obzvláště závažný trestný čin“. Velká porota se skládá ze 16 až 23 členů a rozhoduje o tom, zda existuje důvodné podezření se domnívat, že byl spáchán trestný čin. K dosažení tohoto závěru jsou velké porotě svěřeny vyšetřovací pravomoci, které jí umožňují vydávat předvolání.

<sup>(158)</sup> Viz příloha VI.

<sup>(159)</sup> Pravidlo 17 Federálního trestního řádu.

<sup>(160)</sup> Věc *Spojené státy v. Powell*, 379 U.S. 48 (1964).

<sup>(161)</sup> Věc *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186 (1946).

<sup>(162)</sup> Nejvyšší soud upřesnil, že v případě napadení správního předvolání musí soud posoudit, zda 1) se jedná o vyšetřování za zákonem povoleným účelem, 2) je předmětné předvolání v pravomoci Kongresu nařizovat a 3) „požadované dokumenty jsou pro vyšetřování podstatné“. Soud rovněž poznamenal, že žádost o správní předvolání musí být „přiměřená“, tj. musí obsahovat „přiměřenou, nikoli však nadměrnou, specifikaci dokumentů, které mají být předloženy, a to pro účely příslušného vyšetřování“, včetně „konkrétního popisu místa, které má být prohledáno, a osob nebo věcí, které mají být zajištěny“.

<sup>(163)</sup> Například zákon o právu na finanční soukromí (*Right to Financial Privacy Act*) poskytuje orgánu státní správy pravomoc získat finanční záznamy v držení finanční instituce na základě správního předvolání pouze tehdy, pokud 1) existuje důvod se domnívat, že požadované záznamy jsou podstatné pro legitimní vyšetřování v oblasti prosazování práva, a 2) kopie předvolání byla poskytnuta klientovi spolu s oznámením, v němž je s dostatečnou konkrétností uvedena povaha vyšetřování (12 U.S.C. §3405). Dalším příkladem je zákon o spravedlivém informování o úvěrové spolehlivosti (*Fair Credit Reporting Act*), který zakazuje agenturám podávajícím zprávy o spotřebitelích poskytovat zprávy o spotřebitelích v reakci na žádosti uvedené ve správním předvolání (a umožňuje jim reagovat pouze na žádosti v předvolání velkou porotou nebo soudní příkazy, 15 U.S.C. §1681 a následující). Pokud jde o přístup k informacím v rámci komunikace, platí zvláštní požadavky zákona o uchovávaných komunikacích (*Stored Communications Act*), včetně možnosti použít správní předvolání (podrobný přehled viz 96.–97. bod odůvodnění).

- (95) Za třetí, několik právních základů umožňuje orgánům pro prosazování trestního práva získat přístup ke komunikačním údajům. Soud může vydat příkaz, kterým povolí shromažďování informací v reálném čase o vytáčení, směrování, adresování a signálování, které se netýkají obsahu, ohledně telefonního čísla nebo e-mailu (prostřednictvím použití zařízení pro zaznamenávání informací o odchozí komunikaci sledovaného zařízení (pen register) nebo zařízení pro zaznamenávání informací o příchozí komunikaci sledovaného zařízení (trap and trace)), pokud zjistí, že orgán osvědčil, že informace, které budou pravděpodobně získány, jsou důležité pro probíhající trestní vyšetřování<sup>(164)</sup>. V příkazu musí být mimo jiné uvedena totožnost podezřelého, je-li známa; atributy komunikace, na kterou se vztahuje, a uvedení trestného činu, k němuž se shromažďované informace vztahují. Použití zařízení pro zaznamenávání informací o příchozí nebo odchozí komunikaci sledovaného zařízení může být povoleno na dobu nejvýše šedesáti dnů, kterou lze prodloužit pouze novým soudním příkazem.
- (96) Kromě toho lze na základě zákona o uchovávaných komunikacích získat pro účely prosazování trestního práva přístup k informacím o účastnících, provozním údajům a uchovávanému obsahu komunikací, které mají poskytovatelé internetových služeb, telefonní společnosti a další poskytovatelé služeb, kteří jsou třetí stranou<sup>(165)</sup>. Aby získaly uchovávaný obsah elektronických komunikací, musí orgány pro prosazování trestního práva zpravidla získat od soudce příkaz založený na důvodném podezření, že daný účet obsahuje důkazy o trestném činu<sup>(166)</sup>. Pro získání registračních informací, IP adres a souvisejících časových razítek a fakturačních informací o odběratelích mohou orgány pro prosazování trestního práva využít předvolání. Pro většinu ostatních uchovávaných informací netýkajících se obsahu, jako jsou hlavičky e-mailů bez předmětu, musí orgány pro prosazování trestního práva získat soudní příkaz, který bude vydán, je-li soudce přesvědčen, že existují přiměřené důvody domnívat se, že požadované informace jsou pro probíhající trestní vyšetřování relevantní a závažné.
- (97) Poskytovatelé, kteří obdrží žádosti podle zákona o uchovávaných komunikacích, mohou dobrovolně informovat zákazníka nebo účastníka, jehož informace jsou požadovány, s výjimkou případů, kdy příslušný orgán pro prosazování trestního práva získá ochranný příkaz, který takové oznámení zakazuje<sup>(167)</sup>. Takový ochranný příkaz je soudní příkaz, který požaduje, aby poskytovatel služeb elektronických komunikací nebo služeb dálkové výpočetní techniky, jemuž je určen příkaz, předvolání nebo soudní příkaz, o existenci příkazu, předvolání nebo soudního příkazu neinformoval žádnou jinou osobu, 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, zastrahování potenciálních svědků apod. Memorandum zástupce ministra spravedlnosti (které je závazné pro všechny právníky 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<sup>(168)</sup>. Memorandum rovněž stanoví, že žádosti o vydání ochranného příkazu obecně nesmí usilovat o odložení oznámení o více než jeden rok. Pokud by za výjimečných okolností mohly být nezbytné příkazy s delší dobou trvání, lze o ně žádat pouze s písemným souhlasem nadřízeného orgánu určeného ministrem spravedlnosti nebo příslušným náměstkem ministra spravedlnosti USA. Kromě toho musí státní zástupce při ukončení vyšetřování neprodleně posoudit, zda existuje důvod pro zachování případných nevyřízených ochranných příkazů, a pokud tomu tak není, ochranný příkaz ukončit a zajistit, aby o tom byl poskytovatel služeb informován<sup>(169)</sup>.

<sup>(164)</sup> 18 U.S.C. § 3123.

<sup>(165)</sup> 18 U.S.C. § 2701–2713.

<sup>(166)</sup> 18 U.S.C. § 2701(a)–(b)(1)(A). Pokud je dotčený účastník nebo zákazník informován (buď předem, nebo za určitých okolností prostřednictvím odloženého oznámení), lze informace o obsahu uložené déle než 180 dní získat také na základě správního předvolání nebo předvolání velkou porotou (18 U.S.C. § 2701(b)(1)(B)) nebo soudního příkazu (pokud existují přiměřené důvody domnívat se, že jde o informace relevantní a závažné 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. Věc *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

<sup>(167)</sup> 18 U.S.C. § 2705(b).

<sup>(168)</sup> Viz memorandum vydané zástupcem ministra spravedlnosti 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>.

<sup>(169)</sup> Memorandum zástupkyně ministra spravedlnosti Lisy Moncaové ze dne 27. května 2022 o doplňující politice týkající se žádostí o ochranné příkazy podle 18 U.S.C. § 2705(b).

- (98) Orgány pro prosazování trestního práva mohou rovněž v reálném čase zachycovat odposlech, ústní nebo elektronickou komunikaci na základě soudního příkazu, v němž soudce mimo jiné konstatuje, že existuje důvodné podezření se domnívat, že odposlech nebo elektronický odposlech přinese důkazy o federálním trestném činu nebo o místě pobytu uprchlíka, který se skrývá před trestním stíháním <sup>(170)</sup>.
- (99) Další ochranu poskytují různé politiky a pokyny Ministerstva spravedlnosti, včetně pokynů ministra spravedlnosti pro vnitrostátní operace úřadu FBI (Attorney General Guidelines for Domestic FBI Operations, AGG-DOM), které mimo jiné stanoví povinnost, aby Federální úřad pro vyšetřování (Federal Bureau of Investigation, FBI) používal co nejméně rušivé vyšetřovací metody s ohledem na dopad na soukromí a občanské svobody <sup>(171)</sup>.
- (100) Podle prohlášení vlády USA platí stejná nebo vyšší úroveň ochrany popsaná výše pro vyšetřování donucovacích orgánů na úrovni federálních států (s ohledem na vyšetřování prováděná podle zákonů států) <sup>(172)</sup>. Zejména ustanovení v ústavních zákonech, jakož i zákony a judikatura na úrovni států potvrzují výše uvedenou ochranu proti nepřiměřeným prohlídkám a zajištěním tím, že vyžadují vydání příkazu k prohlídce <sup>(173)</sup>. Podobně jako ochrana poskytovaná na federální úrovni může být příkaz k prohlídce vydán pouze na základě prokázání důvodného podezření a musí obsahovat popis místa, které má být prohledáno, a osoby nebo věci, které mají být zajištěny <sup>(174)</sup>.

<sup>(170)</sup> 18 U.S.C. § 2510–2522.

<sup>(171)</sup> Pokyny ministra spravedlnosti pro vnitrostátní operace Federálního úřadu pro vyšetřování (FBI) (září 2008), dostupné na adrese <http://www.justice.gov/archive/opa/docs/guidelines.pdf>. Další pravidla a postupy ukládající omezení vyšetřovacích činností federálních státních zástupců jsou stanoveny v příručce United States Attorneys' Manual, která je dostupná na adrese <http://www.justice.gov/usam/united-states-attorneys-manual>. K odchýlení se od těchto pokynů je třeba získat předchozí souhlas ředitele úřadu FBI, zástupce ředitele nebo výkonného náměstka ředitele jmenovaného 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 úřad FBI o této skutečnosti informovat ministerstvo spravedlnosti, které následně informuje ministra spravedlnosti a zástupce ministra spravedlnosti.

<sup>(172)</sup> Poznámka pod čarou č. 2 v příloze VI. Viz také např. *Arnold v. město Cleveland*, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993) („V oblasti individuálních práv a občanských svobod poskytuje Ústava Spojených států amerických, pokud se na státy vztahuje, spodní hranici, pod kterou rozhodnutí státních soudů nesmí klesnout“); *Cooper v. Kalifornie*, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L. Ed.2d 730 (1967) („Naše rozhodnutí se samozřejmě nedotýká pravomoci státu stanovit vyšší standardy pro prohlídky a zajištění, než požaduje federální ústava, pokud se tak rozhodne.“); *Petersen v. město Mesa*, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) („Ačkoli arizonská ústava může ukládat přísnější standardy na prohlídky a zajištění než federální ústava, arizonské soudy nemohou poskytovat menší ochranu, než jakou poskytuje čtvrtý dodatek.“).

<sup>(173)</sup> Většina států převzala ochranu vyplývající ze čtvrtého dodatku do svých ústav. Viz Ústava státu Alabama, čl. I, §5; Ústava státu Aljaška, čl. I, § 14; 1; Ústava státu Arkansas, čl. II, § 15; Ústava státu Kalifornie, čl. I, § 13; Ústava státu Colorado, čl. II, § 7; Ústava státu Connecticut, čl. I, § 7; Ústava státu Delaware, čl. I, § 6; Ústava státu Florida, čl. I, § 12; Ústava státu Georgia, čl. I, § I, odst. XIII; Ústava státu Havaj, čl. I, § 7; Ústava státu Idaho, čl. I, § 17; Ústava státu Illinois, čl. I, § 6; Ústava státu Indiana, čl. I, § 11; Ústava státu Iowa, čl. I, § 8; Ústava a listina práv státu Kansas, § 15; Ústava státu Kentucky, § 10; Ústava státu Louisiana, čl. I, § 5; Ústava státu Maine, čl. I, § 5; Ústava a deklarace práv státu Massachusetts, čl. 14; Ústava státu Michigan, čl. I, § 11; Ústava státu Minnesota, čl. I, § 10; Ústava státu Mississippi, čl. III, § 23; Ústava státu Missouri, čl. I, § 15; Ústava státu Montana, čl. II, § 11; Ústava státu Nebraska, čl. I, § 7; Ústava státu Nevada, čl. I, § 18; Ústava státu New Hampshire, bod 1, čl. 19; Ústava státu New Jersey, čl. II, § 7; Ústava státu Nové Mexiko, čl. II, § 10; Ústava státu New York, čl. I, § 12; Ústava státu Severní Dakota, čl. I, § 8; Ústava státu Ohio, čl. I, § 14; Ústava státu Oklahoma, čl. II, § 30; Ústava státu Oregon, čl. I, § 9; Ústava státu Pensylvánie, čl. I, § 8; Ústava státu Rhode Island, čl. I, § 6; Ústava státu Jižní Karolína, čl. I, § 10; Ústava státu Jižní Dakota, čl. VI, § 11; Ústava státu Tennessee, čl. I, § 7; Ústava státu Texas, čl. I, § 9; Ústava státu Utah, čl. I, § 14; Ústava státu Vermont, kapitola I, čl. 11; Ústava státu Západní Virginie, čl. III, § 6; Ústava státu Wisconsin, čl. I, § 11; Ústava státu Wyoming, čl. I, § 4. Ostatní státy (např. Maryland, Severní Karolína a Virginie) zakotvily ve svých ústavách zvláštní formulace týkající se soudních příkazů, které byly soudně interpretovány tak, že poskytují podobnou nebo vyšší ochranu než čtvrtý dodatek (viz Maryland. Deklarace práv, čl. 26; Ústava státu Severní Karolína, čl. I, § 20; Ústava státu Virginie, čl. I, § 10 a příslušná judikatura, např. rozsudek *Hamel v. stát*, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008; stát v. *Johnson*, 861 S.E.2d 474, 483 (N.C. 2021) a *Lowe v. Commonwealth*, 337 S.E.2d 273, 274 (Va. 1985)). A konečně, Arizona a Washington mají ústavní ustanovení, která chrání soukromí obecněji (Ústava státu Arizona čl. 2, § 8; Ústava státu Washington čl. I, § 7) a byla soudy vykládána tak, že poskytují větší ochranu než čtvrtý dodatek (viz např. stát v. *Bolt*, 689 P.2d 519, 523 (Ariz. 1984), stát v. *Ault*, 759 P.2d 1320, 1324 (Ariz. 1988), stát v. *Myrick*, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984), stát v. *Young*, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)).

<sup>(174)</sup> Viz např. kalifornský trestní zákoník § 1524.3 písm. b); pravidla 3.6–3.13 trestního řádu státu Alabama; oddíl 10.79.035; revidovaný zákoník státu Washington; oddíl 19.2–59 kapitoly 5 hlavy 19.2 trestního řádu státu Virginie.

## 3.1.1.2 Další použití shromážděných informací

- (101) Pokud jde o další použití údajů shromážděných federálními orgány pro prosazování trestního práva, ukládají různé zákony, pokyny a normy zvláštní záruky. S výjimkou specifických nástrojů vztahujících se na činnost úřadu FBI (pokynů AGG-DOM a operační příručky úřadu FBI pro vnitrostátní vyšetřování) se požadavky popsané v tomto oddíle obecně vztahují na další používání údajů jakýmkoli federálním orgánem, včetně údajů, k nimž se přistupuje pro občanskoprávní nebo regulační účely. To zahrnuje požadavky vyplývající z memorand / nařízení Úřadu pro řízení a rozpočet, federálního zákona o modernizaci řízení informační bezpečnosti, zákona o elektronické veřejné správě a zákona o federálních záznamech.
- (102) V souladu s pravomocí stanovenou Clinger-Cohenovým zákonem (P.L. 104–106, oddíl 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 obecně závazné pokyny, které se vztahují na všechny federální agentury (včetně donucovacích orgánů) při nakládání s informacemi umožňujícími identifikaci osob <sup>(175)</sup>. Oběžník zejména požaduje, aby všechny federální agentury „omezily vytváření, shromažďování, používání, zpracovávání, uchovávání, udržování, šíření a zveřejňování informací umožňujících identifikaci osob na ty, které jsou zákonem povolené, podstatné a přiměřeně považované za nezbytné pro řádný výkon oprávněných funkcí agentury“ <sup>(176)</sup>. 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. V obecnějším smyslu musí federální agentury zavést komplexní program ochrany soukromí, aby zajistily soulad s platnými požadavky na ochranu soukromí, vypracovat a vyhodnotit politiky ochrany soukromí a řídit rizika pro ochranu soukromí; udržovat postupy pro zjišťování, dokumentování a hlášení případů porušení ochrany soukromí; vypracovat programy zvyšování povědomí o ochraně soukromí a školení pro zaměstnance a dodavatele a zavést politiky a postupy, které zajistí, aby zaměstnanci odpovídali za dodržování požadavků a politik ochrany soukromí <sup>(177)</sup>.
- (103) Zákon o elektronické veřejné správě <sup>(178)</sup> navíc stanoví, že všechny federální agentury (včetně orgánů pro prosazování trestního práva) mají povinnost zavést takovou ochranu bezpečnosti informací, která odpovídá riziku a rozsahu škod, jež by vznikly v důsledku neoprávněného přístupu, použití, zveřejnění, narušení, změny nebo zničení; mít vedoucího pracovníka pro informace, který zajistí dodržování požadavků na bezpečnost informací, a provádět každoroční nezávislé hodnocení (např. generálním inspektorem, viz 109. bod odůvodnění) svého programu a postupů v oblasti bezpečnosti informací <sup>(179)</sup>. Podobně zákon o federálních záznamech (Federal Records Act, FRA) <sup>(180)</sup> a doplňující předpisy stanoví <sup>(181)</sup>, že informace uchovávané federálními agenturami musí podléhat bezpečnostním opatřením zajišťujícím fyzickou integritu informací a jejich ochranu před neoprávněným přístupem.
- (104) Na základě federálních zákonných pravomocí, včetně federálního zákona o modernizaci bezpečnosti informací z roku 2014, vypracovaly Úřad pro řízení a rozpočet a Národní institut pro standardy a technologie normy, které jsou pro federální agentury (včetně orgánů pro prosazování trestního práva) závazné a které dále specifikují minimální požadavky na bezpečnost informací, které musí být zavedeny, včetně kontroly přístupu, zajištění informovanosti a školení, plánování pro nepředvídané události, reakce na incidenty, nástrojů pro audit a odpovědnost, zajištění integrity systému a informací, provádění posouzení rizik v oblasti ochrany soukromí a bezpečnosti atd. <sup>(182)</sup>. Kromě toho musí všechny federální agentury (včetně orgánů pro prosazování trestního

<sup>(175)</sup> Tj. „informace, které lze použít k rozlišení nebo vysledování totožnosti fyzické osoby, a to buď samostatně, nebo v kombinaci s jinými informacemi, které jsou spojeny nebo je lze spojit s konkrétní fyzickou osobou“, viz oběžník OMB č. A-130, s. 33 (definice „informací umožňujících identifikaci osoby“).

<sup>(176)</sup> Oběžník OMB č. A-130, Řízení informací jako strategického zdroje, dodatek II, Odpovědnost za řízení informací umožňujících identifikaci osob, 81 fed. nařízení 49,689 (28. července 2016), s. 17.

<sup>(177)</sup> Dodatek II, §5 písm. a)–h).

<sup>(178)</sup> 44 U.S.C. kapitola 36.

<sup>(179)</sup> 44 U.S.C. § 3544–3545.

<sup>(180)</sup> FAC, 44 U.S.C. § 3105.

<sup>(181)</sup> 36 C.F.R. § 1228,150 a násl., 1228,228 a dodatek A.

<sup>(182)</sup> Viz např. Oběžník OMB č. A-130; NIST SP 800-53, rev. 5, Řízení bezpečnosti a ochrany soukromí pro informační systémy a organizace (10. prosince 2020) a Federální standardy pro zpracování informací Národního institutu pro standardy a technologie 200: Minimální bezpečnostní požadavky na federální informace a informační systémy.

práva) v souladu s pokyny Úřadu pro řízení a rozpočet udržovat a provádět plán pro řešení případů porušení zabezpečení údajů, a to i pokud jde o reakci na taková porušení a hodnocení rizik vzniku škody <sup>(183)</sup>.

- (105) Pokud jde o uchovávání údajů, zákon o federálních záznamech <sup>(184)</sup> stanoví, že federální agentury USA (včetně orgánů pro prosazování trestního práva) mají povinnost zavést lhůty pro uchovávání svých záznamů (po jejichž uplynutí musí být tyto záznamy zlikvidovány), které musí schválit Národní správa archivů a záznamů <sup>(185)</sup>. Délka těchto lhůt pro uchovávání je stanovena s ohledem na různé faktory, jako je typ vyšetřování, zda jsou důkazy stále relevantní pro vyšetřování atd. Pokud jde o úřad FBI, pokyny AGG-DOM stanoví, že úřad FBI musí mít takový plán uchovávání záznamů zaveden a musí mít zavedený systém, který může rychle vyhledat stav a podklady pro vyšetřování.
- (106) V neposlední řadě, oběžník OMB č. A-130 obsahuje také určité požadavky na šíření informací umožňujících identifikaci osob. Šíření a zveřejňování informací umožňujících identifikaci osob se musí v zásadě omezovat na to, co je zákonem povolené, podstatné a přiměřeně považované za nezbytné pro řádný výkon funkcí agentury <sup>(186)</sup>. Při sdílení informací umožňujících identifikaci osob s jinými subjekty státní správy musí federální agentury USA v příslušných případech 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) <sup>(187)</sup>. Pokud jde o důvody, na jejichž základě mohou být informace šířeny, pokyny AGG-DOM a operační příručka úřadu FBI pro vnitrostátní vyšetřování <sup>(188)</sup> například stanoví, že úřad FBI může mít právní povinnost tak učinit (např. na základě mezinárodní dohody) nebo smí za určitých okolností informace šířit, např. jiným americkým agenturám, pokud je zveřejnění slučitelné s účelem, pro který byly informace shromážděny, a souvisí s jejich povinnostmi; výborům Kongresu; zahraničním agenturám, pokud informace souvisí s jejich povinnostmi a šíření je v souladu se zájmy Spojených států; šíření je zejména nezbytné k ochraně bezpečnosti osob nebo majetku nebo k ochraně před trestným činem nebo ohrožením národní bezpečnosti nebo k jejich předcházení a zveřejnění je slučitelné s účelem, pro který byly informace shromážděny <sup>(189)</sup>.

### 3.1.2 Dohled

- (107) Činnost federálních orgánů pro prosazování trestního práva podléhá dohledu různých orgánů <sup>(190)</sup>. Jak je vysvětleno v 92.–99. bodě odůvodnění, ve většině případů to zahrnuje předběžný dohled soudních orgánů, které musí schválit jednotlivá opatření související se shromažďováním před jejich použitím. Kromě toho na různé fáze činnosti orgánů pro prosazování trestního práva, včetně shromažďování a zpracování osobních údajů, dohlížejí další orgány. Tyto soudní a nesoudní orgány společně zajišťují, že orgány pro prosazování trestního práva podléhají nezávislému dohledu.

<sup>(183)</sup> Memorandum 17-12, „Příprava na porušení zabezpečení informací umožňujících identifikaci osob a reakce na ně“ dostupné na adrese [https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12\\_0.pdf](https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf) a Oběžník OMB č. A-130. Například postupy při reakci na porušení zabezpečení údajů Ministerstva spravedlnosti, viz <https://www.justice.gov/file/4336/download>.

<sup>(184)</sup> FRA, 44 U.S.C. § 3101 a násl.

<sup>(185)</sup> 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 písm. c), 2906).

<sup>(186)</sup> Oběžník OMB č. A-130, oddíl 5.f.1. písm. d).

<sup>(187)</sup> Oběžník OMB č. A-130, dodatek I § 3 písm. d).

<sup>(188)</sup> Viz rovněž operační příručka úřadu FBI pro vnitrostátní vyšetřování, oddíl 14.

<sup>(189)</sup> AGG-DOM, oddíl VI, B a C; operační příručka úřadu FBI pro vnitrostátní vyšetřování, oddíl 14.

<sup>(190)</sup> Mechanismy uvedené v tomto oddíle se vztahují také na shromažďování a používání údajů federálními orgány pro občanskoprávní a regulační účely. Federální občanskoprávní a regulační agentury podléhají kontrole ze strany příslušných generálních inspektorů a dohledu ze strany Kongresu, včetně Nejvyššího kontrolního úřadu (Government Accountability Office), což je kontrolní a vyšetřovací agentura Kongresu. Pokud agentura nemá jmenovaného úředníka pro ochranu soukromí a občanských svobod – což je pozice, která se obvykle vyskytuje v agenturách, jako je Ministerstvo spravedlnosti a Ministerstvo vnitřní bezpečnosti, vzhledem k jejich povinnostem v oblasti prosazování práva a národní bezpečnosti –, spadají tyto povinnosti do kompetence vyššího úředníka agentury pro ochranu soukromí (Senior Agency Official for Privacy, SAOP). Všechny federální agentury jsou ze zákona povinny jmenovat vyššího úředníka agentury pro ochranu soukromí, který nese odpovědnost za zajištění souladu agentury se zákony o ochraně soukromí a za dohled nad souvisejícími záležitostmi. Viz např. dokument OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy (2016).

- (108) Za prvé, v rámci různých útvarů s odpovědností za prosazování trestního práva existují úředníci pro ochranu soukromí a občanských svobod <sup>(191)</sup>. V závislosti na pověřovacích aktech se konkrétní pravomoci těchto úředníků sice mohou lišit, ale většinou k nim patří dozor nad postupy, aby bylo zajištěno, že dané ministerstvo/agentura přistupuje k ochraně občanských svobod a soukromí adekvátně, že zavedlo/a odpovídající postupy pro řešení stížností fyzických osob, které mají za to, že jejich soukromí nebo občanské svobody byly porušeny. Vedoucí jednotlivých ministerstev 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 <sup>(192)</sup>. Úředníci pro ochranu soukromí a občanských svobod předkládají Kongresu pravidelné zprávy, mimo jiné o počtu a povaze stížností obdržených ministerstvem/agenturou, a shrnutí o vyřízení těchto stížností, provedených kontrolách a šetřeních a dopadu kroků podniknutých úředníkem <sup>(193)</sup>.
- (109) Za druhé, na činnost Ministerstva spravedlnosti, včetně úřadu FBI, dohlíží nezávislý generální inspektor <sup>(194)</sup>. Generální inspektoři jsou ze zákona nezávislí <sup>(195)</sup> a odpovídají za provádění nezávislých vyšetřování, auditů a inspekci programů a činností ministerstva. Mají přístup ke všem záznamům, zprávám, auditům, přezkumům, dokumentům, listinám, doporučením a dalším relevantním materiálům, v případě potřeby i prostřednictvím předvolání, a mohou vyslyšet <sup>(196)</sup>. Generální inspektoři sice vydávají nezávazná doporučení k nápravě, avšak jejich zprávy, včetně zpráv o následných krocích (nebo jejich absenci) <sup>(197)</sup> se obecně zveřejňují a předkládají Kongresu, který na tomto základě může vykonat svou funkci dohledu (viz 111. bod odůvodnění) <sup>(198)</sup>.

<sup>(191)</sup> Viz 42 U.S.C. § 2000ee-1. Patří sem například Ministerstvo spravedlnosti, Ministerstvo vnitřní bezpečnosti a úřad FBI. Na Ministerstvu vnitřní bezpečnosti je navíc hlavní úředník pro ochranu soukromí odpovědný za zachování a posílení ochrany soukromí a podporu transparentnosti v rámci ministerstva (6 U.S.C. 142, oddíl 222). Všechny systémy, technologie, formuláře a programy Ministerstva vnitřní bezpečnosti, 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, písemnostem, doporučením a dalším materiálům, které má ministerstvo k dispozici, a to v případě potřeby i na základě předvolání. Úředník pro ochranu soukromí musí každoročně podávat Kongresu zprávu o činnostech ministerstva, které mají dopad na ochranu soukromí, včetně stížností na porušení ochrany soukromí.

<sup>(192)</sup> 42 U.S.C. § 2000ee-1(d).

<sup>(193)</sup> Viz 42 U.S.C. § 2000ee-1 (f)(1)–(2). Například ze zprávy hlavního úředníka 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](https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf)).

<sup>(194)</sup> Obdobně byl zákonem o vnitřní bezpečnosti z roku 2002 zřízen Úřad generálního inspektora Ministerstva vnitřní bezpečnosti.

<sup>(195)</sup> Generální inspektoři jsou jmenováni nastálo a smí je odvolat pouze prezident, který při tom musí Kongresu písemně sdělit důvody odvolání.

<sup>(196)</sup> Viz zákon o generálních inspektorech z roku 1978, § 6.

<sup>(197)</sup> V této souvislosti viz např. přehled vypracovaný Úřadem generálního inspektora Ministerstva spravedlnosti o jeho vydaných doporučeních a rozsahu, v jakém byla provedena prostřednictvím následných opatření ministerstva a agentury, <https://oig.justice.gov/sites/default/files/reports/22-043.pdf>.

<sup>(198)</sup> Viz zákon o generálních inspektorech z roku 1978, § 4(5) a 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, inspekci, zvláštních přezkumů a vyšetřování programů a činností Ministerstva spravedlnosti. Tyto činnosti zahrnovaly 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 vyšetřování ohledně programů a postupů agentur Ministerstva spravedlnosti v oblasti bezpečnosti informací, které zahrnuje testování účinnosti politik, postupů a praktik v oblasti bezpečnosti informací u reprezentativní podskupiny systémů agentur.

- (110) Za třetí, v rozsahu, v jakém provádějí protiteroristické činnosti, podléhají útvary s odpovědností za prosazování trestního práva dohledu Výboru pro dohled nad ochranou soukromí a občanských svobod (Privacy and Civil Liberties Oversight Board, PCLOB), nezávislé agentury v rámci výkonné moci zahrnující výbor složený z pěti zástupců obou politických stran jmenovaných prezidentem se souhlasem Senátu na pevné období šesti let <sup>(199)</sup>. Podle svého zakládajícího statutu jsou výboru PCLOB svěřeny povinnosti v oblasti protiteroristické politiky a jejího provádění s ohledem na ochranu soukromí a občanských svobod. V rámci přezkumu může tento výbor přistupovat ke všem relevantním záznamům, zprávám, auditům, přezkumům, dokumentům, listinám a doporučením jednotlivých zpravodajských služeb, včetně utajovaných informací, provádět pohovory a vyslýchat svědky <sup>(200)</sup>. Výboru jsou předkládány zprávy úředníků pro otázky ochrany občanských svobod a soukromí několika federálních ministerstev či služeb <sup>(201)</sup>, přičemž výbor může vydávat doporučení orgánům státní správy a donucovacím orgánům, a naopak výbor předkládá pravidelné zprávy výborům Kongresu a prezidentovi <sup>(202)</sup>. Zprávy výboru, včetně těch, které jsou určeny Kongresu, musí být v maximální možné míře zveřejněny <sup>(203)</sup>.
- (111) V neposlední řadě podléhají činnosti v oblasti prosazování trestního práva dohledu zvláštních výborů v Kongresu USA (výbory Sněmovny reprezentantů a Senátu pro justici). Výbory pro justici provádějí pravidelný dohled různými způsoby, zejména prostřednictvím slyšení, vyšetřování, přezkumů a zpráv <sup>(204)</sup>.

### 3.1.3 Nápravná opatření

- (112) Jak již bylo uvedeno, orgány pro prosazování trestního práva musí ke shromažďování osobních údajů ve většině případů získat předchozí soudní povolení. 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 mohou taková předvolání napadnout u soudu pro jejich nepřiměřenost, tj. proto, že jsou příliš široká, represivní nebo zatěžující <sup>(205)</sup>.
- (113) Fyzické osoby mohou v první řadě podat žádost nebo stížnost orgánům pro prosazování trestního práva ohledně nakládání s jejich osobními údaji. To zahrnuje možnost požádat o přístup k osobním údajům a o jejich opravu <sup>(206)</sup>. Pokud jde o činnosti související s bojem proti terorismu, mohou fyzické osoby rovněž podat stížnost úředníkům pro ochranu soukromí a občanských svobod (nebo jiným úředníkům pro ochranu soukromí) v rámci donucovacích orgánů <sup>(207)</sup>.
- (114) Právo USA dále fyzickým osobám poskytuje několik možností soudní nápravy vůči orgánu veřejné moci nebo jeho úředníkovi v případech, kdy tyto orgány zpracovávají osobní údaje <sup>(208)</sup>. Mezi tyto možnosti patří zejména zákon o správním řízení (Administrative Procedure Act, APA), zákon o svobodě informací (Freedom of Information Act, FOIA) a zákon o soukromí elektronických komunikací (Electronic Communications Privacy Act, ECPA), které mohou využít všechny fyzické osoby bez ohledu na jejich státní příslušnost s výhradou některých platných podmínek.

<sup>(199)</sup> Členové výboru 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 výboru příslušníky stejné politické strany. Osoba jmenovaná do výboru nesmí být po dobu svého působení ve výboru voleným úředníkem, funkcionářem nebo zaměstnancem federální vlády, s výjimkou funkce člena tohoto výboru. Viz 42 U.S.C. § 2000ee (h).

<sup>(200)</sup> 42 U.S.C. § 2000ee (g).

<sup>(201)</sup> Viz 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Mezi ty patří alespoň Ministerstvo spravedlnosti, Ministerstvo obrany, Ministerstvo vnitřní bezpečnosti, plus další ministerstva, agentury či prvky výkonné moci, které výbor PCLOB označil za příslušné ke kontrole.

<sup>(202)</sup> 42 U.S.C. § 2000ee, (e).

<sup>(203)</sup> 42 U.S.C. § 2000ee (f).

<sup>(204)</sup> Výbory například pořádají tematická slyšení (viz např. nedávné slyšení výboru pro justici Sněmovny reprezentantů na téma „digitální policejní zátahy“, <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983>), jakož i pravidelná slyšení týkající se dohledu, např. úřadu FBI nebo Ministerstva spravedlnosti, 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>.

<sup>(205)</sup> Viz příloha VI.

<sup>(206)</sup> Oběžník OMB č. A-130, dodatek II, oddíl 3 písm. a) a f), který vyžaduje, aby federální agentury zajistily na žádost fyzických osob odpovídající přístup a opravu a aby stanovily postupy pro přijímání a vyřizování stížností a žádostí týkajících se ochrany soukromí.

<sup>(207)</sup> Viz 42 U.S.C. § 2000ee-1, pokud jde například o Ministerstvo spravedlnosti a Ministerstvo vnitřní bezpečnosti. Viz také memorandum OMB M-16-24, *Role and Designation of Senior Agency Officials for Privacy*.

<sup>(208)</sup> Mechanismy nápravy uvedené v tomto oddíle se vztahují také na shromažďování a používání údajů federálními orgány pro občanskoprávní a regulační účely.

- (115) Obecně podle zákona o správním řízení <sup>(209)</sup> má „kdokoli, jemuž krok agentury způsobí právní křivdu nebo kdo je krokem agentury negativně postižen nebo poškozen,“ právo domáhat se soudního přezkumu <sup>(210)</sup>. Sem spadá možnost požádat soud, „aby prohlásil za neplatné nebo zrušil krok, zjištění a závěry agentury, které byly shledány [...] aktem svévole či zvlů, zneužitím diskreční pravomoci či jinak v rozporu se zákonem“ <sup>(211)</sup>.
- (116) Konkrétněji pak hlava II zákona ECPA <sup>(212)</sup> stanoví systém zákonných práv v oblasti soukromí a jako taková upravuje přístup donucovacích orgánů k obsahu telefonních, ústních nebo elektronických komunikací uložených poskytovateli služeb, kteří jsou třetí stranou <sup>(213)</sup>. Trestně postihuje nezákonný (tj. nepovolený soudem nebo jinak nepřípustný) přístup k takovým komunikacím a dává postižené fyzické osobě možnost právní ochrany podáním občanskoprávní žaloby u federálního soudu USA na náhradu škody skutečné a na náhradu škody ve formě sankce, jakož i na vydání přiměřeného nebo deklaratorního nápravného opatření proti úředníkovi vlády, který takové nezákonné činy vědomě spáchal, nebo proti Spojeným státům.
- (117) Několik dalších zákonů dává fyzickým osobám právo žalovat orgán veřejné moci nebo úředníka USA, pokud jde o zpracování osobních údajů, například zákon o odposleších (Wiretap Act) <sup>(214)</sup>, zákon o počítačových podvodech a zneužití počítače (Computer Fraud and Abuse Act) <sup>(215)</sup>, zákon o deliktích žalobách u federálního soudu (Federal Torts Claim Act) <sup>(216)</sup>, zákon o právu na finanční soukromí (Right to Financial Privacy Act) <sup>(217)</sup> a zákon o spravedlivém informování o úvěrové spolehlivosti (Fair Credit Reporting Act) <sup>(218)</sup>.

<sup>(209)</sup> 5 U.S.C. § 702.

<sup>(210)</sup> Soudnímu přezkumu podléhá obecně jen „konečný“, nikoli „předběžný, procesní nebo zprostředkovací“ úkon agentury. Viz 5 U.S.C. § 704.

<sup>(211)</sup> 5 U.S.C. § 706(2)(A).

<sup>(212)</sup> 18 U.S.C. § 2701–2712.

<sup>(213)</sup> Zákon ECPA chrání komunikace držené dvěma definovanými třídami poskytovatelů síťových služeb, a to poskytovateli: i) služeb elektronických komunikací, např. telefonie či elektronické pošty; ii) dálkových počítačových služeb, jako jsou služby ukládání či zpracování počítačových dat.

<sup>(214)</sup> 18 U.S.C. § 2510 a násl. Podle zákona o odposleších (18 U.S.C. § 2520) může osoba, jejíž telefonní, ústní nebo elektronická komunikace je odposlouchávána, zveřejněna nebo úmyslně použita, zahájit občanskoprávní řízení pro porušení zákona o odposleších, a to za určitých okolností i proti jednotlivému vládnímu úředníkovi nebo Spojeným státům. Pokud jde o shromažďování informací netýkajících se obsahu (např. IP adresy, e-mailové adresy odesílatele/příjemce), viz také kapitola o zařízeních pro zaznamenávání informací o příchozí a odchozí komunikaci sledovaného zařízení hlavy 18 (18 U.S.C. § 3121–3127 a pro občanskoprávní řízení § 2707).

<sup>(215)</sup> 18 U.S.C. § 1030. Podle zákona o počítačových podvodech a zneužití počítače může osoba zažalovat jinou osobu, a za některých okolností i jednotlivého vládního úředníka, za záměrný nepovolený přístup (nebo překročení povoleného přístupu) za účelem získání informací od finanční instituce, z počítačového systému vlády USA nebo jiného konkrétního počítače.

<sup>(216)</sup> 28 U.S.C. § 2671 a násl. Podle zákona o deliktích žalobách u federálního soudu může osoba za určitých okolností zažalovat Spojené státy za „nedbalé nebo protiprávní jednání nebo opomenutí jakéhokoli zaměstnance vlády jednajícího v rámci své funkce nebo zaměstnání“.

<sup>(217)</sup> 12 U.S.C. § 3401 a násl. Podle zákona o právu na finanční soukromí může osoba za určitých okolností zažalovat Spojené státy za získání nebo zveřejnění chráněných finančních záznamů v rozporu se zákonem. Přístup vlády k chráněným finančním záznamům je obecně zakázán, ledaže vláda podá žádost podmíněnou zákonným předvoláním nebo příkazem k prohlídce nebo, s výhradou omezení, formální písemnou žádost, přičemž fyzická osoba, o jejíž informace se žádá, musí být o takové žádosti informována.

<sup>(218)</sup> 15 U.S.C. § 1681–1681x. Podle zákona o spravedlivém informování o úvěrové spolehlivosti může osoba zažalovat jinou osobu, která nevyhoví požadavkům (zejména nutnosti zákonného povolení) na sběr, šíření a využívání informací o úvěrové spolehlivosti spotřebitelů, nebo za určitých okolností vládní agenturu.

- (118) Podle zákona FOIA <sup>(219)</sup>, 5 U.S.C. § 552, má každá osoba právo získat přístup k záznamům federálního úřadu, a to i v případě, že obsahují její osobní údaje. Po vyčerpání správních opravných prostředků se jednotlivec může tohoto práva na přístup dovolávat u soudu, pokud tyto záznamy nejsou chráněny před zveřejněním na základě výjimky nebo zvláštní výjimky pro prosazování práva <sup>(220)</sup>. V takovém případě soud posoudí, zda se některá z výjimek uplatní nebo zda se na ni příslušný orgán veřejné moci oprávněně odvolal.

### 3.2 Přístup orgánů veřejné moci USA k údajům a použití údajů těmito orgány pro účely národní bezpečnosti

- (119) Právo Spojených států ukládá různá omezení a záruky v oblasti přístupu k osobním údajům a použití těchto údajů pro účely národní bezpečnosti a stanoví dohledové a nápravné mechanismy, které jsou v souladu s požadavky uvedenými v 89. bodě odůvodnění tohoto rozhodnutí. Podmínky, za kterých lze takový přístup uskutečnit, a záruky týkající se využívání těchto pravomocí jsou podrobně posouzeny v následujících oddílech.

#### 3.2.1 Právní základy, omezení a záruky

##### 3.2.1.1 Použitelný právní rámec

- (120) Osobní údaje předávané z Unie organizacím rámce EU–USA pro ochranu údajů mohou být shromažďovány orgány USA pro účely národní bezpečnosti na základě různých právních nástrojů za zvláštních podmínek a záruk.
- (121) Jakmile organizace nacházející se ve Spojených státech obdrží osobní údaje, mohou zpravodajské služby USA usilovat o přístup k těmto údajům pro účely národní bezpečnosti pouze na základě zákonného oprávnění, konkrétně podle zákona o dohledu nad zahraniční informační službou (Foreign Intelligence Surveillance Act, FISA) anebo zákonných ustanovení umožňujících přístup prostřednictvím tzv. National Security Letters (NSL) <sup>(221)</sup>. Zákon FISA obsahuje několik právních základů, které lze použít pro sběr (a následné zpracování) osobních údajů subjektů údajů z Unie předávaných na základě rámce EU–USA pro ochranu údajů (§ 105 zákona FISA <sup>(222)</sup>, § 302 zákona FISA <sup>(223)</sup>, § 402 zákona FISA <sup>(224)</sup>, § 501 zákona FISA <sup>(225)</sup> a § 702 zákona FISA <sup>(226)</sup>), jak je blíže popsáno ve 142.–152. bodě odůvodnění.

<sup>(219)</sup> 5 U.S.C. § 552.

<sup>(220)</sup> Tato vyloučení jsou však přesně definována. Například podle 5 U.S.C. § 552 (b)(7) jsou práva podle zákona FOIA vyloučena u „záznamů nebo informací sestavených pro účely prosazení práva, ale jen v rozsahu, kdy by předložení takových záznamů nebo informací pro účely prosazení práva A) s velkou pravděpodobností mohlo zasáhnout do donucovacího řízení, B) osobu připravilo o právo na spravedlivý proces nebo nestranné rozhodnutí soudu, C) s velkou pravděpodobností mohlo představovat bezdůvodné porušení soukromí osoby, D) s velkou pravděpodobností mohlo odhalit totožnost důvěrného zdroje, včetně státního, místního nebo cizího orgánu nebo úřadu nebo jakékoli soukromé instituce, která na důvěrném základě poskytla informaci, a pokud jde o záznam nebo informace sestavené trestním donucovacím orgánem v průběhu trestního vyšetřování nebo agenturou vykonávající zákonné zpravodajské vyšetřování v oblasti národní bezpečnosti, informace poskytnuté důvěrným zdrojem, E) odkrylo metody a postupy vyšetřování nebo stíhání, nebo odkrylo pokyny pro takové vyšetřování nebo stíhání, pokud by takové odkrytí s velkou pravděpodobností mohlo vést k riziku obejití zákona, nebo F) s velkou pravděpodobností mohlo ohrozit život nebo fyzickou bezpečnost jakékoli fyzické osoby.“ Dále „kdykoli je předložena žádost, ve které jde o přístup k záznamům[, jejichž předložení by s velkou pravděpodobností mohlo zasáhnout do donucovacího řízení], a A) vyšetřování nebo řízení se týká možného porušení trestního práva a B) je důvod domnívat se, že i) subjekt vyšetřování nebo řízení si není vědom toho, že takové vyšetřování nebo řízení probíhá, a ii) odhalení existence záznamů by s velkou pravděpodobností mohlo zasáhnout do donucovacího řízení, může agentura pouze během doby, kdy tato okolnost trvá, přistupovat k záznamům, jako by nepodléhaly požadavkům tohoto paragrafu.“ (5 U.S.C. § 552 (c)(1)).

<sup>(221)</sup> 12 U.S.C. § 3414; 15 U.S.C. § 1681u–1681v a 18 U.S.C. § 2709. Viz 153. bod odůvodnění.

<sup>(222)</sup> 50 U.S.C. § 1804, který se týká tradičního elektronického sledování fyzických osob.

<sup>(223)</sup> 50 U.S.C. § 1822, který se týká fyzických prohlídek pro účely zahraničního zpravodajství.

<sup>(224)</sup> 50 U.S.C. § 1842 s § 1841 odst. 2 a § 3127 hlavy 18, který se týká instalace zařízení pro zaznamenávání informací o příchozí a odchodní komunikaci sledovaného zařízení.

<sup>(225)</sup> 50 U.S.C. § 1861, který umožňuje úřadu FBI podat „žádost o vydání příkazu, kterým se běžnému dopravci, veřejnému ubytovacímu zařízení, fyzickému úložišti nebo půjčovně vozidel nařizuje vydat záznamy, které má v držení, pro účely vyšetřování s cílem shromáždit zahraniční zpravodajské informace nebo vyšetřování týkající se mezinárodního terorismu“.

<sup>(226)</sup> 50 U.S. kodexu § 1881a, který umožňuje složkám zpravodajské komunity USA usilovat o přístup k informacím, včetně obsahu internetové komunikace, od amerických společností, se zaměřením na určité osoby, které nejsou osobami USA a nacházejí se mimo území Spojených států, a to za součinnosti poskytovatelů elektronických komunikací uložené právními předpisy.

- (122) Zpravodajské služby USA mají rovněž možnosti shromažďovat osobní údaje mimo území Spojených států, což může zahrnovat osobní údaje předávané mezi Unii a Spojenými státy. Shromažďování údajů mimo Spojené státy se zakládá na výkonném dekretu č. 12333 (EO 12333) <sup>(227)</sup>, který vydal prezident <sup>(228)</sup>.
- (123) Shromažďování informací prostřednictvím signálového zpravodajství je formou shromažďování zpravodajských informací, která je pro toto zjištění o odpovídající ochraně nerelevantnější, neboť se týká shromažďování elektronických komunikací a údajů z informačních systémů. Takové shromažďování mohou zpravodajské služby USA provádět jak na území Spojených států (na základě zákona FISA), tak při předávání údajů do Spojených států (na základě výkonného dekretu č. 12333).
- (124) Dne 7. října 2022 vydal prezident USA výkonný dekret č. 14086 o posílení záruk pro signálové zpravodajství Spojených států, který stanovil omezení a záruky pro veškeré činnosti v oblasti signálového zpravodajství USA. Tento výkonný dekret do značné míry nahrazuje prezidentskou politickou směrnicí (Presidential Political Directive, PPD-28) <sup>(229)</sup>, posiluje podmínky, omezení a záruky, které se vztahují na všechny činnosti v oblasti signálového zpravodajství (tj. na základě zákona FISA a výkonného dekretu č. 12333) bez ohledu na to, kde se odehrávají <sup>(230)</sup>, a zavádí nový nápravný mechanismus, jehož prostřednictvím se mohou fyzické osoby těchto záruk dovolávat a vymáhat je <sup>(231)</sup> (podrobněji viz 176. až 194. bod odůvodnění). Tímto způsobem provádí v právu USA výsledek jednání, která proběhla mezi EU a USA po zrušení rozhodnutí Komise o odpovídající ochraně týkající se štitu na ochranu soukromí Soudním dvorem (viz 6. bod odůvodnění). Jedná se proto o obzvláště důležitý prvek právního rámce posuzovaného v tomto rozhodnutí.
- (125) Omezení a záruky zavedené výkonným dekretem č. 14086 doplňují omezení a záruky stanovené v § 702 zákona FISA a výkonném dekretu č. 12333. Požadavky popsané níže (v oddílech 3.2.1.2 a 3.2.1.3) musí zpravodajské služby uplatňovat při zapojení do činností v oblasti signálového zpravodajství podle § 702 zákona FISA a výkonného dekretu č. 12333, např. při výběru/určení kategorií zahraničních zpravodajských informací, které mají být získány podle § 702 zákona FISA; shromažďování informací získaných zahraniční zpravodajskou činností nebo kontrarozvědkou podle výkonného dekretu č. 12333 a při rozhodování o individuálním cíleném sběru podle § 702 zákona FISA a výkonného dekretu č. 12333.
- (126) Požadavky stanovené v tomto výkonném dekretu vydaném prezidentem jsou závazné pro celou zpravodajskou komunitu. Musí být nadále prováděny prostřednictvím politik a postupů služeb, které je promítnou do konkrétních pokynů pro každodenní činnosti. V tomto ohledu poskytuje výkonný dekret č. 14086 zpravodajským službám USA maximálně jeden rok na aktualizaci svých stávajících politik a postupů (tj. do 7. října 2023), aby je uvedly do souladu s požadavky výkonného dekretu. Tyto aktualizované politiky a postupy musí být vypracovány v konzultaci s ministrem spravedlnosti, úředníkem pro ochranu občanských svobod Úřadu ředitele národních zpravodajských služeb (Civil Liberties Protection Officer of the Director of National Intelligence, dále také jako „úředník ODNI CLPO“) a výborem PCLOB – nezávislým orgánem dohledu oprávněným přezkoumávat politiky výkonné moci
- 
- <sup>(227)</sup> EO 12333: Zpravodajské činnosti USA, Federální rejstřík sv. 40, č. 235 (8. prosince 1981 ve znění z 30. července 2008). Výkonný dekret č. 12333 obecněji definuje cíle, směry, povinnosti a odpovědnosti zpravodajské činnosti USA (včetně úlohy jednotlivých prvků zpravodajské komunity) a stanoví obecné parametry provádění zpravodajské činnosti.
- <sup>(228)</sup> Ústava USA ve svém článku II stanoví, že odpovědnost za zajištění národní bezpečnosti, včetně zejména shromažďování zahraničních zpravodajských informací, spadá do pravomoci prezidenta jako vrchního velitele ozbrojených sil.
- <sup>(229)</sup> Výkonný dekret č. 14086 nahrazuje předchozí prezidentskou směrnicí, PPD-28, s výjimkou jejího oddílu 3 a doplňující přílohy (která stanoví, že zpravodajské agentury musí každoročně přezkoumávat své priority a požadavky v oblasti signálového zpravodajství s ohledem na přínosy činností v oblasti signálového zpravodajství pro národní zájmy USA, jakož i na rizika, která tyto činnosti představují) a oddílu 6 (který obsahuje obecná ustanovení), viz memorandum o národní bezpečnosti k částečnému zrušení prezidentské politické směrnice 28, dostupné na <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/>
- <sup>(230)</sup> Viz ustanovení § 5 písm. f) výkonného dekretu č. 14086, které vysvětluje, že výkonný dekret má stejnou oblast působnosti jako směrnice PPD-28, která se podle poznámky pod čarou č. 3 vztahovala na činnosti v oblasti signálového zpravodajství prováděné za účelem shromažďování komunikací nebo informací o komunikacích, s výjimkou činností v oblasti signálového zpravodajství prováděných za účelem testování nebo vývoje schopností signálového zpravodajství.
- <sup>(231)</sup> V tomto ohledu viz např. § 5 písm. h) výkonného dekretu č. 14086, který objasňuje, že záruky ve výkonném dekretu vytvářejí právní nárok a jednotlivci je mohou vymáhat prostřednictvím nápravného mechanismu.

a jejich provádění s ohledem na ochranu soukromí a občanských svobod (viz 110. bod odůvodnění, pokud jde o úlohu a postavení výboru PCLOB) – a musí být zveřejněny <sup>(232)</sup>. Jakmile budou aktualizované politiky a postupy zavedeny, výbor PCLOB navíc provede přezkum, aby zajistil jejich soulad s výkonným dekretem. Do 180 dnů od dokončení takového přezkumu ze strany výboru PCLOB musí každá zpravodajská služba pečlivě zvážit a provést nebo jinak řešit všechna doporučení výboru PCLOB. Dne 3. července 2023 vláda USA tyto aktualizované politiky a postupy zveřejnila <sup>(233)</sup>.

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

- (127) Výkonný dekret č. 14086 stanoví řadu zastřešujících požadavků, které se vztahují na všechny činnosti v oblasti signálového zpravodajství (shromažďování, používání, šíření atd. osobních údajů).
- (128) Za prvé, základem pro tyto činnosti musí být zákon nebo povolení prezidentem a musí být prováděny v souladu s právem USA, včetně Ústavy <sup>(234)</sup>.
- (129) Za druhé, musí být zavedena vhodná ochranná opatření, která zajistí, aby soukromí a občanské svobody byly nedílnou součástí plánování takových činností <sup>(235)</sup>.
- (130) Zejména lze jakoukoli činnost v oblasti signálového zpravodajství provádět pouze „po rozhodnutí, že na základě přiměřeného posouzení všech relevantních faktorů jsou tyto činnosti nezbytné k prosazování potvrzené zpravodajské priority“ (pokud jde o pojem „potvrzená zpravodajská priorita“, viz 135. bod odůvodnění) <sup>(236)</sup>.
- (131) Tyto činnosti mohou být kromě toho prováděny pouze „v rozsahu a způsobem, který je přiměřený potvrzené zpravodajské prioritě, pro kterou byly povoleny“ <sup>(237)</sup>. 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 pobytu“ <sup>(238)</sup>.
- (132) A konečně, aby se zajistilo dodržování těchto obecných požadavků – které odrážejí zásady zákonnosti, nezbytnosti a přiměřenosti –, podléhají činnosti v oblasti signálového zpravodajství dohledu (podrobněji viz oddíl 3.2.2) <sup>(239)</sup>.
- (133) Tyto zastřešující požadavky jsou s ohledem na shromažďování informací prostřednictvím signálového zpravodajství dále odůvodněny řadou podmínek a omezení, které zajišťují, že zásahy do práv jednotlivců jsou omezeny na to, co je nezbytné a přiměřené k dosažení legitimního cíle.
- (134) Za prvé, výkonný dekret omezuje důvody, na jejichž základě lze shromažďovat informace prostřednictvím činností v oblasti signálového zpravodajství, dvěma způsoby. Na jedné straně výkonný dekret stanoví legitimní cíle, které lze sledovat shromažďováním informací prostřednictvím signálového zpravodajství, např. pochopení nebo posouzení možností, záměrů nebo činností zahraničních organizací, včetně mezinárodních teroristických organizací, které představují skutečnou nebo potenciální hrozbu pro národní bezpečnost Spojených států; ochrana před zahraničním vojenským potenciálem 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 <sup>(240)</sup>. Na druhou stranu výkonný dekret přináší výčet určitých cílů, které nesmí být nikdy sledovány prostřednictvím činností

<sup>(232)</sup> Viz ustanovení § 2(c)(iv)(C) výkonného dekretu č. 14086.

<sup>(233)</sup> <https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086>

<sup>(234)</sup> Ustanovení § 2(a)(i) výkonného dekretu č. 14086.

<sup>(235)</sup> Ustanovení § 2(a)(ii) výkonného dekretu č. 14086.

<sup>(236)</sup> Viz ustanovení § 2(a)(ii)(A) výkonného dekretu č. 14086. To vždy nevyžaduje, aby činnosti v oblasti signálového zpravodajství byly jediným prostředkem k prosazování aspektů potvrzené zpravodajské priority. Shromažďování informací prostřednictvím signálového zpravodajství lze například použít k zajištění alternativních cest k ověření (např. k potvrzení informací získaných z jiných zpravodajských zdrojů) nebo k udržení spolehlivého přístupu ke stejným informacím (ustanovení § 2(c)(i)(A) výkonného dekretu č. 14086).

<sup>(237)</sup> Ustanovení § 2(a)(ii)(B) výkonného dekretu č. 14086.

<sup>(238)</sup> Ustanovení § 2(a)(ii)(B) výkonného dekretu č. 14086.

<sup>(239)</sup> Ustanovení § 2(a)(iii) ve spojení s ustanovením § 2(d) výkonného dekretu č. 14086.

<sup>(240)</sup> Ustanovení § 2(b)(i) výkonného dekretu č. 14086. Vzhledem k omezenému seznamu legitimních cílů ve výkonném dekretu, který nezahrnuje možné budoucí hrozby, výkonný dekret umožňuje prezidentovi tento seznam aktualizovat, pokud se objeví nové požadavky na národní bezpečnost, například nové hrozby pro národní bezpečnost. Tyto aktualizace musí být v zásadě zveřejněny, pokud prezident nerozhodne, že by to samo o sobě představovalo riziko pro národní bezpečnost Spojených států (§ 2(b)(i)(B) výkonného dekretu č. 14086).

v oblasti signálového zpravodajství, např. za účelem umlčení kritiky, nesouhlasu nebo svobodného vyjadřování myšlenek či politických názorů fyzických osob nebo tisku; za účelem znevýhodnění osob na základě jejich etnického původu, rasy, pohlaví, genderové identity, sexuální orientace nebo náboženství; nebo za účelem poskytnutí konkurenční výhody společností USA <sup>(241)</sup>.

- (135) Kromě toho se zpravodajské služby nemohou opírat o legitimní cíle stanovené ve výkonném dekretu č. 14086, aby ospravedlnily shromažďování informací prostřednictvím signálového zpravodajství, ale musí je pro operativní účely dále zdůvodnit na základě konkrétnějších priorit, pro které lze informace prostřednictvím signálového 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 národních zpravodajských služeb (prostřednictvím tzv. rámce národních zpravodajských priorit) a předkládá je prezidentovi ke schválení <sup>(242)</sup>. Předtím, než ředitel navrhne prezidentovi zpravodajské priority, musí v souladu s výkonným dekretem č. 14086 získat pro každou prioritu posouzení od úředníka ODNI CLPO, zda každá priorita 1) podporuje jeden nebo více legitimních cílů uvedených ve výkonném dekretu; 2) nebyla navržena ani se nepředpokládá, že by vedla ke shromažďování informací prostřednictvím signálového zpravodajství pro zakázané cíle uvedené ve výkonném dekretu, a 3) byla stanovena po náležitém zvážení soukromí a občanských svobod všech osob bez ohledu na jejich státní příslušnost nebo místo pobytu <sup>(243)</sup>. V případě, že ředitel nesouhlasí s posouzením úředníka CLPO, musí být prezidentovi předložena obě stanoviska <sup>(244)</sup>.
- (136) Tento proces proto zejména zajišťuje, aby se hledisko ochrany soukromí zohledňovalo již v počáteční fázi, kdy se vytvářejí zpravodajské priority.
- (137) Za druhé, jakmile je zpravodajská priorita stanovena, řídí se rozhodnutí o tom, zda a v jakém rozsahu lze pro její prosazení shromažďovat informace prostřednictvím signálového zpravodajství, řadou požadavků. Tyto požadavky realizují zastrešující standardy nezbytnosti a přiměřenosti stanovené v ustanovení § 2 písm. a) výkonného dekretu.
- (138) Zejména lze shromažďovat informace prostřednictvím signálového zpravodajství pouze „na základě rozhodnutí, že podle přiměřeného posouzení všech relevantních faktorů je shromažďování nezbytné k dosažení konkrétní zpravodajské priority“ <sup>(245)</sup>. Při určování, zda je konkrétní činnost shromažďování informací prostřednictvím signálového zpravodajství nezbytná k dosažení potvrzené zpravodajské priority, musí zpravodajské agentury USA zvážit dostupnost, proveditelnost a vhodnost jiných, méně invazivních zdrojů a metod, včetně diplomatických a veřejných zdrojů <sup>(246)</sup>. Pokud jsou tyto alternativní, méně rušivé zdroje a metody k dispozici, musí být upřednostněny <sup>(247)</sup>.
- (139) Pokud je při uplatňování těchto kritérií shromažďování informací prostřednictvím signálového zpravodajství považováno za nezbytné, musí být „co nejvíce přizpůsobeno“ a nesmí „nepřiměřeně ovlivňovat soukromí a občanské svobody“ <sup>(248)</sup>. 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 řádně zohlednit všechny relevantní faktory, jako je povaha sledovaného cíle; rušivost shromažďování, včetně délky jeho trvání; pravděpodobný přínos shromažďování k dosažení sledovaného cíle; rozumně předvídatelné důsledky pro fyzické osoby a povaha a citlivost shromažďovaných údajů <sup>(249)</sup>.

<sup>(241)</sup> Ustanovení § 2(b)(iii) výkonného dekretu č. 14086.

<sup>(242)</sup> Ustanovení § 102A zákona o národní bezpečnosti a § 2(b)(iii) výkonného dekretu č. 14086.

<sup>(243)</sup> 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 § 2(b)(iii)(A)(1)–(3), viz § 4(n) výkonného dekretu č. 14086.

<sup>(244)</sup> Ustanovení § 2(b)(iii)(C) výkonného dekretu č. 14086.

<sup>(245)</sup> Ustanovení § 2(b) a (c)(i)(A) výkonného dekretu č. 14086.

<sup>(246)</sup> Ustanovení § 2(c)(i)(A) výkonného dekretu č. 14086.

<sup>(247)</sup> Ustanovení § 2(c)(i)(A) výkonného dekretu č. 14086.

<sup>(248)</sup> Ustanovení § 2(c)(i)(B) výkonného dekretu č. 14086.

<sup>(249)</sup> Ustanovení § 2(c)(i)(B) výkonného dekretu č. 14086.

- (140) Pokud jde o druh shromažďování informací prostřednictvím signálového zpravodajství, shromažďování údajů v rámci Spojených států, které je pro toto zjištění o odpovídající ochraně nejvýznamnější, neboť se týká údajů, které byly předány organizacím v USA, musí být vždy cílené, jak je podrobněji vysvětleno ve 142. až 153. bodě odůvodnění.
- (141) „Hromadné shromažďování“<sup>(250)</sup> může probíhat jen mimo území Spojených států, a to na základě výkonného dekretu č. 12333. I v tomto případě je třeba podle výkonného dekretu č. 14086 upřednostnit cílené shromažďování<sup>(251)</sup>. Naopak hromadné shromažďování je povoleno pouze v případě, že informace nezbytné k prosazení potvrzené zpravodajské priority nelze přiměřeně získat cíleným shromažďováním<sup>(252)</sup>. Pokud je nutné provádět hromadné shromažďování údajů mimo Spojené státy, použijí se zvláštní ochranná opatření podle výkonného dekretu č. 14086<sup>(253)</sup>. Za prvé musí být použity metody a technická opatření, aby se shromážděné údaje omezily pouze na ty, které jsou nezbytné k prosazení potvrzené zpravodajské priority, a zároveň aby se minimalizovalo shromažďování informací, které nejsou relevantní<sup>(254)</sup>. Za druhé, výkonný dekret omezuje použití hromadné shromážděných informací (včetně dotazování) na šest konkrétních cílů, včetně ochrany před terorismem, braní rukojmí a držení zajatců cizí vládou, organizací nebo jinou osobou nebo jejich jménem; ochrany proti zahraniční špionáži, sabotáži nebo atentátu; ochrany před hrozbami vyplývajícími z vývoje, držení nebo šíření zbraní hromadného ničení nebo souvisejících technologií a hrozeb a tak dále<sup>(255)</sup>. A konečně, jakékoliv dotazování na informace shromážděné hromadně prostřednictvím signálového zpravodajství 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 náležitě zohledňují dopad dotazování na soukromí a občanské svobody všech osob bez ohledu na jejich státní příslušnost nebo místo jejich pobytu<sup>(256)</sup>.
- (142) Kromě požadavků uvedených ve výkonném dekretu č. 14086 podléhá shromažďování údajů, které byly předány organizaci ve Spojených státech, prostřednictvím signálového zpravodajství zvláštním omezením a zárukám podle § 702 zákona FISA<sup>(257)</sup>. Ustanovení § 702 zákona FISA umožňuje shromažďování zahraničních zpravodajských informací cílením na osoby, které nejsou osobami USA a o nichž se lze důvodně domnívat, že se nacházejí mimo Spojené státy, s povinnou součinností poskytovatelů služeb elektronických komunikací z USA<sup>(258)</sup>. Aby bylo možné shromažďovat zahraniční zpravodajské informace podle § 702 zákona FISA, předkládají Ministr spravedlnosti a ředitel národních zpravodajských služeb každoročně Soudu pro uplatňování zákona FISA (FISC)
- 
- <sup>(250)</sup> Tj. shromažďování velkého množství informací prostřednictvím signálového zpravodajství, které jsou z technických nebo operativních důvodů získávány bez použití diskriminačních prvků (například bez použití konkrétních identifikátorů nebo selekčních termínů), viz § 4(b) výkonného dekretu č. 14086. Podle výkonného dekretu č. 14086 a jak je dále vysvětleno ve 141. bodě odůvodnění, hromadné shromažďování podle výkonného dekretu č. 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 nahodilý. Hromadné shromažďování je proto třeba postavit do protikladu ke shromažďování na všeobecném a nerozlišujícím základě („plošné sledování“) bez omezení a ochranných opatření.
- <sup>(251)</sup> Ustanovení § 2(c)(iii)(A) výkonného dekretu č. 14086.
- <sup>(252)</sup> Ustanovení § 2(c)(iii)(A) výkonného dekretu č. 14086.
- <sup>(253)</sup> Specifická pravidla pro hromadné shromažďování podle výkonného dekretu č. 14086 se vztahují i na cílené shromažďování informací prostřednictvím signálového zpravodajství, které dočasně využívá údaje získané bez diskriminačních prvků (např. konkrétních selekčních termínů nebo identifikátorů), tj. hromadné (což je možné pouze mimo území Spojených států). To neplatí v případě, kdy jsou takové údaje použity pouze na podporu počáteční technické fáze cíleného shromažďování informací prostřednictvím signálového zpravodajství, jsou uchovávány pouze po krátkou dobu nezbytnou k dokončení této fáze a ihned poté jsou vymazány (§ 2(c)(iii)(D) výkonného dekretu č. 14086). V tomto případě je jediným účelem počátečního shromažďování bez diskriminačních prvků umožnit cílené shromažďování informací použitím konkrétního identifikátoru nebo selekčního termínu. V takovém scénáři jsou do vládních databází vkládány pouze údaje, které odpovídají uplatnění určitého diskriminačního prvku, zatímco ostatní údaje jsou zničeny. Takové cílené shromažďování se proto stále řídí obecnými pravidly, která se vztahují na shromažďování informací prostřednictvím signálového zpravodajství, včetně § 2(a)–(b) a 2(c)(i) výkonného dekretu č. 14086.
- <sup>(254)</sup> Ustanovení § 2(c)(iii)(A) výkonného dekretu č. 14086.
- <sup>(255)</sup> Ustanovení § 2(c)(iii)(B) výkonného dekretu č. 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 (§ 2(c)(iii)(C) výkonného dekretu č. 14086). Pokud jde o dotazy na údaje shromážděné hromadně, viz § 2(c)(iii)(D) výkonného dekretu č. 14086.
- <sup>(256)</sup> Ustanovení § 2(a)(ii)(A) ve spojení s ustanovením § 2(c)(iii)(D) výkonného dekretu č. 14086. Viz též příloha VII.
- <sup>(257)</sup> 50 U.S.C. § 1881.
- <sup>(258)</sup> 50 U.S.C. § 1881a (a). Jak uvedl výbor PCLOB, sledování podle § 702 „spočívá výhradně v zaměření na konkrétní osoby[, které nejsou osobami USA], o nichž bylo učiněno individuální rozhodnutí“ (Výbor pro dohled nad ochranou soukromí a občanských svobod, zpráva o programu sledování podle § 702 zákona o dohledu nad zahraniční informační službou, 2. července 2014, zpráva podle § 702, s. 111). Viz také zpráva Úřadu pro ochranu občanských svobod Národní bezpečnostní agentury (NSA CLPO) – Provádění § 702 zákona o dohledu nad zahraniční informační službou ze strany NSA, ze dne 16. dubna 2014. Pojem „poskytovatel služeb elektronických komunikací“ je definován v 50 U.S.C. § 1881 (a)(4).

osvědčení, která určují kategorie zahraničních zpravodajských informací, jež mají být získány<sup>(259)</sup>. K osvědčením musí být přiloženy postupy cíleného výběru, minimalizační postupy a postupy dotazování, které rovněž schvaluje soud a které jsou pro zpravodajské služby USA právně závazné.

- (143) Soud pro uplatňování zákona FISA je nezávislý soud<sup>(260)</sup> zřízený federálním zákonem, proti jehož rozhodnutím se lze odvolat k Odvolacímu soudu pro uplatňování zákona FISA<sup>(261)</sup> a nakonec k Nejvyššímu soudu Spojených států<sup>(262)</sup>. Soudu pro uplatňování zákona FISA (i Odvolacímu soudu pro uplatňování zákona FISA) je nápomocen stálý panel pěti právníků a pěti odborných znalců se zkušenostmi ve věcech národní bezpečnosti i občanských svobod<sup>(263)</sup>. Z této skupiny soud jmenuje jednu osobu, která bude soudu jako *amicus curiae* nápomocna při posuzování žádosti o příkaz nebo přezkum, která podle soudu představuje nový nebo významný výklad práva, ledaže soud shledá, že takové jmenování není vhodné<sup>(264)</sup>. Tím se zejména zajistí, aby soud ve svém hodnocení řádně zohledňoval hledisko ochrany soukromí. Soud může také jmenovat fyzickou osobu nebo organizaci, aby soudu jako *amicus curiae* poskytly například odborný znalecký posudek, je-li to dle názoru soudu vhodné, nebo na návrh fyzické osoby či organizace svolit k přerušení jednání za účelem vypracování posudku (*amicus curiae* brief)<sup>(265)</sup>.
- (144) Soud pro uplatňování zákona FISA přezkoumává osvědčení a související postupy (zejména postupy cíleného výběru a minimalizace) z hlediska souladu s požadavky zákona FISA. Pokud se domnívá, že požadavky nejsou splněny, může osvědčení zcela nebo zčásti zamítnout a požádat o změnu postupů<sup>(266)</sup>. V tomto ohledu Soud pro uplatňování zákona FISA opakovaně potvrdil, že se jeho přezkum postupů podle § 702 týkajících se cíleného výběru a minimalizace neomezuje pouze na postupy, jak jsou napsány, ale zahrnuje také to, jak vláda tyto postupy provádí<sup>(267)</sup>.
- (145) Jednotlivá rozhodnutí o cíleném sběru provádí Národní bezpečnostní agentura (NSA – zpravodajská agentura odpovědná za cílený sběr podle § 702 zákona FISA) v souladu s postupy cíleného sběru schválenými Soudem pro uplatňování zákona FISA, které stanoví, že agentura NSA má povinnost na základě všech okolností posoudit, zda je pravděpodobné, že se zacílením na konkrétní osobu získá kategorie zahraničních zpravodajských informací uvedená v osvědčení<sup>(268)</sup>. Toto posouzení musí být konkrétní a založené na faktech a vycházet z analytického úsudku,

<sup>(259)</sup> 50 U.S.C. § 1881a (g).

<sup>(260)</sup> Soud pro uplatňování zákona FISA je složen ze soudců jmenovaných předsedou Nejvyššího soudu Spojených států ze soudců okrskových soudů, které předtím jmenoval prezident a schválil Senát. Soudci, kteří jsou jmenováni nastálo a mohou být odvoláni jen na základě zákonného důvodu, slouží u Soudu pro uplatňování zákona FISA v překrývajících se sedmiletých funkčních obdobích. Podle zákona FISA musí být soudci vybráni z nejméně sedmi různých soudních obvodů. Viz 50 U.S.C. § 1803 (a). Soudcům jsou nápomocni zkušení soudní právníci, kteří tvoří právnícký personál soudu a kteří připravují právní analýzy žádosti o shromažďování údajů. Viz dopis ctihodného Reggieho B. Waltona, předsedajícího soudce, Soud pro uplatňování zákona FISA USA, adresovaný ctihodnému Patricku J. Leahymu, předsedovi Výboru pro soudnictví, Senát USA (29. července 2013) (Waltonův dopis), s. 2, k dispozici na <https://fas.org/irp/news/2013/07/fisc-leahy.pdf>.

<sup>(261)</sup> Odvolací soud pro uplatňování zákona FISA je složen ze soudců jmenovaných předsedou Nejvyššího soudu Spojených států ze soudců okrskových nebo odvolacích soudů, kteří slouží v překrývajících se sedmiletých funkčních obdobích. Viz 50 U.S.C. § 1803 (b).

<sup>(262)</sup> Viz 50 U.S.C. § 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

<sup>(263)</sup> 50 U.S.C. § 1803 (i)(1),(3)(A).

<sup>(264)</sup> 50 U.S.C. § 1803 (i)(2)(A).

<sup>(265)</sup> 50 U.S.C. § 1803 (i)(2)(B).

<sup>(266)</sup> Viz např. stanovisko Soudu pro uplatňování zákona FISA ze dne 18. října 2018, dostupné na: [https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018\\_Cert\\_FISC\\_Opin\\_18Oct18.pdf](https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf), potvrzené stanoviskem Odvolacího soudu pro uplatňování zákona FISA ze dne 12. července 2019, dostupným na: [https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018\\_Cert\\_FISCSCR\\_Opinion\\_12Jul19.pdf](https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCSCR_Opinion_12Jul19.pdf)

<sup>(267)</sup> Viz např. Soud pro uplatňování zákona FISA, Memorandum, stanovisko a usnesení č. 35 (18. listopadu 2020) (schváleno ke zveřejnění dne 26. dubna 2021), (příloha D).

<sup>(268)</sup> 50 U.S.C. § 1881a(a), Postupy používané Národní bezpečnostní agenturou pro sledování osob, které nejsou osobami USA a o nichž se lze důvodně domnívat, že se nacházejí mimo Spojené státy, za účelem získání zahraničních zpravodajských informací podle § 702 zákona o dohledu nad zahraniční informační službou z roku 1978, v platném znění, z března 2018 (postupy cíleného sběru agentury NSA), dostupné na: [https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018\\_Cert\\_NSA\\_Tar\\_geting\\_27Mar18.pdf](https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Tar_geting_27Mar18.pdf), s. 1–4, dále vysvětleno ve zprávě výboru PCLOB, s. 41–42.

specializovaného odborného vzdělávání a zkušeností analytika, jakož i z povahy zahraničních zpravodajských informací, které mají být získány<sup>(269)</sup>. Cílený sběr se provádí pomocí tzv. selektorů, které identifikují konkrétní komunikační zařízení, jako je e-mailová adresa nebo telefonní číslo cíle, ale nikdy ne klíčová slova nebo jména osob<sup>(270)</sup>.

(146) Analytici Národní bezpečnostní agentury nejprve identifikují osoby, které nejsou osobami USA a které se nacházejí v zahraničí a jejichž sledování povede na základě posouzení analytiků k zahraničním zpravodajským činnostem, které jsou konkretizovány v osvědčení<sup>(271)</sup>. Jak je stanoveno v postupech cíleného sběru agentury NSA, agentura NSA může zaměřit sledování na cíl pouze tehdy, když se o tomto cíli již něco dozvěděla<sup>(272)</sup>. To může vyplývat z informací z různých zdrojů, například ze zpravodajství lidských zdrojů. 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 cílené sledování schváleno rozsáhlým přezkumným mechanismem uvnitř agentury NSA<sup>(273)</sup>, budou „zaúkolovány“ (tj. vyvinuty a použity) selektory identifikující komunikační prostředky (např. e-mailová adresa) používané cíli<sup>(274)</sup>.

(147) Agentura NSA musí zdokumentovat věcný základ pro výběr cíle<sup>(275)</sup> a v pravidelných intervalech po prvotním zacílení potvrdit, že standard zacílení je nadále plněn<sup>(276)</sup>. Jakmile přestane být standard zacílení plněn, musí být sběr ukončen<sup>(277)</sup>. Výběr každého cíle ze strany agentury NSA a záznam o každém zaznamenaném posouzení a zdůvodnění zacílení jsou každé dva měsíce přezkoumávány z hlediska souladu s postupy cíleného sběru úředníky úřadů pro dohled nad zpravodajskými službami na Ministerstvu spravedlnosti, kteří jsou povinni oznámit jakékoli porušení Soudu pro uplatňování zákona FISA a Kongresu<sup>(278)</sup>. Písemná dokumentace agentury NSA usnadňuje Soudu pro uplatňování zákona FISA dohled nad tím, zda jsou konkrétní osoby správně zacíleny podle § 702 zákona FISA, v souladu s jeho dozorovými pravomocemi popsány v 173. až 174. bodě odůvodnění<sup>(279)</sup>. A konečně, ředitel národních zpravodajských služeb je rovněž povinen každoročně informovat o celkovém počtu cílů podle § 702 zákona FISA ve veřejných výročních statistických zprávách o transparentnosti. Společnosti, které dostávají směrnice podle § 702 zákona FISA, mohou zveřejňovat souhrnné údaje (prostřednictvím zpráv o transparentnosti) o žádostech, které obdržely<sup>(280)</sup>.

<sup>(269)</sup> Postupy cíleného sběru agentury NSA, s. 4.

<sup>(270)</sup> Dokument výboru PCLOB, Zpráva podle § 702, s. 32–33, 45 s dalšími odkazy. Viz také pololetní hodnocení dodržování postupů a pokynů vydaných podle § 702 zákona o dohledu nad zahraniční informační službou, předložené ministrem spravedlnosti a ředitelem Národní zpravodajské služby, vykazované období: 1. prosinec 2016 – 31. květen 2017, s. 41 (říjen 2018), dostupné na: [https://www.dni.gov/files/icotr/18th\\_Joint\\_Assessment.pdf](https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf).

<sup>(271)</sup> Zpráva podle § 702 výboru PCLOB, s. 42–43.

<sup>(272)</sup> Postupy cíleného sběru agentury NSA, s. 2.

<sup>(273)</sup> Zpráva podle § 702 výboru PCLOB, s. 46 Agentura NSA musí například ověřovat, zda mezi cílem a selektorem existuje spojení, dále musí zdokumentovat zahraniční zpravodajské informace, které očekává, že získá, tyto informace musí být ověřeny a schváleny dvěma senior analytiky agentury NSA a celý postup musí být zaznamenán pro účely následných kontrol dodržování předpisů, které provádí úřad ODNI a Ministerstvo spravedlnosti. Viz zpráva NSA CLPO – Provádění § 702 zákona o dohledu nad zahraniční informační službou ze strany NSA, ze dne 16. dubna 2014.

<sup>(274)</sup> 50 U.S.C. § 1881a (h).

<sup>(275)</sup> Postupy cíleného sběru agentury NSA, s. 8. Viz také Zpráva podle § 702 výboru PCLOB, s. 46. Neposkytnutí písemného zdůvodnění představuje incident v oblasti dodržování dokumentace, který musí být nahlášen Soudu pro uplatňování zákona FISA a Kongresu. Viz pololetní hodnocení dodržování postupů a pokynů vydaných podle § 702 zákona o dohledu nad zahraniční informační službou, předložené ministrem spravedlnosti a ředitelem Národní zpravodajské služby, vykazované období: 1. prosince 2016 – 31. května 2017, s. 41 (říjen 2018), Zpráva Ministerstva spravedlnosti / úřadu ODNI o dodržování předpisů pro Soud pro uplatňování zákona FISA za období prosinec 2016 – květen 2017, s. A-6, dostupné na [https://www.dni.gov/files/icotr/18th\\_Joint\\_Assessment.pdf](https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf).

<sup>(276)</sup> Viz podání vlády USA k Soudu pro uplatňování zákona FISA, Shrnutí významných požadavků podle § 702, s. 2–3 (15. července 2015) a informace uvedené v příloze VII.

<sup>(277)</sup> Viz podání vlády USA k Soudu pro uplatňování zákona FISA, Shrnutí významných požadavků podle § 702, s. 2–3 (15. července 2015), které stanoví, že „[p]okud vláda později vyhodnotí, že se neočekává, že by pokračování v plnění úkolu cílového selektoru vedlo k získání zahraničních zpravodajských informací, je nutné okamžité zrušení úkolu a prodloužení může mít za následek incident, který podléhá ohlášení“. Viz rovněž informace uvedené v příloze VII.

<sup>(278)</sup> Zpráva podle § 702 výboru PCLOB, s. 70–72; pravidlo 13 písm. b) jednacího řádu Soudu USA pro uplatňování zákona FISA, dostupné na <https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf>.

<sup>(279)</sup> Viz také Zpráva Ministerstva spravedlnosti / úřadu ODNI o dodržování předpisů pro Soud pro uplatňování zákona FISA za období prosinec 2016 – květen 2017 na s. A-6.

<sup>(280)</sup> 50 U.S.C. § 1874.

- (148) Pokud jde o další právní základy pro shromažďování osobních údajů předávaných organizacím v USA, platí jiná omezení a záruky. Obecně platí, že hromadné shromažďování údajů je výslovně zakázáno na základě § 402 zákona FISA (instalace zařízení k záznamu informací o příchozí a odchozí komunikaci) a prostřednictvím National Security Letters, a místo toho je vyžadováno použití konkrétních „selekčních termínů“<sup>(281)</sup>.
- (149) K provádění tradičního elektronického sledování fyzických osob (podle § 105 zákona FISA) musí zpravodajské služby Soudu pro uplatňování zákona FISA předložit žádost s uvedením skutečností a okolností, které odůvodňují domněnku, že existuje důvodné podezření, že zařízení je využíváno nebo má být využito cizí mocí nebo agentem cizí moci<sup>(282)</sup>. Soud pro uplatňování zákona FISA mimo jiné posoudí, zda na základě předložených skutečností existuje důvodné podezření, že tomu tak opravdu je<sup>(283)</sup>.
- (150) K provedení prohlídky prostor nebo majetku, která má vyústit v kontrolu, zajištění atd. informací, materiálů nebo majetku (např. počítačového zařízení) na základě § 301 zákona FISA, je nutná žádost o vydání příkazu Soudem pro uplatňování zákona FISA<sup>(284)</sup>. Taková žádost musí mimo jiné prokázat, že existuje důvodné podezření, že cílem prohlídky je cizí moc nebo agent cizí moci; že prostor nebo majetek, které mají být prohledány, obsahuje zahraniční zpravodajské informace a že prostor, který má být prohledán, je ve vlastnictví, užívání, držení (agenta) cizí moci nebo je cizí moci/cizí mocí či agentovi/agentem cizí moci předáván<sup>(285)</sup>.
- (151) Stejně tak instalace zařízení pro zaznamenávání informací o příchozí a odchozí komunikaci (podle § 402 zákona FISA) vyžaduje, aby u Soudu pro uplatňování zákona FISA (nebo u magistrátního soudce USA) byla podána žádost o příkaz a aby byl použit specifický selekční termín, tzn. termín, který konkrétně identifikuje osobu, účet atd. a který má v co největší přijatelné míře omezit záběr vyhledávaných informací<sup>(286)</sup>. Tato pravomoc se netýká obsahu komunikací, nýbrž je zaměřena na informace o zákazníkovi či účastníkovi, který službu používá (např. jméno, adresa, účastnické číslo, délka/druh poskytované služby, zdroj/způsob úhrady).
- (152) Ustanovení § 501 zákona FISA<sup>(287)</sup>, které umožňuje shromažďování obchodních záznamů veřejného 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)<sup>(288)</sup>, rovněž vyžaduje podání žádosti u Soudu pro uplatňování zákona FISA nebo u magistrátního soudce. V této žádosti musí být uvedeny požadované záznamy a konkrétní a vypovídající skutečnosti, které zakládají důvod se domnívat, že osoba, již se záznamy týkají, je cizí mocí nebo agentem cizí moci<sup>(289)</sup>.
- (153) Konečně, National Security Letters 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, elektronickém odběru a transakčních záznamech<sup>(290)</sup>. Zákon o National Security Letters, který povoluje přístup k elektronické komunikaci, může používat pouze úřad FBI a stanoví, že žádosti musí obsahovat termín, který konkrétně identifikuje osobu, subjekt, telefonní číslo nebo účet, a potvrzení, že informace jsou relevantní pro povolené vyšetřování v oblasti národní bezpečnosti za účelem ochrany před mezinárodním terorismem nebo nezákonnými zpravodajskými činnostmi<sup>(291)</sup>. Příjemci National Security Letters mají právo napadnout je u soudu<sup>(292)</sup>.

<sup>(281)</sup> 50 U.S.C. § 1842(c)(3), a pokud jde o National Security Letters, 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).

<sup>(282)</sup> Pojem „agent cizí moci“ může zahrnovat osoby, které nejsou osobami USA a které jsou zapojeny do mezinárodního terorismu nebo mezinárodního šíření zbraní hromadného ničení (včetně přípravných kroků) (50 U.S.C. § 1801 (b)(1)).

<sup>(283)</sup> 50 U.S.C. § 1804. Viz také § 1841 odst. 4, pokud jde o volbu selekčních termínů.

<sup>(284)</sup> 50 U.S.C. § 1821(5).

<sup>(285)</sup> 50 U.S.C. § 1823(a).

<sup>(286)</sup> 50 U.S.C. § 1842 ve spojení s § 1841(2) a § 3127 hlavy 18.

<sup>(287)</sup> 50 U.S.C. § 1862.

<sup>(288)</sup> 50 U.S.C. § 1861–1862.

<sup>(289)</sup> 50 U.S.C. § 1862(b).

<sup>(290)</sup> 12 U.S.C. § 3414; 15 U.S.C. § 1681u–1681v a 18 U.S.C. § 2709.

<sup>(291)</sup> 18 U.S.C. § 2709(b).

<sup>(292)</sup> Např. 18 U.S.C. § 2709(d).

### 3.2.1.3 Další použití shromážděných informací

- (154) Zpracování osobních údajů shromážděných zpravodajskými službami USA prostřednictvím signálového zpravodajství podléhá řadě záruk.
- (155) 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 zabezpečení informací, které musí být zavedeny (např. vícefaktorové ověřování, šifrování atd.)<sup>(293)</sup>. Přístup ke shromážděným údajům musí být omezen na oprávněné, vyškolené pracovníky, pro které je znalost informací nezbytná pro plnění jejich úkolů<sup>(294)</sup>. V obecnějším smyslu musí zpravodajské služby svým zaměstnancům poskytnout odpovídající školení, včetně školení v oblasti postupů pro podávání zpráv a řešení porušení zákona (včetně výkonného dekretu č. 14086)<sup>(295)</sup>.
- (156) Za druhé, zpravodajské služby 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<sup>(296)</sup>.
- (157) Za třetí, pokud jde o uchovávání údajů, výkonný dekret č. 14086 objasňuje, že osobní údaje osob, které nejsou osobami USA, podléhají stejným lhůtám uchovávání jako údaje osob USA<sup>(297)</sup>. Zpravodajské služby musí definovat konkrétní lhůty uchovávání a/nebo faktory, které je třeba vzít v úvahu při určování délky použitelných lhůt uchovávání (např. zda jsou informace důkazem trestného činu; zda informace představují zahraniční zpravodajské informace; zda jsou informace potřebné k ochraně bezpečnosti osob nebo organizací, včetně obětí nebo cílů mezinárodního terorismu), které jsou stanoveny v různých právních nástrojích<sup>(298)</sup>.
- (158) Za čtvrté, pokud jde o šíření osobních údajů shromážděných prostřednictvím signálového zpravodajství, platí zvláštní pravidla. Obecně platí, že osobní údaje o osobách, které nejsou osobami USA, mohou být šířeny pouze v případě, že se jedná o stejný druh informací, které mohou být šířeny o osobách USA, např. informace potřebné k ochraně bezpečnosti určité osoby nebo organizace (např. cíle, oběti nebo rukojmí mezinárodních teroristických organizací)<sup>(299)</sup>. Osobní údaje navíc nelze šířit pouze z důvodu státní příslušnosti nebo země pobytu osoby nebo za účelem obejití požadavků výkonného dekretu č. 14086<sup>(300)</sup>. K šíření v rámci vlády USA může dojít pouze v případě,

<sup>(293)</sup> Ustanovení § 2(c)(iii)(B)(1) výkonného dekretu č. 14086. Viz také hlava VIII zákona o národní bezpečnosti (podrobně popisující požadavky na přístup k utajovaným informacím), výkonný dekret č. 12333, § 1.5 (požadující po vedoucích komunity zpravodajských služeb, aby dodržovali pokyny pro sdílení a bezpečnost informací, informační soukromí a další právní požadavky), směrnice o národní bezpečnosti č. 42: „Národní politika pro bezpečnost telekomunikačních a informačních systémů národní bezpečnosti“ (ukládající Výboru pro národní bezpečnostní systémy, aby výkonným složkám a službám poskytoval pokyny pro systémovou bezpečnost systémů národní bezpečnosti) a Národní bezpečnostní memorandum č. 8: „Zlepšení kybernetické bezpečnosti systémů národní bezpečnosti, ministerstva obrany a zpravodajské komunity“ (stanovící časový plán a pokyny pro implementaci požadavků na kybernetickou bezpečnost systémů národní bezpečnosti, včetně vícefaktorového ověřování, šifrování, cloudových technologií a služeb detekce koncových bodů).

<sup>(294)</sup> Ustanovení § 2(c)(iii)(B)(2) výkonného dekretu č. 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 oprávněných správních, testovacích, vývojových, bezpečnostních nebo dohledových funkcí (§ 2(c)(iii)(B)(3) výkonného dekretu č. 14086).

<sup>(295)</sup> Ustanovení § 2(d)(ii) výkonného dekretu č. 14086.

<sup>(296)</sup> Ustanovení § 2(c)(iii)(C) výkonného dekretu č. 14086.

<sup>(297)</sup> Ustanovení § 2(c)(iii)(A)(2)(a)–(c) výkonného dekretu č. 14086. Obecněji řečeno, každá služba musí zavést politiky a postupy určené k minimalizaci šíření a uchovávání osobních údajů shromážděných prostřednictvím signálového zpravodajství (§ 2(c)(iii)(A) výkonného dekretu č. 14086).

<sup>(298)</sup> Viz např. ustanovení § 309 zákona o povolení zpravodajské činnosti pro fiskální rok 2015; postupy minimalizace přijaté jednotlivými zpravodajskými službami podle § 702 zákona FISA a schválené Soudem pro uplatňování zákona FISA; postupy schválené ministrem spravedlnosti a zákonem o federálních záznamech (vyžadující, aby federální agentury USA, včetně služeb národní bezpečnosti, stanovily lhůty uchovávání svých záznamů, které musí schválit Národní správa archivů a záznamů).

<sup>(299)</sup> Ustanovení § 2(c)(iii)(A)(1)(a) a 5(d) výkonného dekretu č. 14086 ve spojení s ustanovením § 2.3 výkonného dekretu č. 12333.

<sup>(300)</sup> Ustanovení § 2(c)(iii)(A)(1)(b) a (e) výkonného dekretu č. 14086.

že oprávněná a vyškolená osoba se důvodně domnívá, že příjemce má potřebu informace znát <sup>(301)</sup> a bude je náležitě chránit <sup>(302)</sup>. 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) <sup>(303)</sup>.

- (159) A konečně, mimo jiné i proto, aby se usnadnil dohled nad dodržováním platných právních požadavků, jakož i účinná náprava, je každá zpravodajská služba povinna podle výkonného dekretu č. 14086 vést příslušnou dokumentaci o shromažďování informací prostřednictvím signálového zpravodajství. Požadavky na dokumentaci zahrnují takové prvky, jako je faktický základ pro posouzení, že určitá sběrná činnost je nezbytná k dosažení potvrzené zpravodajské priority <sup>(304)</sup>.
- (160) Kromě výše uvedených záruk vyplývajících z výkonného dekretu č. 14086 pro používání informací shromážděných prostřednictvím signálového zpravodajství podléhají všechny zpravodajské služby USA obecnějším požadavkům na účelové omezení, minimalizaci, přesnost, zabezpečení, uchovávání a šíření údajů, které vyplývají zejména z oběžníku OMB č. A-130, zákona o elektronické veřejné správě, zákona o federálních záznamech (viz 101.–106. bod odůvodnění) a pokynů Výboru pro národní bezpečnostní systémy (Committee on National Security Systems (dále také jako „výbor CNSS“)) <sup>(305)</sup>.

### 3.2.2 Dohled

- (161) Činnost zpravodajských služeb USA podléhá dohledu různých orgánů.
- (162) Za prvé, výkonný dekret č. 14086 stanoví, že každá zpravodajská služba musí mít právní úředníky na vyšší úrovni a úředníky pro dohled a dodržování předpisů, kteří zajistí dodržování platných právních předpisů USA <sup>(306)</sup>. Musí zejména provádět pravidelný dohled nad činnostmi v oblasti signálového zpravodajství a zajišťovat nápravu jakéhokoli nedodržení předpisů. Zpravodajské služby musí těmto úředníkům umožnit přístup ke všem relevantním informacím, aby mohli vykonávat své funkce dohledu, a nesmějí podnikat žádné kroky, které by bránily jejich činností dohledu nebo je nepřiměřeně ovlivňovaly <sup>(307)</sup>. Každý závažný případ nedodržení předpisů <sup>(308)</sup> zjištěný úředníkem pro dohled nebo jiným zaměstnancem musí být kromě toho neprodleně oznámen vedoucímu zpravodajské služby a řediteli národních zpravodajských služeb, kteří musí zajistit, aby byla přijata veškerá nezbytná opatření k nápravě a zabránění opakování závažného případu nedodržení předpisů <sup>(309)</sup>.
- (163) Tuto funkci dohledu plní úředníci s určenou funkcí v oblasti dodržování předpisů, jakož i úředníci pro ochranu soukromí a občanských svobod a generální inspektoři <sup>(310)</sup>.

<sup>(301)</sup> Viz např. pokyny AGG-DOM, které stanoví, že úřad FBI může šířit informace pouze v případě, že je příjemce potřebuje znát k plnění svého poslání nebo k ochraně veřejnosti.

<sup>(302)</sup> Ustanovení § 2(c)(iii)(A)(1)(c) výkonného dekretu č. 14086. Zpravodajské služby mohou například šířit informace za okolností, které jsou důležité pro vyšetřování trestného činu nebo se k němu vztahují, včetně například šíření varování před hrozbou zabití, vážného ublížení na zdraví nebo únosu; šíření informací o kybernetických hrozbách, incidentech nebo reakcích na narušení a informování obětí nebo varování potenciálních obětí trestných činů.

<sup>(303)</sup> Ustanovení § 2(c)(iii)(A)(1)(d) výkonného dekretu č. 14086.

<sup>(304)</sup> Ustanovení § 2(c)(iii)(E) výkonného dekretu č. 14086.

<sup>(305)</sup> Viz politika výboru CNSS č. 22, politika řízení rizik kybernetické bezpečnosti a pokyn výboru CNSS č. 1253, který obsahuje podrobné pokyny k bezpečnostním opatřením, jež mají být zavedena pro systémy národní bezpečnosti.

<sup>(306)</sup> Ustanovení § 2(d)(i)(A)–(B) výkonného dekretu č. 14086.

<sup>(307)</sup> Ustanovení § 2(d)(i)(B)–(C) výkonného dekretu č. 14086.

<sup>(308)</sup> 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(l) výkonného dekretu č. 14086.

<sup>(309)</sup> Ustanovení § 2(d)(iii) výkonného dekretu č. 14086.

<sup>(310)</sup> Ustanovení § 2(d)(i)(B) výkonného dekretu č. 14086.

(164) Stejně jako v případě orgánů pro prosazování trestního práva existují úředníci pro ochranu soukromí a občanských svobod ve všech zpravodajských službách<sup>(311)</sup>. K pravomocem těchto úředníků většinou patří dozor nad postupy, aby bylo zajištěno, že dané ministerstvo/služba přistupuje k ochraně občanských svobod a soukromí adekvátně a že zavedlo/zavedla odpovídající postupy pro řešení stížností fyzických osob, které mají za to, že jejich soukromí nebo občanské svobody byly porušeny (a v některých případech, např. jako Úřad ředitele národních zpravodajských služeb (Office of the Director of National Intelligence, dále také jako „úřad ODNI“), mohou mít sami pravomoc stížnosti prošetřovat<sup>(312)</sup>). Vedoucí zpravodajských služeb musí zajistit, aby úředníci pro ochranu soukromí a občanských svobod měli k dispozici 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<sup>(313)</sup>. Úředníci pro ochranu soukromí a občanských svobod předkládají Kongresu a výboru PCLOB pravidelné zprávy, mimo jiné o počtu a povaze stížností obdržených ministerstvem/službou, se shrnutím o vyřízení těchto stížností, provedených kontrolách a šetřeních a dopadu kroků podniknutých úředníkem<sup>(314)</sup>.

(165) Za druhé, každá zpravodajská služba má nezávislého generálního inspektora, do jehož popisu práce patří mimo jiné dohled nad zahraniční zpravodajskou činností. Sem patří odbor generálního inspektora zpravodajské komunity v rámci úřadu ODNI, kterému je svěřena všeobecná pravomoc nad celou zpravodajskou komunitou a který je oprávněn šetřit stížnosti nebo informace týkající se údajného nezákonného jednání či zneužití pravomoci v souvislosti s programy či činnostmi úřadu ODNI a/nebo zpravodajské komunity<sup>(315)</sup>. Stejně jako v případě orgánů pro prosazování trestního práva (viz 109. bod odůvodnění) jsou tito generální inspektori ze zákona nezávislí<sup>(316)</sup> a odpovědní za provádění auditů a vyšetřování týkajících se programů a operací prováděných příslušnou službou pro účely národního zpravodajství, a to i pokud jde o zneužití nebo porušení zákona<sup>(317)</sup>. Mají přístup ke všem záznamům, zprávám, auditům, přezkumům, dokumentům, listinám, doporučením a dalším relevantním

<sup>(311)</sup> Viz 42 U.S.C. § 2000ee-1. Patří k nim např. Ministerstvo zahraničních věcí, Ministerstvo spravedlnosti, Ministerstvo vnitřní bezpečnosti, Ministerstvo obrany, agentura NSA, Ústřední zpravodajská služba (Central Intelligence Agency, CIA), úřad FBI a úřad ODNI.

<sup>(312)</sup> Viz ustanovení § 3(c) výkonného dekretu č. 14086.

<sup>(313)</sup> 42 U.S.C. § 2000ee-1(d).

<sup>(314)</sup> Viz 42 U.S.C. § 2000ee-1 (f)(1),(2). Například ze zprávy Úřadu pro občanské svobody, soukromí a transparentnost agentury NSA za období leden 2021 až 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., přičemž zohlednil různé faktory, jako je množství a druh informací souvisejících s danou činností, dotčené osoby, účel a předpokládané využití údajů, zavedené záruky ke zmírnění případných rizik pro soukromí atd. ([https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%20CLPT%20JANUARY%20-%20JUNE%202021%20\\_FINAL.PDF](https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%20CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF)). Podobné zprávy Úřadu pro ochranu soukromí a občanských svobod služby CIA za leden až červen 2019 poskytují informace o dohledových činnostech úřadu, např. o přezkumu dodržování pokynů ministra spravedlnosti podle výkonného dekretu č. 12333, pokud jde o uchovávání a šíření informací, o poradenství poskytnutém k provádění směrnice PPD 28 a k požadavkům na identifikaci a řešení případů porušení zabezpečení údajů a o přezkumech používání osobních údajů a nakládání s nimi (<https://www.cia.gov/static/9d762fbef6669c7e6d7f1e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf>).

<sup>(315)</sup> Tento generální inspektor je jmenován prezidentem po potvrzení Senátu a odvolat jej může jen prezident.

<sup>(316)</sup> Generální inspektori jsou jmenováni nastálo a smí je odvolat pouze prezident, který při tom musí Kongresu písemně sdělit důvody odvolání. To však nemusí nutně znamenat, že se nemusí řídit příkazy. V některých případech může ministr nebo ředitel agentury generálnímu inspektorovi zakázat zahájit, vykonat nebo dokončit audit nebo vyšetřování, bylo-li usouzeno, že je to nezbytné k ochraně důležitých národních (bezpečnostních) zájmů. Kongres však musí být o výkonu této pravomoci informován a může na tomto základě pohnat příslušného ministra/ředitele k odpovědnosti. Viz např. zákon o generálních inspektorech z roku 1978, § 8 (pro Ministerstvo obrany); § 8E (pro Ministerstva spravedlnosti), § 8G (d)(2)(A),(B) (pro agenturu NSA); 50. U.S.C. § 403q (b) (pro službu CIA); zákon o povolení zpravodajské činnosti pro fiskální rok 2010 (Intelligence Authorization Act For Fiscal Year 2010), § 405(f) (pro zpravodajskou komunitu).

<sup>(317)</sup> Zákon o generálních inspektorech z roku 1978, v platném znění, Pub. L. 117–108 ze dne 8. dubna 2022. Jak je vysvětleno například v pololetních zprávách pro Kongres za období od 1. dubna 2021 do 31. března 2022, generální inspektor agentury NSA provedl hodnocení nakládání s informacemi o osobách USA shromážděnými podle výkonného dekretu č. 12333, procesu čištění údajů shromážděných prostřednictvím signálového zpravodajství, automatizovaného nástroje pro cílení používaného agenturou NSA a dodržování pravidel pro dokumentaci a dotazování s ohledem na shromažďování údajů podle § 702 zákona FISA a v této souvislosti vydal několik doporučení (viz <https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907>, 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 šetření provedené generálním inspektorem zpravodajské komunity týkající se bezpečnosti informací a neoprávněného vyrazování utajovaných informací týkajících se národní bezpečnosti ([https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG\\_Semiannual\\_Report\\_April\\_2021\\_to\\_September\\_2021.pdf](https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf), s. 8 a 11 a [https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21\\_SAR/Oct%202021-Mar%202022%20ICIG%20SAR\\_Unclass\\_FINAL.pdf](https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf), s. 19–20).

materiálům, v případě potřeby i prostřednictvím předvolání, a mohou vyslýchat <sup>(318)</sup>. Generální inspektori předávají případy podezření na trestné činy k trestnímu stíhání a předkládají vedoucím služeb doporučení k nápravě <sup>(319)</sup>. Zatímco jejich doporučení jsou nezávazná, jejich zprávy, včetně zpráv o následných krocích (nebo jejich absenci) <sup>(320)</sup> se obecně zveřejňují a předkládají Kongresu, který na tomto základě může vykonat svou funkci dohledu (viz 168.–169. bod odůvodnění) <sup>(321)</sup>.

- (166) Za třetí, Výbor pro dohled nad zpravodajstvím, který je zřízený v rámci Poradního výboru prezidenta pro zpravodajství, dohlíží na to, jak a zda zpravodajské orgány USA dodržují Ústavu USA a veškeré platné předpisy <sup>(322)</sup>. Poradní výbor prezidenta pro zpravodajství je poradní orgán v rámci výkonné kanceláře prezidenta, který se skládá ze šestnácti členů jmenovaných prezidentem z řad osob mimo vládu USA. Výbor pro dohled nad zpravodajstvím se skládá nejvýše z pěti členů jmenovaných prezidentem z řad členů Poradního výboru prezidenta pro zpravodajství. Podle výkonného dekretu č. 12333 <sup>(323)</sup> jsou vedoucí všech zpravodajských služeb povinni hlásit Výboru pro dohled nad zpravodajstvím jakoukoli zpravodajskou činnost, u níž existuje důvodné podezření, že by mohla být nezákonná nebo v rozporu s výkonným dekretem nebo prezidentskou směrnicí. Aby se zajistilo, že Výbor pro dohled nad zpravodajstvím bude mít přístup k informacím nezbytným pro výkon svých funkcí, nařizuje výkonný dekret č. 13462 řediteli Národního zpravodajství a vedoucím zpravodajských služeb, aby poskytovali veškeré informace a součinnost, jež Výbor pro dohled nad zpravodajstvím určí jako potřebné pro výkon svých funkcí, a to v rozsahu povoleném zákonem <sup>(324)</sup>. Výbor pro dohled nad zpravodajstvím je zase povinen informovat prezidenta o zpravodajských činnostech, o nichž se domnívá, že mohou být v rozporu se zákony USA (včetně výkonných dekretů) a že se jimi ministr spravedlnosti, ředitel národního zpravodajství nebo vedoucí zpravodajské služby dostatečně nezabývají <sup>(325)</sup>. Výbor pro dohled nad zpravodajstvím je kromě toho povinen informovat ministra spravedlnosti o možném porušení trestního práva.

- (167) Za čtvrté, zpravodajské služby podléhají dohledu ze strany výboru PCLOB. Podle jeho zakládajícího statutu jsou výboru PCLOB svěřeny povinnosti v oblasti protiteroristické politiky a jejího provádění s ohledem na ochranu soukromí a občanských svobod. V rámci přezkumu činnosti zpravodajských služeb může tento výbor přistupovat ke všem relevantním záznamům, zprávám, auditům, přezkumům, dokumentům, listinám a doporučením jednotlivých zpravodajských služeb, včetně utajovaných informací, provádět pohovory a vyslýchat svědky <sup>(326)</sup>. Výboru jsou předkládány zprávy úředníků pro otázky ochrany občanských svobod a soukromí několika federálních ministerstev či služeb <sup>(327)</sup>, přičemž výbor může vydávat doporučení orgánům státní správy a zpravodajským službám, a naopak výbor předkládá pravidelné zprávy výborům Kongresu a prezidentovi <sup>(328)</sup>. Zprávy výboru, včetně těch, které jsou určeny Kongresu, musí být v maximální možné míře zveřejněny <sup>(329)</sup>. Výbor PCLOB vydal několik zpráv o dohledu a následných opatřeních, včetně analýzy programů prováděných na základě § 702 zákona FISA a v této souvislosti i ochrany soukromí, provádění směrnice PPD 28 a výkonného dekretu č. 12333 <sup>(330)</sup>.

<sup>(318)</sup> Viz zákon o generálních inspektorech z roku 1978, § 6.

<sup>(319)</sup> Viz tamtéž § 4, 6–5.

<sup>(320)</sup> Pokud jde o následná opatření, která jsou přijímána v návaznosti na zprávy a doporučení generálních inspektorů, viz např. reakce na zprávu generálního inspektora Ministerstva spravedlnosti, který zjistil, že úřad FBI nebyl dostatečně transparentní vůči Soudu pro uplatňování zákona FISA v žádostech z let 2014 až 2019, což vedlo k reformám s cílem zlepšit dodržování předpisů, dohled a odpovědnost v úřadu FBI (např. ředitel úřadu FBI nařídil více než 40 nápravných opatření, včetně 12 specifických pro proces podle zákona FISA týkajících se dokumentace, dohledu, vedení spisů, školení a auditů) (viz <https://www.justice.gov/opa/pr/departments-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance> a <https://oig.justice.gov/reports/2019/o20012.pdf>). Viz např. také audit generálního inspektora Ministerstva spravedlnosti týkající se úlohy a odpovědnosti kanceláře generálního rady úřadu FBI při dohledu nad dodržováním platných zákonů, politik a postupů týkajících se činností úřadu FBI v oblasti národní bezpečnosti a dodatek č. 2, který obsahuje dopis úřadu FBI, v němž přijímá všechna doporučení. V této souvislosti je v dodatku č. 3 uveden přehled následných opatření a informací, které generální inspektor požadoval od úřadu FBI, aby mohl svá doporučení uzavřít (<https://oig.justice.gov/sites/default/files/reports/22-116.pdf>).

<sup>(321)</sup> Viz zákon o generálních inspektorech z roku 1978, § 4(5) a 5.

<sup>(322)</sup> Viz výkonný dekret č. 13462.

<sup>(323)</sup> Ustanovení § 1.6(c) výkonného dekretu č. 12333.

<sup>(324)</sup> Ustanovení § 8(a) výkonného dekretu č. 13462.

<sup>(325)</sup> Ustanovení § 6(b) výkonného dekretu č. 13462.

<sup>(326)</sup> 42 U.S.C. § 2000ee (g).

<sup>(327)</sup> Viz 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Mezi ty patří alespoň Ministerstvo spravedlnosti, Ministerstvo obrany, Ministerstvo vnitřní bezpečnosti, ředitel národních zpravodajských služeb a Ústřední zpravodajská služba, plus další ministerstva, agentury či prvky výkonné moci, které výbor PCLOB označil za příslušné ke kontrole.

<sup>(328)</sup> 42 U.S.C. § 2000ee (e).

<sup>(329)</sup> 42 U.S.C. § 2000ee (f).

<sup>(330)</sup> Dostupné na <https://www.pclob.gov/Oversight>

Výbor PCLOB je rovněž pověřen výkonem zvláštních funkcí dohledu, pokud jde o provádění výkonného dekretu č. 14086, zejména přezkoumáváním, zda jsou postupy zpravodajských služeb v souladu s výkonným dekretem (viz 126. bod odůvodnění), a hodnocením fungování nápravného mechanismu (viz 194. bod odůvodnění).

- (168) Za páté, kromě těchto mechanismů dohledu v rámci výkonné moci mají odpovědnost za dohled nad veškerou zahraniční zpravodajskou činností USA zvláštní výbory Kongresu USA (výbory Sněmovny reprezentantů a Senátu pro zpravodajství a pro justici). Členové těchto výborů mají přístup k utajovaným informacím i ke zpravodajským metodám a programům<sup>(331)</sup>. Výbory vykonávají dohled různými způsoby, zejména prostřednictvím slyšení, vyšetřování, přezkumů a zpráv<sup>(332)</sup>.
- (169) Výbory Kongresu dostávají pravidelné zprávy o zpravodajské činnosti, mimo jiné od ministra spravedlnosti, ředitele národních zpravodajských služeb, zpravodajských služeb a dalších orgánů dohledu (např. generálních inspektorů), viz 164. až 165. bod odůvodnění. Konkrétně podle zákona o národní bezpečnosti (National Security Act) „[p] rezident zajistí, aby výbory Kongresu pro zpravodajství byly plně a aktuálně informovány o zpravodajské činnosti Spojených států, včetně o veškeré významné očekávané zpravodajské činnosti, jak je stanoveno v této podkapitole“<sup>(333)</sup>. Kromě toho „[p]rezident zajistí, aby byly výbory Kongresu pro zpravodajství bezodkladně informovány o veškeré nelegální zpravodajské činnosti i o nápravných opatřeních, jež byla nebo mají být přijata v souvislosti s touto nelegální činností“<sup>(334)</sup>.
- (170) Ze zvláštních zákonů nadto vyplývají další požadavky na podávání zpráv. Podle zákona FISA je ministr spravedlnosti zejména povinen „plně informovat“ výbory Senátu a Sněmovny reprezentantů pro zpravodajství a pro justici o činnostech vlády podle určitých paragrafů tohoto zákona<sup>(335)</sup>. Vláda je podle tohoto zákona dále povinna těmto výborům Kongresu předkládat kopie veškerých rozhodnutí, příkazů či stanovisek Soudu pro uplatňování zákona FISA nebo Odvolacího soudu pro uplatňování zákona FISA, které obsahují „významný výklad či interpretaci“ ustanovení zákona FISA. Pokud jde o sledování podle § 702 zákona FISA, probíhá parlamentní dohled formou povinných hlášení výborům Kongresu pro zpravodajství a pro justici a častých brífinků a slyšení. Patří k nim pololetní zpráva ministra spravedlnosti o používání § 702 zákona FISA s podkladovými dokumenty, včetně zpráv Ministerstva spravedlnosti a Úřadu ředitele národních zpravodajských služeb o dodržování předpisů a popisu všech případů nesouladu<sup>(336)</sup>, a samostatné pololetní hodnocení ministra spravedlnosti a ředitele národních zpravodajských služeb o dodržování postupů cíleného sběru a minimalizace<sup>(337)</sup>.

<sup>(331)</sup> 50 U.S.C. § 3091.

<sup>(332)</sup> Výbory například pořádají tematická slyšení (viz např. nedávné slyšení výboru pro justici Sněmovny reprezentantů na téma „digitální policejní zátahy“, <https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983>, a slyšení výboru pro zpravodajství Sněmovny reprezentantů o využívání umělé inteligence zpravodajskou komunitou, <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263>), pravidelná slyšení týkající se dohledu, např. úřadu FBI a oddělení národní bezpečnosti Ministerstva spravedlnosti, 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>. Jako příklad vyšetřování viz vyšetřování senátního výboru pro zpravodajství týkající se ruského vměšování do voleb v USA v roce 2016, viz <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures>. Pokud jde o podávání zpráv, viz např. přehled činnosti (v oblasti dohledu) výboru ve zprávě senátního výboru pro zpravodajství za období od 4. ledna 2019 do 3. ledna 2021 pro Senát, <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4>

<sup>(333)</sup> Viz 50 U.S.C. § 3091(a)(1). Toto ustanovení obsahuje obecné požadavky, pokud jde o dohled Kongresu v oblasti národní bezpečnosti.

<sup>(334)</sup> Viz 50 U.S.C. § 3091(b).

<sup>(335)</sup> Viz 50 U.S.C. § 1808, 1846, 1862, 1871, 1881f.

<sup>(336)</sup> Viz 50 U.S.C. § 1881f.

<sup>(337)</sup> Viz 50 U.S.C. § 1881a(l)(1).

- (171) Podle zákona FISA musí vláda USA kromě toho každý rok Kongresu (a veřejnosti) oznamovat počet příkazů vyžádaných a obdržených podle zákona FISA a mimo jiné odhad počtu osob USA a osob, které nejsou osobami USA, které se staly cílem sledování<sup>(338)</sup>. Zákon dále stanoví povinnost zveřejňovat počty vydaných National Security Letters, a to opět jak u osob USA, tak u osob, které nejsou osobami USA (příčemž adresátům příkazů a osvědčení podle zákona FISA i žádostí na základě National Security Letters dovoluje za určitých podmínek vydávat zprávy o transparentnosti)<sup>(339)</sup>.
- (172) Zpravodajská komunita vyvíjí různé snahy o zajištění transparentnosti svých (zahraničních) zpravodajských činností. Například v roce 2015 úřad ODNI přijal Zásady transparentnosti zpravodajských služeb a Plán provádění transparentnosti a nařídil každé zpravodajské službě, aby jmenovala úředníka pro transparentnost zpravodajských služeb, který bude podporovat transparentnost a vést iniciativy v oblasti transparentnosti<sup>(340)</sup>. V rámci těchto snah zpravodajská komunita zveřejnila a nadále zveřejňuje odtajněné části politik, postupů, zpráv o dohledu, zpráv o činnostech podle § 702 zákona FISA a výkonného dekretu č. 12333, rozhodnutí Soudu pro uplatňování zákona FISA a další materiály, a to i na specializované internetové stránce „IC on the Record“, kterou spravuje úřad ODNI<sup>(341)</sup>.
- (173) A konečně, shromažďování osobních údajů podle § 702 zákona FISA podléhá kromě kontroly ze strany orgánů dohledu uvedených v 162. až 168. bodě odůvodnění také dohledu ze strany Soudu pro uplatňování zákona FISA<sup>(342)</sup>. Podle pravidla č. 13 jednacího řádu Soudu pro uplatňování zákona FISA jsou pracovníci odpovědní za dodržování předpisů ve zpravodajských službách USA povinni hlásit veškerá porušení postupů cílení, minimalizace a dotazování podle § 702 zákona FISA Ministerstvu spravedlnosti a úřadu ODNI, které je následně hlásí Soudu pro uplatňování zákona FISA. Kromě toho Ministerstvo spravedlnosti a úřad ODNI předkládají Soudu pro uplatňování zákona FISA pololetní společné hodnotící zprávy o dohledu, které identifikují trendy v oblasti dodržování postupů cíleného sběru; poskytují statistické údaje; popisují kategorie incidentů týkajících se dodržování předpisů; podrobně popisují důvody, proč došlo k určitým incidentům v oblasti dodržování předpisů o cíleném sběru, a uvádějí opatření, která zpravodajské služby přijaly, aby se zabránilo jejich opakování<sup>(343)</sup>.
- (174) V případě potřeby (např. pokud je zjištěno porušení postupů cíleného sběru) může Soud nařídit příslušné zpravodajské službě, aby přijala opatření k nápravě<sup>(344)</sup>. Příslušná nápravná opatření mohou být v rozsahu od individuálních až po strukturální opatření, např. od ukončení získávání údajů a vymazání nezákonně získaných údajů až po změnu praxe shromažďování údajů, včetně pokynů a školení pro zaměstnance<sup>(345)</sup>. Kromě toho Soud pro uplatňování zákona FISA při každoročním přezkumu osvědčení podle § 702 posuzuje případy nedodržení

<sup>(338)</sup> 50 U.S.C. § 1873(b). Podle § 402 navíc „ředitel národních zpravodajských služeb v konzultaci s ministrem spravedlnosti provede přezkum odtajnění každého rozhodnutí, příkazu nebo stanoviska vydaného Soudem pro uplatňování zákona FISA nebo Odvolacím soudem pro uplatňování zákona FISA (podle definice § 601 písm. e)), které obsahují významný výklad či interpretaci jakéhokoli ustanovení zákona, včetně jakéhokoli nového nebo významného výkladu či interpretace termínu „konkrétní selekční termín“, a ve shodě s tímto přezkumem zveřejní každé takové rozhodnutí, příkaz nebo stanovisko v co největším proveditelném rozsahu“.

<sup>(339)</sup> 50 U.S.C. § 1873(b)(7) a 1874.

<sup>(340)</sup> <https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic>

<sup>(341)</sup> Viz „IC on the Record“, dostupné na <https://icontherecord.tumblr.com/>

<sup>(342)</sup> V minulosti dospěl Soud pro uplatňování zákona FISA k závěru, že „[s]oud je přesvědčen, že prováděcí agentury, jakož i [úřad ODNI] a [odbor národní bezpečnosti Ministerstva spravedlnosti] věnují značné zdroje svým povinnostem v oblasti dodržování předpisů a dohledu podle § 702. Obecně platí, že případy nedodržení předpisů jsou neprodleně identifikovány a jsou přijata vhodná nápravná opatření, včetně vyčištění informací, které byly získány neoprávněně nebo které jinak podléhají požadavkům na zničení podle platných postupů“. Soud pro uplatňování zákona FISA, Memorandum stanovisko a příkaz [nadpis redigován] (2014), k dispozici na <https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf>

<sup>(343)</sup> Viz např. Zpráva Ministerstva spravedlnosti / úřadu ODNI o dodržování § 702 zákona FISA za období od června 2018 do listopadu 2018 určená Soudu pro uplatňování zákona FISA, s. 21–65.

<sup>(344)</sup> 50 U.S.C. § 1803(h). Viz také Zpráva podle § 702 výboru PCLOB, s. 76. Kromě toho viz Memorandum stanovisko a příkaz Soudu pro uplatňování zákona FISA ze dne 3. října 2011 jako příklad příkazu k odstranění nedostatků, v němž bylo vládě nařízeno, aby zjištěné nedostatky odstranila do 30 dnů. Dostupné na <https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf>. Viz Waltonův dopis, oddíl 4, s. 10–11. Viz také stanovisko Soudu pro uplatňování zákona FISA ze dne 18. října 2018, dostupné na [https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018\\_Cert\\_FISC\\_Opin\\_18Oct18.pdf](https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf), potvrzené stanoviskem Odvolacího soudu pro uplatňování zákona FISA ze dne 12. července 2019, dostupné na [https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018\\_Cert\\_FISC\\_Opinion\\_12Jul19.pdf](https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opinion_12Jul19.pdf), v němž Soud pro uplatňování zákona FISA mimo jiné nařídil vládě, aby splnila určité požadavky na oznamování, dokumentaci a podávání zpráv vůči Soudu pro uplatňování zákona FISA.

<sup>(345)</sup> Viz např. Soud pro uplatňování zákona FISA, Memorandum, stanovisko a příkaz č. 76 (6. prosince 2019) (schváleno ke zveřejnění dne 4. září 2020), v němž Soud pro uplatňování zákona FISA 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 podle § 702 zákona FISA, které byly odvolány z důvodů dodržování předpisů, jakož i o dalších záležitostech. Viz též příloha VII.

předpisů, aby určil, zda jsou předložená osvědčení v souladu s požadavky zákona FISA. Stejně tak, pokud Soud pro uplatňování zákona FISA zjistí, že vládní osvědčení nebyla dostatečná, a to i z důvodu konkrétních případů nedodržování předpisů, může vydat tzv. příkaz k odstranění nedostatků, který vládě ukládá, aby do 30 dnů porušení napravila, nebo jí ukládá, aby osvědčení podle § 702 přestala nebo nezačala provádět. V neposlední řadě Soud pro uplatňování zákona FISA posuzuje trendy, které v otázkách dodržování předpisů pozoruje, a může požadovat změny postupů nebo dodatečný dohled a podávání zpráv, aby se trendy v dodržování předpisů řešily <sup>(346)</sup>.

### 3.2.3 Nápravná opatření

- (175) Jak je podrobněji vysvětleno v tomto oddíle, ve Spojených státech existuje řada možností, jak subjektům údajů Unie 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.
- (176) Za prvé, podle výkonného dekretu č. 14086, doplněného nařízením ministra spravedlnosti, kterým se zřizuje Soud pro přezkum ochrany údajů, je zřízen zvláštní nápravný mechanismus, který se zabývá stížnostmi fyzických osob týkajícími se činností v oblasti signálového zpravodajství USA a řeší je. Každá fyzická osoba v EU je oprávněna podat nápravnému mechanismu stížnost týkající se údajného porušení právních předpisů USA upravujících činnosti v oblasti signálového zpravodajství (např. výkonného dekretu č. 14086, § 702 zákona FISA, výkonného dekretu č. 12333), které negativně postihuje její zájmy v oblasti soukromí a občanských svobod <sup>(347)</sup>. Tento nápravný mechanismus je k dispozici osobám ze zemí nebo organizací regionální hospodářské integrace, které ministr spravedlnosti USA určil jako „kvalifikované státy“ <sup>(348)</sup>. Dne 30. června 2023 byly Evropská unie a tři země Evropského sdružení volného obchodu, které společně tvoří Evropský hospodářský prostor, ministrem spravedlnosti podle § 3 písm. f) výkonného dekretu č. 14086 označeny za „kvalifikovaný stát“ <sup>(349)</sup>. Tímto označením není dotčen čl. 4 odst. 2 Smlouvy o Evropské unii.
- (177) Subjekt údajů v Unii, který si přeje podat takovou stížnost, ji musí podat dozorovému úřadu v členském státě EU, který je příslušný pro dohled nad zpracováním osobních údajů orgány veřejné moci <sup>(350)</sup> (úřad pro ochranu osobních údajů). Tím je zajištěn snadný přístup k nápravnému mechanismu, neboť se fyzické osoby mohou obrátit na orgán „v blízkosti svého domova“, s nímž mohou komunikovat ve svém vlastním jazyce. Poté, co se ověří splnění požadavků pro podání stížnosti uvedených ve 178. bodě odůvodnění, předá příslušný úřad pro ochranu osobních údajů stížnost – prostřednictvím sekretariátu Evropského sboru pro ochranu osobních údajů – nápravnému mechanismu.
- (178) Podání stížnosti k nápravnému mechanismu podléhá omezeným požadavkům na přípustnost, neboť fyzické osoby nemusí prokazovat, že jejich údaje byly skutečně předmětem činností v oblasti signálového zpravodajství USA <sup>(351)</sup>. Aby nápravný mechanismus mohl zahájit přezkum, je třeba současně poskytnout určité základní informace, např. o osobních údajích, o nichž se důvodně předpokládá, že byly předány do USA, a o prostředcích, kterými se předpokládá, že byly předány; o totožnosti subjektů vlády USA, o nichž se předpokládá, že se podílely na údajném porušení (pokud jsou známy); o důvodech podporujících tvrzení, že došlo k porušení právních předpisů USA (ačkoli to opět nevyžaduje prokázání, že osobní údaje byly skutečně shromážděny zpravodajskými službami USA), a o povaze požadované nápravy.

<sup>(346)</sup> Viz příloha VII.

<sup>(347)</sup> Viz ustanovení § 4(k)(iv) výkonného dekretu č. 14086, které stanoví, že stížnost k nápravnému mechanismu musí podat stěžovatel jednající vlastním jménem (tj. nikoli jako zástupce vládní, nevládní nebo mezivládní organizace). Pojem „negativně postižený“ nevyžaduje, aby stěžovatel splňoval určitou hranici, aby měl přístup k nápravnému mechanismu (v tomto ohledu viz 178. bod odůvodnění). Spíše objasňuje, že úředník ODNI CLPO a Soud pro přezkum ochrany údajů mají pravomoc napravit porušení právních předpisů USA upravujících činnosti signálového zpravodajství, která negativně postihují individuální zájmy stěžovatele v oblasti soukromí a občanských svobod. Naopak porušení požadavků podle platných právních předpisů USA, které nejsou určeny k ochraně fyzických osob (např. rozpočtové požadavky), by do pravomoci úředníka ODNI CLPO a Soudu pro přezkum ochrany údajů nespádalo.

<sup>(348)</sup> Ustanovení § 3(f) výkonného dekretu č. 14086.

<sup>(349)</sup> <https://www.justice.gov/opcl/executive-order-14086>

<sup>(350)</sup> Ustanovení § 4(d)(v) výkonného dekretu č. 14086.

<sup>(351)</sup> Viz ustanovení § 4(k)(i)–(iv) výkonného dekretu č. 14086.

- (179) Prvotní šetření stížností předložených tomuto nápravnému mechanismu provádí úředník ODNI CLPO, jehož stávající zákonná úloha a pravomoci byly rozšířeny o tyto konkrétní kroky přijímané podle výkonného dekretu č. 14086 <sup>(352)</sup>. V rámci zpravodajské komunity je úředník CLPO mimo jiné odpovědný za zajištění toho, aby ochrana občanských svobod a soukromí byla vhodně začleněna do politik a postupů úřadu ODNI a zpravodajských služeb; za dohled nad dodržováním příslušných požadavků na občanské svobody a soukromí ze strany úřadu ODNI a za provádění posouzení dopadu na soukromí <sup>(353)</sup>. Úředníka CLPO ODNI může odvolat pouze ředitel národních zpravodajských služeb na základě zákonného důvodu, tj. v případě pochybení, nesprávného postupu, porušení bezpečnosti, zanedbání povinností nebo nezpůsobilosti <sup>(354)</sup>.
- (180) Při provádění přezkumu má úředník CLPO ODNI pro účely svého posouzení přístup k informacím a může se opírat o povinnou součinnost úředníků pro ochranu soukromí a občanských svobod v různých zpravodajských službách <sup>(355)</sup>. Zpravodajské služby mají zakázáno bránit přezkumu prováděnému úředníkem ODNI CLPO nebo jej nepřiměřeně narušovat. To se týká i ředitele národních zpravodajských služeb, který nesmí do přezkumu zasahovat <sup>(356)</sup>. Při přezkoumávání stížnosti musí úředník ODNI CLPO „uplatňovat zákon nestranně“ s přihlédnutím jak k zájmům národní bezpečnosti v rámci činností v oblasti signálového zpravodajství, tak k ochraně soukromí <sup>(357)</sup>.
- (181) V rámci svého přezkumu úředník ODNI CLPO určí, zda došlo k porušení platných právních předpisů USA, a pokud ano, rozhodne o vhodné nápravě <sup>(358)</sup>. Ta se týká opatření, která plně napravují zjištěné porušení, jako je ukončení nezákonného získávání údajů, vymazání nezákonně shromážděných údajů, vymazání výsledků nepatřičně provedených dotazů na jinak zákonně shromážděné údaje, omezení přístupu k zákonně shromážděným údajům na příslušně vyskolený personál nebo stažení zpravodajských zpráv obsahujících údaje, které byly získány bez zákonného oprávnění nebo které byly nezákonně šířeny <sup>(359)</sup>. Rozhodnutí úředníka ODNI CLPO o jednotlivých stížnostech (včetně nápravy) jsou pro dotčené zpravodajské služby závazná <sup>(360)</sup>.
- (182) Úředník ODNI CLPO musí vést dokumentaci o svém přezkumu a vypracovat rozhodnutí v důvěrném režimu, v němž vysvětlí základ pro svá skutková zjištění, uvede, zda k dotčenému porušení došlo, a stanoví vhodnou nápravu <sup>(361)</sup>. Pokud přezkum provedený úředníkem ODNI CLPO odhalí porušení některého z oprávnění podléhajících dohledu Soudu pro uplatňování zákona FISA, musí úředník CLPO rovněž předložit zprávu v důvěrném režimu náměstkovi ministra spravedlnosti pro národní bezpečnost, který je následně povinen oznámit nedodržení Soudu pro uplatňování zákona FISA, který může přijmout další donucovací opatření (v souladu s postupem popsaným v 173. až 174. bodě odůvodnění) <sup>(362)</sup>.
- (183) Po dokončení přezkumu úředník ODNI CLPO informuje prostřednictvím vnitrostátního orgánu stěžovatele, že „v přezkumu buď nebylo zjištěno žádné dotčené porušení, nebo že úředník ODNI CLPO vydal rozhodnutí, ve kterém je stanovena povinnost vyžadující vhodnou nápravu“ <sup>(363)</sup>. To umožňuje chránit důvěrnost činností prováděných za účelem ochrany národní bezpečnosti a zároveň poskytnout fyzickým osobám rozhodnutí potvrzující, že jejich stížnost byla řádně prošetřena a vyřízena. Proti tomuto rozhodnutí se navíc může fyzická osoba odvolat. Za tímto účelem bude stěžovatel informován o možnosti podat odvolání k Soudu pro přezkum ochrany údajů, aby přezkoumal rozhodnutí úředníka CLPO (viz 184. a další body odůvodnění), a o tom, že v případě, že by bylo odvolání k soudu podáno, bude vybrán zvláštní advokát, který bude hájit zájmy stěžovatele <sup>(364)</sup>.

<sup>(352)</sup> Ustanovení § 3(c)(iv) výkonného dekretu č. 14086. Viz rovněž zákon o národní bezpečnosti z roku 1947, 50 U.S.C. §403-3d, § 103D týkající se úlohy úředníka CLPO v rámci úřadu ODNI.

<sup>(353)</sup> 50 U.S.C § 3029 (b).

<sup>(354)</sup> Ustanovení § 3(c)(iv) výkonného dekretu č. 14086.

<sup>(355)</sup> Ustanovení § 3(c)(iii) výkonného dekretu č. 14086.

<sup>(356)</sup> Ustanovení § 3(c)(iv) výkonného dekretu č. 14086.

<sup>(357)</sup> Ustanovení § 3(c)(i)(B)(i) a (iii) výkonného dekretu č. 14086.

<sup>(358)</sup> Ustanovení § 3(c)(i) výkonného dekretu č. 14086.

<sup>(359)</sup> Ustanovení § 4(a) výkonného dekretu č. 14086.

<sup>(360)</sup> Ustanovení § 3(c)(d) výkonného dekretu č. 14086.

<sup>(361)</sup> Ustanovení § 3(c)(i)(F)–(G) výkonného dekretu č. 14086.

<sup>(362)</sup> Viz též ustanovení § 3(c)(i)(D) výkonného dekretu č. 14086.

<sup>(363)</sup> Ustanovení § 3(c)(i)(E)(1) výkonného dekretu č. 14086.

<sup>(364)</sup> Ustanovení § 3(c)(i)(E)(2)–(3) výkonného dekretu č. 14086.

- (184) Každý stěžovatel, stejně jako každá složka zpravodajské komunity, může požádat o přezkum rozhodnutí úředníka ODNI CLPO u Soudu pro přezkum ochrany údajů. Takové žádosti o přezkum musí být podány do 60 dnů od přijetí oznámení úředníka ODNI CLPO, že jeho přezkum je ukončen, a musí obsahovat veškeré informace, které chce fyzická osoba Soudu pro přezkum ochrany údajů poskytnout (např. argumenty týkající se právních otázek nebo použití právních předpisů na skutkové okolnosti případu) <sup>(365)</sup>. Subjekty údajů z Unie mohou své žádosti podávat opět příslušnému úřadu pro ochranu osobních údajů (viz 177. bod odůvodnění).
- (185) Soudu pro přezkum ochrany údajů je nezávislý soud zřízený ministrem spravedlnosti na základě výkonného dekretu č. 14086 <sup>(366)</sup>. Skládá se z nejméně šesti soudců, které jmenuje ministr spravedlnosti po konzultaci s výborem PCLOB, ministrem obchodu a ředitelem národních zpravodajských služeb na čtyřleté funkční období, které lze prodloužit <sup>(367)</sup>. Při jmenování soudců ministrem spravedlnosti se vychází z kritérií, která výkonná moc používá při posuzování kandidátů na federální soudce, přičemž se přihlíží k případným předchozím soudním zkušenostem <sup>(368)</sup>. Soudci musí být kromě toho praktikující právní odborníci (tj. aktivní členové komory s dobrou pověstí a řádně oprávnění k výkonu právníkové praxe) a musí mít odpovídající zkušenosti v oblasti práva na ochranu soukromí a národní bezpečnosti. Ministr spravedlnosti musí usilovat o to, aby alespoň polovina soudců měla předchozí soudní praxi, a všichni soudci musí mít bezpečnostní prověrku, aby mohli mít přístup k utajovaným informacím týkajícím se národní bezpečnosti <sup>(369)</sup>.
- (186) Do funkce k Soudu pro přezkum ochrany údajů mohou být jmenovány pouze fyzické osoby, které splňují kvalifikační požadavky uvedené ve 185. bodě odůvodnění a nejsou zaměstnanci výkonné moci v době svého jmenování ani těmito zaměstnanci v předchozích dvou letech nebyly. Stejně tak nesmí mít soudci během svého funkčního období u Soudu pro přezkum ochrany údajů žádné úřední povinnosti ani pracovní poměr u vládních orgánů USA (kromě funkce soudce u Soudu pro přezkum ochrany údajů) <sup>(370)</sup>.
- (187) Nezávislost rozhodovacího procesu je zajištěna řadou záruk. Zejména je zakázáno, aby výkonná moc (ministr spravedlnosti a zpravodajské služby) zasahovala do přezkumu Soudu pro přezkum ochrany údajů nebo jej nepřiměřeně narušovala <sup>(371)</sup>. Samotný Soud pro přezkum ochrany údajů je povinen rozhodovat případy nestranně <sup>(372)</sup>, přičemž se řídí vlastním jednacím řádem (přijatým většinou hlasů). Soudce Soudu pro přezkum ochrany údajů může kromě toho odvolat pouze ministr spravedlnosti, a to pouze na základě zákonného důvodu (tj. v případě pochybení, nesprávného postupu, narušení bezpečnosti, zanedbání povinností nebo nezpůsobilosti), a to po řádném zohlednění norem platných pro federální soudce, které jsou stanoveny v pravidlech pro řízení týkající se chování soudců a jejich nezpůsobilosti <sup>(373)</sup>.
- 
- <sup>(365)</sup> Ustanovení § 201.6(a)–(b) nařízení ministra spravedlnosti.
- <sup>(366)</sup> Ustanovení § 3(d)(i) a nařízení ministra spravedlnosti. Nejvyšší soud Spojených států uznal možnost, aby ministr spravedlnosti zřizoval nezávislé orgány s rozhodovací pravomocí, včetně pravomoci rozhodovat v jednotlivých případech, viz zejména rozsudek ve věci *United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954) a *United States v. Nixon*, 418 U.S. 683, 695 (1974). Dodržování různých požadavků vyplývajících z výkonného dekretu č. 14086, např. kritérií a postupu pro jmenování a odvolání soudců Soudu pro přezkum ochrany údajů, podléhá zejména dohledu generálního inspektora Ministerstva spravedlnosti (viz také 109. bod odůvodnění o zákonné pravomoci generálních inspektorů).
- <sup>(367)</sup> Ustanovení § 3(d)(i)(A) výkonného dekretu č. 14086 a § 201.3(a) nařízení ministra spravedlnosti.
- <sup>(368)</sup> Ustanovení § 201.3(b) nařízení ministra spravedlnosti.
- <sup>(369)</sup> Ustanovení § 3(d)(i)(B) výkonného dekretu č. 14086.
- <sup>(370)</sup> Ustanovení § 3(d)(i)(A) výkonného dekretu č. 14086 a § 201.3(a) a (c) nařízení ministra spravedlnosti. Fyzické osoby jmenované do funkce k Soudu pro přezkum ochrany údajů se mohou podílet na mimosoudních činnostech, včetně podnikání, finančních aktivit, neziskových fundraisingových a fiduciárních činností, jakož i na výkonu právníkové praxe, pokud tyto činnosti nenarušují nestranný výkon jejich povinností nebo účinnost či nezávislost Soudu pro přezkum ochrany údajů (§ 201.7(c) nařízení ministra spravedlnosti).
- <sup>(371)</sup> Ustanovení § 3(d)(iii)–(iv) výkonného dekretu č. 14086 a § 201.7(d) nařízení ministra spravedlnosti.
- <sup>(372)</sup> Ustanovení § 3(d)(i)(D) výkonného dekretu č. 14086 a § 201.9 nařízení ministra spravedlnosti.
- <sup>(373)</sup> Ustanovení § 3(d)(iv) výkonného dekretu č. 14086 a § 201.7(d) nařízení ministra spravedlnosti. Viz také věc *Bumap v. Spojené státy*, 252 U.S. 512, 515 (1920), ve které byla potvrzena dlouholetá zásada v právu USA, že pravomoc odvolávat souvisí s pravomocí jmenovat (jak připomněl také Úřad právního poradce Ministerstva spravedlnosti v dokumentu „*The Constitutional Separation of Powers Between the President and Congress*“, 20 Op. O.L.C. 124, 166 (1996)).

- (188) Žádosti k Soudu pro přezkum ochrany údajů posuzují senáty složené ze tří soudců, včetně předsedy, kteří musí jednat v souladu s Kodexem chování pro soudce USA <sup>(374)</sup>. Každému senátu je nápomocen zvláštní advokát <sup>(375)</sup>, který má přístup ke všem informacím týkajícím se případu, včetně utajovaných informací <sup>(376)</sup>. Úkolem zvláštního advokáta je zajistit, aby byly zastoupeny zájmy stěžovatele a aby byl senát Soudu pro přezkum ochrany údajů dobře informován o všech relevantních právních a skutkových otázkách <sup>(377)</sup>. Zvláštní advokát může za účelem získání bližších informací pro své stanovisko ohledně žádosti o přezkum podané fyzickou osobou Soudu pro přezkum ochrany údajů požádat stěžovatele o informace prostřednictvím písemných otázek <sup>(378)</sup>.
- (189) Soud pro přezkum ochrany údajů přezkoumává rozhodnutí učiněná úředníkem 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 z šetření provedeného úředníkem ODNI CLPO, jakož i na základě veškerých informací a podání poskytnutých stěžovatelem, zvláštním advokátem nebo zpravodajskou službou <sup>(379)</sup>. Senát Soudu pro přezkum ochrany údajů má přístup ke všem informacím potřebným k provedení přezkumu, které může získat prostřednictvím úředníka ODNI CLPO (senát může např. požádat úředníka CLPO o doplnění jeho záznamu o další informace nebo skutková zjištění, pokud je to pro provedení přezkumu nezbytné) <sup>(380)</sup>.
- (190) Při zpracování závěrů přezkumu může Soud pro přezkum ochrany údajů 1) rozhodnout, že neexistují důkazy, které by naznačovaly, že došlo k činnostem v oblasti signálového zpravodajství zahrnujícím osobní údaje stěžovatele, 2) rozhodnout, že zjištění úředníka ODNI CLPO byla právně správná a podložena přesvědčivými důkazy, nebo 3) vydat vlastní rozhodnutí, pokud nesouhlasí se zjištěními úředníka ODNI CLPO (ohledně toho, zda došlo k porušení platných právních předpisů USA, nebo ohledně vhodné nápravy) <sup>(381)</sup>.

<sup>(374)</sup> Ustanovení § 3(d)(i)(B) výkonného dekretu č. 14086 a § 201.7(a)–(c) nařízení ministra spravedlnosti. Úřad pro ochranu soukromí a občanských svobod Ministerstva spravedlnosti (Office of Privacy and Civil Liberties of the Department of Justice, dále také jen „úřad OPCL“), který je odpovědný za poskytování administrativní podpory Soudu pro přezkum ochrany údajů a zvláštním advokátům (viz § 201.5 nařízení ministra spravedlnosti), 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 úřad OPCL vybral jako prvního).

<sup>(375)</sup> Ustanovení § 201.4 nařízení ministra spravedlnosti. Nejméně dva zvláštní advokáti jsou jmenováni ministrem spravedlnosti po konzultaci s ministrem obchodu, ředitelem národních zpravodajských služeb a výborem PCLOB, a to na dobu dvou funkčních období, která lze prodloužit. Zvláštní advokáti musí mít odpovídající zkušenosti v oblasti práva na ochranu soukromí a národní bezpečnosti, musí být zkušenými advokáty, aktivními členy advokátní komory s dobrou pověstí a řádně oprávněnými k výkonu právní praxe. 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 senátu nápomocen, viz § 201.8(a) nařízení ministra spravedlnosti.

<sup>(376)</sup> Ustanovení § 201.8(c) a 201.11 nařízení ministra spravedlnosti.

<sup>(377)</sup> Ustanovení § 3(d)(i)(C) výkonného dekretu č. 14086 a § 201.8(e) nařízení ministra spravedlnosti. Zvláštní advokát nejedná jako zástupce stěžovatele ani s ním nemá vztah advokáta a klienta.

<sup>(378)</sup> Viz ustanovení § 201.8(d)(e) nařízení ministra spravedlnosti. Tyto dotazy nejprve přezkoumá úřad OPCL po konzultaci s příslušnou složkou zpravodajské komunity s cílem identifikovat a vyloučit veškeré utajované nebo důvěrné či chráněné informace před jejich předáním stěžovateli. Další informace, které zvláštní advokát obdrží v reakci na takové otázky, jsou zahrnuty do podání zvláštního advokáta k Soudu pro přezkum ochrany údajů.

<sup>(379)</sup> Ustanovení § 3(d)(i)(D) výkonného dekretu č. 14086.

<sup>(380)</sup> Ustanovení § 3(d)(iii) výkonného dekretu č. 14086 a § 201.9(b) nařízení ministra spravedlnosti.

<sup>(381)</sup> Ustanovení § 3(d)(i)(E) výkonného dekretu č. 14086 a § 201.9(c)–(e) nařízení ministra spravedlnosti. Podle definice pojmu „vhodná náprava“ v § 4(a) výkonného dekretu č. 14086 musí Soud pro přezkum ochrany údajů při rozhodování o nápravném opatření k úplnému vyřešení porušení zohlednit „způsoby, jakými se porušení zjištěného druhu obvykle řešilo“, tj. Soud pro přezkum ochrany údajů mimo jiné zvažuje, jak byly podobné problémy s dodržováním předpisů řešeny v minulosti, aby zajistil, že náprava bude účinná a vhodná.

- (191) V každém případě Soud pro přezkum ochrany údajů přijímá písemné rozhodnutí většinou hlasů. V případě, že přezkum odhalí porušení platných pravidel, v rozhodnutí se uvede případná vhodná náprava, která zahrnuje vymazání nezákonně shromážděných údajů, vymazání výsledků nepatřičně provedených dotazů, omezení přístupu k zákonně shromážděným údajům na příslušně vyškolený personál nebo stažení zpravodajských zpráv obsahujících údaje, které byly získány bez zákonného oprávnění nebo které byly nezákonně šířeny<sup>(382)</sup>. Rozhodnutí Soudu pro přezkum ochrany údajů je závazné a pravomocné, pokud jde o stížnost, která mu byla předložena<sup>(383)</sup>. Pokud přezkum odhalí porušení některého z oprávnění podléhajících dohledu Soudu pro uplatňování zákona FISA, musí Soud pro přezkum ochrany údajů rovněž předložit zprávu v důvěrném režimu náměstkovi ministra spravedlnosti pro národní bezpečnost, který je následně povinen oznámit nedodržení Soudu pro uplatňování zákona FISA, který může přijmout další donucovací opatření (v souladu s postupem popsáním ve 173. až 174. bodě odůvodnění)<sup>(384)</sup>.
- (192) Každé rozhodnutí senátu Soudu pro přezkum ochrany údajů je předáno úředníkovi ODNI CLPO<sup>(385)</sup>. V případech, kdy byl přezkum Soudu pro přezkum ochrany údajů zahájen na základě žádosti stěžovatele, je stěžovatel prostřednictvím vnitrostátního orgánu vyrozuměn o tom, že Soud pro přezkum ochrany údajů přezkum ukončil a že „v přezkumu buď nebylo zjištěno žádné dotčené porušení, nebo že Soud pro přezkum ochrany údajů vydal rozhodnutí, ve kterém je stanovena povinnost vyžadující vhodnou nápravu“<sup>(386)</sup>. Úřad pro ochranu soukromí a občanských svobod Ministerstva spravedlnosti vede záznamy o všech informacích, které Soud pro přezkum ochrany údajů přezkoumal, a o všech vydaných rozhodnutích, které jsou k dispozici jako nezávazný precedens pro budoucí senáty Soudu pro přezkum ochrany údajů<sup>(387)</sup>.
- (193) Ministerstvo obchodu je rovněž povinno vést záznamy o každém stěžovateli, který podal stížnost<sup>(388)</sup>. V zájmu zvýšení transparentnosti musí Ministerstvo obchodu nejméně jednou za pět let kontaktovat příslušné zpravodajské služby, aby ověřilo, zda byly informace týkající se přezkumu provedeného Soudem pro přezkum ochrany údajů odtajněny<sup>(389)</sup>. Pokud tomu tak je, bude dotyčná fyzická osoba informována o tom, že tyto informace mohou být k dispozici podle platných právních předpisů (tj. že může požádat o přístup k těmto informacím podle zákona o svobodném přístupu k informacím, viz 199. bod odůvodnění).
- (194) A konečně, správné fungování tohoto nápravného mechanismu bude předmětem pravidelného a nezávislého hodnocení. Konkrétně, podle výkonného dekretu č. 14086 podléhá fungování nápravného mechanismu každoročnímu přezkumu ze strany výboru PCLOB, nezávislého orgánu (viz 110. bod odůvodnění)<sup>(390)</sup>. V rámci tohoto přezkumu bude výbor PCLOB mimo jiné posuzovat, zda úředník ODNI CLPO a Soud pro přezkum ochrany údajů vyřizují stížnosti včas; zda získaly úplný přístup k potřebným informacím; zda byly v procesu přezkumu řádně zohledněny hmotněprávní záruky stanovené ve výkonném dekretu č. 14086 a zda zpravodajská komunita plně dodržela rozhodnutí úředníka ODNI CLPO a Soudu pro přezkum ochrany údajů. Výbor PCLOB vypracuje zprávu o výsledku svého přezkumu určenou prezidentovi, ministru spravedlnosti, řediteli národních zpravodajských služeb, vedoucím zpravodajských služeb, úředníkovi ODNI CLPO a výborům Kongresu pro zpravodajství, která bude rovněž zveřejněna v neutajované verzi – a následně bude podkladem pro pravidelný přezkum fungování tohoto rozhodnutí, který bude provádět Komise. Ministr spravedlnosti, ředitel národních zpravodajských služeb, úředník ODNI CLPO a vedoucí zpravodajských služeb jsou povinni provést nebo jinak řešit všechna doporučení obsažená v těchto zprávách. Kromě toho bude výbor PCLOB každoročně vydávat veřejné osvědčení o tom, zda nápravný mechanismus vyřizuje stížnosti v souladu s požadavky výkonného dekretu č. 14086.

<sup>(382)</sup> Ustanovení § 4(a) výkonného dekretu č. 14086.

<sup>(383)</sup> Ustanovení § 3(d)(ii) výkonného dekretu č. 14086 a § 201.9(g) nařízení ministra spravedlnosti. Vzhledem k tomu, že rozhodnutí Soudu pro přezkum ochrany údajů je pravomocné a závazné, nemůže žádný jiný výkoný nebo správní orgán (včetně prezidenta Spojených států) rozhodnutí Soudu pro přezkum ochrany údajů zrušit. To potvrdila i judikatura Nejvyššího soudu, která objasnila, že delegováním jedinečné pravomoci ministra spravedlnosti v rámci výkonné moci vydávat závazná rozhodnutí na nezávislý orgán se ministr spravedlnosti sám zbavuje možnosti jakkoli nařizovat rozhodnutí tohoto orgánu (viz věc *United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954)).

<sup>(384)</sup> Ustanovení § 3(d)(i)(F) výkonného dekretu č. 14086 a § 201.9(i) nařízení ministra spravedlnosti.

<sup>(385)</sup> Ustanovení § 201.9(h) nařízení ministra spravedlnosti.

<sup>(386)</sup> Ustanovení § 3(d)(i)(H) výkonného dekretu č. 14086 a § 201.9(h) nařízení ministra spravedlnosti. Pokud jde o povahu oznámení, viz § 201.9 (h)(3) nařízení ministra spravedlnosti.

<sup>(387)</sup> Ustanovení § 201.9(j) nařízení ministra spravedlnosti.

<sup>(388)</sup> Ustanovení § 3(d)(v)(A) výkonného dekretu č. 14086.

<sup>(389)</sup> Ustanovení § 3(d)(v) výkonného dekretu č. 14086.

<sup>(390)</sup> Ustanovení § 3(e) výkonného dekretu č. 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](https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf)

- (195) Kromě zvláštního nápravného mechanismu zřízeného podle výkonného dekretu č. 14086 jsou všem fyzickým osobám (bez ohledu na jejich státní příslušnost nebo bydliště) k dispozici i možnosti nápravy před obecnými soudy USA <sup>(391)</sup>.
- (196) Zákon FISA a související zákon poskytuje fyzickým osobám především možnost domáhat se občanskoprávními žalobami proti Spojeným státům peněžité náhrady škody v případě, kdy informace o nich byly použity nebo zveřejněny nezákonně a vědomě <sup>(392)</sup>; žalovat úředníky vlády USA jednající za svou osobu o peněžitou náhradu škody <sup>(393)</sup> a napadnout zákonnost sledování (a domáhat se utajení informací) v případě, kdy vláda USA hodlá použít nebo zveřejnit informace získané nebo odvozené z elektronického sledování proti fyzické osobě v soudním nebo správním řízení v USA <sup>(394)</sup>. V obecné rovině, pokud vláda hodlá použít informace získané během zpravodajských operací proti podezřelému v trestním řízení, ústavní a zákonné požadavky <sup>(395)</sup> ukládají povinnost zpřístupnit určité informace, aby obžalovaný mohl napadnout zákonnost shromažďování a použití důkazů vládou.
- (197) Kromě toho existuje několik zvláštních možností, jak se domáhat právního postihu vůči vládním úředníkům za nezákonný přístup vlády k osobním údajům nebo jejich nezákonné použití, mimo jiné k účelům národní bezpečnosti (tj. zákon o počítačových podvodech a zneužití počítače (Computer Fraud and Abuse Act) <sup>(396)</sup>; zákon o soukromí elektronických komunikací (Electronic Communications Privacy Act) <sup>(397)</sup> a zákon o právu na finanční soukromí (Right to Financial Privacy Act) <sup>(398)</sup>). Všechny tyto právní kroky se týkají konkrétních údajů, cílů a/nebo typů přístupu (např. vzdálený přístup k počítači prostřednictvím internetu) a jsou dostupné za určitých podmínek (např. úmyslné/vědomé jednání, zneužití úřední pravomoci, vznik škody).
- (198) Obecnější možnost nápravy nabízí zákon o správním řízení (Administrative Procedure Act, APA) <sup>(399)</sup>, podle kterého „kdokoli, jemuž krok agentury způsobí právní křivdu nebo kdo je krokem agentury negativně postižen nebo poškozen,“ má právo domáhat se soudního přezkumu <sup>(400)</sup>. Sem spadá možnost požádat soud, „aby prohlásil za neplatné nebo zrušil krok, zjištění a závěry agentury, které byly shledány [...] aktem svévole či zvlé, zneužitím diskreční pravomoci či jinak v rozporu se zákonem“ <sup>(401)</sup>. V roce 2015 rozhodl například federální odvolací soud na základě žaloby podle zákona o správním řízení, že hromadný sběr metadat o telefonních hovorech americkou vládou nebyl podle § 501 zákona FISA povolen <sup>(402)</sup>.
- 
- <sup>(391)</sup> Přístup k těmto možnostem je podmíněn prokázáním „aktivní legitimity“. Tento standard, který se vztahuje na všechny fyzické osoby bez ohledu na státní příslušnost, vychází z požadavku „case or controversy“ podle článku III Ústavy USA. Podle Nejvyššího soudu to vyžaduje, aby 1) fyzická osoba utrpěla „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) bylo pravděpodobné, nikoli spekulativní, že příznivé rozhodnutí soudu tuto újmu napraví (viz věc *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992)).
- <sup>(392)</sup> 18 U.S.C. § 2712.
- <sup>(393)</sup> 50 U.S.C. § 1810.
- <sup>(394)</sup> 50 U.S.C. § 1806.
- <sup>(395)</sup> Viz věc *Brady v. Maryland*, 373 U.S. 83 (1963), resp. Jencksův zákon, 18 U.S.C. § 3500.
- <sup>(396)</sup> 18 U.S.C. § 1030.
- <sup>(397)</sup> 18 U.S.C. § 2701–2712.
- <sup>(398)</sup> 12 U.S.C. § 3417.
- <sup>(399)</sup> 5 U.S.C. § 702.
- <sup>(400)</sup> Soudnímu přezkumu podléhá obecně jen „konečný“, nikoli „předběžný, procesní nebo zprostředkovací“ úkon agentury. Viz 5 U.S.C. § 704.
- <sup>(401)</sup> 5 U.S.C. § 706(2)(A).
- <sup>(402)</sup> Věc *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.

- (199) A konečně, kromě možností nápravy uvedených v 176. až 198. bodě odůvodnění má každá fyzická osoba právo žádat o přístup k existujícím záznamům federální služby podle zákona FOIA, a to i v případě, že obsahují osobní údaje dané fyzické osoby <sup>(403)</sup>. Získání takového přístupu může rovněž usnadnit zahájení řízení před obecnými soudy, a to i na podporu prokázání aktivní legitimace. Zpravodajské služby mohou odepřít informace, které spadají pod určité vyjmenované výjimky, včetně přístupu k utajovaným informacím o národní bezpečnosti a informacím týkajícím se vyšetřování donucovacích orgánů <sup>(404)</sup>, ale stěžovatelé, kteří nejsou s odpovědí spokojeni, mají možnost ji napadnout žádostí o správní a následně soudní přezkum (před federálními soudy) <sup>(405)</sup>.
- (200) Z výše uvedeného vyplývá, že pokud donucovací orgány a národní bezpečnostní orgány USA přistupují k osobním údajům spadajícím do oblasti působnosti tohoto rozhodnutí, řídí se takový přístup právním rámcem, který stanoví podmínky, za nichž může přístup probíhat, a je zajištěno, aby byly přístup a další využívání údajů omezeny na to, co je nezbytné a přiměřené sledovaným cílům v oblasti veřejného zájmu. Těchto záruk se mohou dovolávat fyzické osoby, které mají právo na účinnou nápravu.

#### 4. ZÁVĚR

- (201) Komise se domnívá, že Spojené státy – prostřednictvím zásad vydaných Ministerstvem obchodu USA – zajišťují úroveň ochrany osobních údajů předávaných z Unie certifikovaným organizacím ve Spojených státech na základě rámce EU–USA pro ochranu údajů, která je v zásadě rovnocenná úrovni zaručené nařízením (EU) 2016/679.
- (202) Komise se navíc domnívá, že účinné uplatňování zásad je zaručeno povinnostmi transparentnosti a správou rámce pro ochranu údajů ze strany Ministerstva obchodu. Kromě toho mechanismy dohledu a možnosti nápravy v právu USA jako celek umožňují, aby bylo porušení pravidel ochrany údajů v praxi zjištěno a potrestáno, a nabízejí právní prostředky nápravy tak, aby subjekt údajů získal přístup k osobním údajům, které se ho týkají, a aby mohly být tyto údaje opraveny nebo vymazány.
- (203) 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 na základě rámce EU–USA pro ochranu údajů, který je činěn ve veřejném zájmu, zejména pro účely prosazování trestního práva a národní bezpečnosti, bude 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 ve světle Listiny základních práv Evropské unie, pro osobní údaje předávané z Evropské unie organizacím certifikovaným na základě rámce EU–USA pro ochranu údajů.
- (204) Vzhledem k tomu, že omezení, záruky a nápravné mechanismy stanovené výkonným dekretem č. 14086 jsou základními prvky právního rámce Spojených států, z něhož vychází posouzení Komise, je přijetí tohoto rozhodnutí založeno zejména na přijetí aktualizovaných politik a postupů k provedení výkonného dekretu č. 14086 všemi zpravodajskými službami Spojených států a určení Unie jako kvalifikované organizace pro účely nápravného mechanismu, k čemuž došlo dne 3. července 2023 (viz 126. bod odůvodnění) a 30. června 2023 (viz 176. bod odůvodnění).

<sup>(403)</sup> 5 U.S.C. § 552. Podobné zákony existují na úrovni jednotlivých federálních států USA.

<sup>(404)</sup> Jedná-li se o takový případ, obdrží fyzická osoba zpravidla jen standardní odpověď, kterou agentura odmítá jak potvrdit, tak popřít, že takové záznamy existují. Viz věc *ACLU v CIA*, 710 F.3d 422 (D.C. Cir. 2014). Kritéria a doba trvání utajení jsou stanoveny ve výkonném dekretu č. 13526, který obecně stanoví, že na základě doby trvání citlivosti informací z hlediska národní bezpečnosti musí být stanoveno konkrétní datum nebo událost pro odtajnění, kdy musí být informace automaticky odtajněna (viz § 1.5 výkonného dekretu č. 13526).

<sup>(405)</sup> Soud nově rozhoduje, zda jsou záznamy odpírány dle předpisů a může vládě nařídít jejich zpřístupnění (5 U.S.C § 552(a)(4)(B)).

## 5. ÚČINKY TOHOTO ROZHODNUTÍ A ČINNOST ÚŘADŮ PRO OCHRANU OSOBNÍCH ÚDAJŮ

- (205) Členské státy a jejich orgány musí přijmout opatření nezbytná k dosažení souladu s akty orgánů Unie, neboť jim v zásadě svědčí presumpce legality, a tudíž zakládají právní účinky tak dlouho, dokud nejsou vzaty zpět, zrušeny v rámci žaloby na neplatnost nebo prohlášeny za neplatné v návaznosti na žádost o rozhodnutí o předběžné otázce nebo na námitku protiprávnosti.
- (206) V důsledku toho je rozhodnutí Komise o odpovídající ochraně podle čl. 45 odst. 3 nařízení (EU) 2016/679 závazné pro všechny orgány členských států, kterým je určeno, a to i pro nezávislé dozorové úřady. Zejména může docházet k předáním od správce nebo zpracovatele v Unii certifikovaným organizacím ve Spojených státech, aniž by bylo nutné získat další povolení.
- (207) Je třeba připomenout, že podle čl. 58 odst. 5 nařízení (EU) 2016/679 a podle vysvětlení Soudního dvora v rozsudku ve věci Schrems <sup>(406)</sup>, jestliže vnitrostátní úřad pro ochranu osobních údajů zpochybňuje, a to i na základě stížnosti, slučitelnost rozhodnutí Komise o odpovídající ochraně se základními právy fyzické osoby na soukromí a ochranu údajů, musí mu vnitrostátní právo poskytnout procesní prostředek, který mu umožní uplatnit tyto výtky před vnitrostátním soudem, který může být povinen předložit Soudnímu dvoru žádost o rozhodnutí o předběžné otázce <sup>(407)</sup>.

## 6. MONITOROVÁNÍ A PŘEZKUM TOHOTO ROZHODNUTÍ

- (208) Podle judikatury Soudního dvora <sup>(408)</sup> a podle čl. 45 odst. 4 nařízení (EU) 2016/679 by Komise po přijetí rozhodnutí o odpovídající ochraně měla neustále sledovat příslušný vývoj ve třetí zemi, aby mohla posoudit, zda třetí země stále zajišťuje v zásadě rovnocennou úroveň ochrany. Takové ověřování je každopádně závazné tehdy, když Komise obdrží informace vyvolávající v tomto ohledu určité odůvodněné pochybnosti.
- (209) Komise by tedy měla průběžně sledovat situaci ve Spojených státech, pokud jde o právní rámec a skutečnou praxi zpracování osobních údajů, jak jsou posouzeny v tomto rozhodnutí. Aby tento proces usnadnily, měly by orgány USA neprodleně informovat Komisi o důležitých změnách právního řádu USA, které mají dopad na právní rámec, jenž je předmětem tohoto rozhodnutí, jakož i o vývoji postupů souvisejících se zpracováním osobních údajů, které jsou posuzovány v tomto rozhodnutí, a to jak z hlediska zpracování osobních údajů certifikovanými organizacemi ve Spojených státech, tak z hlediska omezení a záruk použitelných na přístup orgánů veřejné moci k osobním údajům.
- (210) Aby Komise navíc mohla účinně plnit svou kontrolní funkci, měly by ji členské státy informovat o veškerých relevantních krocích vnitrostátních úřadů pro ochranu osobních údajů, zejména v souvislosti s dotazy nebo stížnostmi subjektů údajů z Unie týkajícími se předávání osobních údajů z Unie certifikovaným organizacím ve Spojených státech. Komise by rovněž měla být informována o jakýchkoli známkách toho, že kroky orgánů veřejné moci USA odpovědných za prevenci, vyšetřování, odhalování nebo stíhání trestných činů nebo za národní bezpečnost, včetně jakýchkoli orgánů dohledu, nezajišťují požadovanou úroveň ochrany.

<sup>(406)</sup> Rozsudek ve věci Schrems, bod 65.

<sup>(407)</sup> Rozsudek ve věci Schrems, bod 65: „V tomto ohledu přísluší vnitrostátnímu normotvůrci, aby stanovil procesní prostředky, které by dotyčnému vnitrostátnímu orgánu dozoru umožnily uplatnit výtky, jež považuje za opodstatněné, před vnitrostátními soudy, aby tyto soudy v případě, že sdílejí pochybnosti vyjádřené tímto orgánem ohledně platnosti rozhodnutí Komise, předložily žádost o rozhodnutí o předběžné otázce za účelem přezkumu platnosti tohoto rozhodnutí.“

<sup>(408)</sup> Rozsudek ve věci Schrems, bod 76.

- (211) V souladu s čl. 45 odst. 3 nařízení (EU) 2016/679 <sup>(409)</sup> by Komise po přijetí tohoto rozhodnutí měla pravidelně přezkoumávat, zda zjištění týkající se odpovídající úrovně ochrany zajištěné Spojenými státy na základě rámce EU–USA pro ochranu údajů jsou i nadále skutkově i právně podložena. Vzhledem k tomu, že zejména výkonný dekret č. 14086 a nařízení ministra spravedlnosti stanoví povinnost vytvoření nových mechanismů a zavedení nových záruk, 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 Komise v úzké konzultaci s výborem zřízeným podle čl. 93 odst. 1 nařízení (EU) 2016/679 a Evropským sborem pro ochranu osobních údajů rozhodne o pravidelnosti budoucích přezkumů <sup>(410)</sup>.
- (212) Za účelem provedení přezkumů by se Komise měla sejit s Ministerstvem obchodu, Federální obchodní komisí a Ministerstvem dopravy, případně za účasti dalších útvarů a služeb zapojených do provádění rámce EU–USA pro ochranu údajů, jakož i pokud jde o záležitosti týkající se přístupu vlády k údajům, se zástupci Ministerstva spravedlnosti, Úřadu ředitele národních zpravodajských služeb (včetně úředníka CLPO), dalších složek zpravodajské komunity, Soudu pro přezkum ochrany údajů a zvláštních advokátů. Účast na této schůzce by měla být otevřena zástupcům členů Evropského sboru pro ochranu osobních údajů.
- (213) Přezkumy by měly zahrnovat všechny aspekty fungování tohoto rozhodnutí, pokud jde o zpracování osobních údajů ve Spojených státech, a zejména uplatňování a provádění zásad, přičemž zvláštní pozornost by měla být věnována ochraně poskytované v případě dalšího předávání; vývoji relevantní judikatury; účinnosti výkonu individuálních práv; sledování a prosazování souladu se zásadami; jakož i omezením a zárukám, pokud jde o přístup orgánů státní správy, především provádění a uplatňování záruk zavedených výkonným dekretem č. 14086, a to i prostřednictvím politik a postupů vypracovaných zpravodajskými službami; vzájemnému vztahu mezi výkonným dekretem č. 14086 a § 702 zákona FISA a výkonným dekretem č. 12333; a účinnosti dozorových mechanismů a možností nápravy (včetně fungování nového nápravného mechanismu zřízeného podle výkonného dekretu č. 14086). V souvislosti s těmito přezkumy se pozornost zaměří také na spolupráci mezi úřady pro ochranu osobních údajů a příslušnými orgány Spojených států, včetně tvorby pokynů a vývoje dalších výkladových nástrojů týkajících se uplatňování zásad, jakož i dalších aspektů fungování tohoto rámce.
- (214) Na základě přezkumu by Komise měla připravit veřejně přístupnou zprávu, kterou předloží Evropskému parlamentu a Radě.

## 7. POZASTAVENÍ POUŽITELNOSTI, ZRUŠENÍ NEBO ZMĚNA TOHOTO ROZHODNUTÍ

- (215) Pokud z dostupných informací, zejména z informací vyplývajících ze sledování tohoto rozhodnutí nebo poskytnutých orgány USA nebo členských států, vyplýne, že úroveň ochrany poskytovaná údajům předávaným na základě tohoto rozhodnutí již nemusí být odpovídající, měla by Komise urychleně informovat příslušné orgány USA a požadovat, aby byla ve stanovené a přiměřené lhůtě přijata vhodná opatření.
- (216) Pokud po uplynutí stanovené lhůty příslušné orgány USA tato opatření nepřijmou nebo jiným způsobem uspokojivě neprokážou, že toto rozhodnutí je nadále založeno na odpovídající úrovni ochrany, zahájí Komise postup podle čl. 93 odst. 2 nařízení (EU) 2016/679 s cílem částečně nebo úplně zrušit toto rozhodnutí nebo pozastavit jeho použitelnost.
- (217) Alternativně Komise tento postup zahájí s cílem změnit toto rozhodnutí, zejména tím, že se na předávání údajů budou vztahovat další podmínky nebo že se omezí oblasti působnosti zjištění o odpovídající úrovni ochrany jen na předávání údajů, u nichž je odpovídající úroveň ochrany nadále zaručena.

<sup>(409)</sup> Podle čl. 45 odst. 3 nařízení (EU) 2016/679 „[u]vedený prováděcí akt stanoví mechanismus pro pravidelný přezkum [...], který zohlední veškerý relevantní vývoj v dotčené třetí zemi nebo mezinárodní organizaci“.

<sup>(410)</sup> V čl. 45 odst. 3 nařízení (EU) 2016/679 se stanoví, že pravidelný přezkum se musí provádět „nejméně každé čtyři roky“. Viz také Evropský sbor pro ochranu osobních údajů, Referenční rámec pro odpovídající ochranu, WP 254 rev. 01.

- (218) Komise by měla zahájit postup vedoucí k pozastavení použitelnosti nebo zrušení zejména v případě:
- a) náznaků, že organizace, které obdržely osobní údaje z Unie podle tohoto rozhodnutí, nedodržují zásady a že tento nesoulad není účinně řešen příslušnými orgány dohledu a donucovacími orgány;
  - b) náznaků, že orgány USA nedodržují platné podmínky a omezení pro přístup orgánů veřejné moci USA pro účely prosazování práva a národní bezpečnosti k osobním údajům předávaným na základě rámce EU–USA pro ochranu údajů, nebo
  - c) neúčinného řešení stížností subjektů údajů z Unie, a to i ze strany úředníka ODNI CLPO a/nebo Soudu pro přezkum ochrany údajů.
- (219) Komise by rovněž měla zvážit zahájení postupu vedoucího ke změně, pozastavení použitelnosti nebo zrušení tohoto rozhodnutí, pokud příslušné orgány USA neposkytnou informace nebo objasnění, jež jsou nezbytné k posouzení úrovně ochrany poskytované osobním údajům předávaným z Unie do Spojených států nebo dodržování tohoto rozhodnutí. V tomto směru by Komise měla vzít v potaz míru, do jaké lze relevantní informace získat z jiných zdrojů.
- (220) V závažných, naléhavých a řádně odůvodněných případech, například pokud by výkonný dekret č. 14086 nebo nařízení ministra spravedlnosti byly změněny způsobem, který by oslabil úroveň ochrany popsanou v tomto rozhodnutí, nebo pokud by určení Unie jako kvalifikované organizace pro účely nápravného mechanismu, jež učinil ministr spravedlnosti, bylo odvoláno, využije Komise možnost přijmout postupem podle čl. 93 odst. 3 nařízení (EU) 2016/679 okamžitě použitelné prováděcí akty, kterými se toto rozhodnutí zruší, změni nebo se dočasně pozastaví jeho použitelnost.

## 8. ZÁVĚREČNÉ ÚVAHY

- (221) Evropský sbor pro ochranu osobních údajů zveřejnil své stanovisko <sup>(411)</sup>, které bylo při přípravě tohoto rozhodnutí zohledněno.
- (222) Evropský parlament přijal usnesení o odpovídající ochraně poskytované rámcem EU–USA pro ochranu údajů <sup>(412)</sup>.
- (223) Opatření stanovená tímto rozhodnutím jsou v souladu se stanoviskem 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 „seznamu organizací rámce pro ochranu údajů“, který vede a zveřejňuje Ministerstvo obchodu USA v souladu s oddílem I bodem 3 přílohy I.

### Článek 2

Pokud příslušné orgány v členských státech za účelem ochrany fyzických osob s ohledem na zpracování jejich osobních údajů uplatní pravomoc podle článku 58 nařízení (EU) 2016/679, pokud jde o předávání údajů uvedené v článku 1 tohoto rozhodnutí, oznámí dotýcný členský stát tuto skutečnost bezodkladně Komisi.

<sup>(411)</sup> Stanovisko č. 5/2023 k návrhu prováděcího rozhodnutí Evropské komise o odpovídající ochraně osobních údajů podle rámce EU–USA pro ochranu údajů ze dne 28. února 2023.

<sup>(412)</sup> Usnesení Evropského parlamentu ze dne 11. května 2023 o odpovídající ochraně poskytované rámcem EU–USA pro ochranu údajů (2023/2501(RSP)).

### Článek 3

1. Komise neustále sleduje uplatňování právního rámce, který je předmětem tohoto rozhodnutí, včetně podmínek, za kterých dochází k dalšímu předávání, výkonu individuálních práv a přístupu orgánů veřejné moci USA k údajům předaným na základě tohoto rozhodnutí, s cílem posoudit, zda Spojené státy i nadále zajišťují odpovídající úroveň ochrany ve smyslu článku 1.
2. Členské státy a Komise se vzájemně informují o případech, kdy se jeví, že subjekty ve Spojených státech se zákonnou pravomocí prosazovat dodržování zásad uvedených v příloze I neposkytují účinné mechanismy odhalování a dohledu, jež by v praxi umožňovaly odhalovat a postihovat případy porušení zásad uvedených v příloze I.
3. Členské státy a Komise se vzájemně informují o jakýchkoli známkách toho, že zásahy orgánů veřejné moci USA odpovědných za zajišťování národní bezpečnosti, prosazování práva nebo jiné veřejné zájmy do práva fyzických osob na ochranu jejich osobních údajů přesahují rámec toho, co je nezbytné a přiměřené, a/nebo že proti takovým zásahům není účinná právní ochrana.
4. Po uplynutí jednoho roku ode dne oznámení tohoto rozhodnutí členským státům a poté s pravidelností, o níž bude rozhodnuto v úzké konzultaci s výborem zřízeným podle čl. 93 odst. 1 nařízení (EU) 2016/679 a Evropským sborem pro ochranu údajů, Komise vyhodnotí zjištění uvedené v čl. 1 odst. 1 na základě veškerých dostupných informací, včetně informací získaných v rámci přezkumu provedeného společně s příslušnými orgány Spojených států.
5. Pokud má Komise informace o tom, že odpovídající úroveň ochrany již není zajištěna, informuje příslušné orgány USA. Případně rozhodne o pozastavení použitelnosti, změně nebo zrušení tohoto rozhodnutí nebo o omezení jeho působnosti podle čl. 45 odst. 5 nařízení (EU) 2016/679. Komise může takové rozhodnutí přijmout také v případě, kdy nedostatečná spolupráce vlády USA brání Komisi v určení toho, zda Spojené státy i nadále zajišťují odpovídající úroveň ochrany.

### Článek 4

Toto rozhodnutí je určeno členským státům.

V Bruselu dne 10. července 2023

*Za Komisi*  
Didier REYNDERS  
*člen Komise*

## PŘÍLOHA I

## ZÁSADY RÁMCE EU–USA PRO OCHRANU ÚDAJŮ VYDANÉ MINISTERSTVEM OBCHODU USA

## I. PŘEHLED

1. Ačkoli Spojené státy a Evropská unie (dále jen „EU“) mají společný závazek posílit ochranu soukromí, právní stát a uznat význam transatlantických toků údajů k našim občanům, ekonomikám a společnostem, Spojené státy uplatňují jiný přístup k ochraně soukromí než EU. Spojené státy uplatňují odvětvový přístup, který je založen na kombinaci právních předpisů, regulace a samoregulace. Ministerstvo obchodu USA (dále jen „ministerstvo“) vydává zásady rámce EU–USA pro ochranu údajů, včetně doplňkových zásad (společně dále jen „zásady“) a přílohy I zásad (dále jen „příloha I“), v rámci 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“), odvětvím a dalšími zúčastněnými stranami s cílem usnadnit obchod mezi Spojenými státy a EU. Zásady, které jsou klíčovou součástí rámce EU–USA pro ochranu údajů, poskytují organizacím ve Spojených státech spolehlivý mechanismus pro předávání osobních údajů z EU do Spojených států a zároveň zajišťují, aby subjekty údajů z EU i nadále požívaly účinných záruk a ochrany, jak vyžadují evropské právní předpisy, pokud jde o zpracování jejich osobních údajů, jestliže byly předány do zemí mimo EU. Zásady jsou určeny výhradně k použití způsobilými organizacemi ve Spojených státech, které získávají osobní údaje z EU, aby mohly splnit podmínky pro účast v rámci EU–USA pro ochranu údajů, a tím i využívat výhod rozhodnutí Komise o odpovídající ochraně<sup>(1)</sup>. Těmito zásadami není dotčeno uplatňování nařízení (EU) 2016/679 (dále jen „obecné nařízení o ochraně osobních údajů“ nebo „GDPR“) (<sup>2</sup>), které se vztahuje na zpracování osobních údajů v členských státech EU. Zásady také neomezuji povinnosti chránit soukromí, které jinak platí podle práva Spojených států.
2. Aby se organizace mohla spolehnout na rámec EU–USA pro ochranu údajů, pokud jde o předávání osobních údajů z EU, musí se u ministerstva (nebo jeho zmocněnce) autocertifikovat, že dodržuje tyto zásady. Ačkoli rozhodnutí organizací o vstupu do rámce EU–USA pro ochranu údajů jsou zcela dobrovolná, účinné dodržování zásad je povinné: organizace, které se u ministerstva autocertifikují a veřejně deklarují svůj závazek dodržovat zásady, musí tyto zásady dodržovat plně. Pro vstup do rámce EU–USA pro ochranu údajů musí organizace a) podléhat vyšetřovacím a donucovacím pravomocem Federální obchodní komise, Ministerstva dopravy USA nebo jiného subjektu zřízeného zákonem, který účinně zajistí dodržování zásad (*v budoucnu mohou být přílohou zařazeny další subjekty USA zřízené zákonem a uznané EU*); b) veřejně deklarovat svůj závazek dodržovat zásady; c) zveřejnit své politiky ochrany soukromí v souladu s těmito zásadami a d) plně je provést (<sup>3</sup>). Neplnění povinností ze strany organizace je vymahatelné Federální obchodní komisí podle § 5 zákona o Federální obchodní komisi, který zakazuje nekalé nebo klamavé praktiky při obchodování či nekalé nebo klamavé praktiky, které na obchodování dopadají (15 U.S.C. § 45); Ministerstvem dopravy podle 49 U.S.C. § 41712, který zakazuje dopravci nebo zprostředkovateli letenek, aby se v letecké dopravě nebo prodeji letecké dopravy dopouštěli nekalé nebo klamavé praktiky, nebo podle jiných právních předpisů zakazujících takové činy.

(<sup>1</sup>) Za předpokladu, že se rozhodnutí Komise o odpovídající ochraně poskytované rámcem EU–USA pro ochranu údajů vztahuje na Island, Lichtenštejnsko a Norsko, bude se rámec EU–USA pro ochranu údajů vztahovat jak na EU, tak na tyto tři země. Odkazy na EU a její členské státy se proto považují rovněž za odkazy na Island, Lichtenštejnsko a Norsko.

(<sup>2</sup>) 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).

(<sup>3</sup>) Rámcové zásady štítu EU–USA na ochranu soukromí byly změněny na „Zásady rámce EU–USA pro ochranu údajů“. (Viz doplňková zásada autocertifikace).

3. Ministerstvo povede a zpřístupní veřejnosti oficiální seznam organizací z USA, které se u ministerstva autocertifikovaly a oznámily svůj závazek dodržovat zásady (dále jen „seznam organizací rámce pro ochranu údajů“). Výhody rámce EU–USA pro ochranu údajů jsou zajištěny ode dne, kdy ministerstvo zařadí organizaci na seznam organizací rámce pro ochranu údajů. Ministerstvo odstraní ze seznamu organizací rámce pro ochranu údajů ty organizace, které dobrovolně z rámce EU–USA pro ochranu údajů vystoupí nebo nedokončí každoroční opětovnou certifikaci u ministerstva; tyto organizace musí buď nadále uplatňovat zásady na osobní informace, které obdržely na základě rámce EU–USA pro ochranu údajů, a každoročně potvrdit ministerstvu svůj závazek tak učinit (tj. po dobu, po kterou tyto informace uchovávají), poskytovat těmto informacím „odpovídající“ ochranu jinými schválenými prostředky (například prostřednictvím smlouvy, která plně odráží požadavky příslušných standardních smluvních doložek přijatých Komisí), nebo je vrátit či vymazat. Ministerstvo rovněž odstraní ze seznamu organizací rámce pro ochranu údajů ty organizace, které soustavně zásady nedodržují; tyto organizace musí vrátit nebo vymazat osobní informace, které obdržely na základě rámce EU–USA pro ochranu údajů. Odstranění organizace ze seznamu organizací rámce pro ochranu údajů znamená, že již není oprávněna využívat výhod rozhodnutí Komise o odpovídající ochraně za účelem přijímání osobních informací z EU.
4. Ministerstvo rovněž povede a zpřístupní veřejnosti oficiální záznam organizací z USA, které se předtím u ministerstva autocertifikovaly, ale které byly odstraněny ze seznamu organizací rámce pro ochranu údajů. Ministerstvo poskytne jasné upozornění, že tyto organizace již nejsou účastníky rámce EU–USA pro ochranu údajů; že odstranění ze seznamu organizací rámce pro ochranu údajů znamená, že tyto organizace již nemohou tvrdit, že dodržují rámec EU–USA pro ochranu údajů, a musí se vyvarovat jakýchkoli prohlášení nebo zavádějících postupů, které by naznačovaly, že se rámce EU–USA pro ochranu údajů účastní; a že tyto organizace již nejsou oprávněny využívat výhod rozhodnutí Komise o odpovídající ochraně za účelem přijímání osobních informací z EU. Organizace, která i po odstranění ze seznamu organizací rámce pro ochranu údajů nadále tvrdí, že se rámce EU–USA pro ochranu údajů účastní, nebo činí jiná nepravdivá prohlášení týkající se rámce EU–USA pro ochranu údajů, může být předmětem donucovacích opatření ze strany Federální obchodní komise, Ministerstva dopravy nebo jiných donucovacích orgánů.
5. Dodržování těchto zásad může být omezeno: a) v rozsahu nezbytném pro splnění soudního příkazu nebo splnění požadavků veřejného zájmu, prosazování práva nebo národní bezpečnosti, včetně případů, kdy ze zákona nebo nařízení vlády vyplývají protichůdné povinnosti; b) zákonem, soudním příkazem nebo nařízením vlády, které vytvářejí výslovné oprávnění, za předpokladu, že při výkonu takového oprávnění může organizace prokázat, že nedodržování zásad je omezeno na rozsah nezbytný k uspokojení převažujících oprávněných zájmů podpořených tímto oprávněním, nebo c) pokud má obecné nařízení o ochraně osobních údajů za podmínek v něm stanovených umožnit výjimky nebo odchylky za předpokladu, že se tyto výjimky nebo odchylky uplatňují ve srovnatelných souvislostech. V této souvislosti zahrnují záruky stanovené v právních předpisech USA na ochranu soukromí a občanských svobod záruky požadované výkonným dekretem č. 14086 <sup>(4)</sup> za podmínek v něm stanovených (včetně jeho požadavků nezbytnosti a přiměřenosti). V souladu s cílem posílit ochranu soukromí by organizace měly usilovat o úplné a transparentní provádění těchto zásad, a to i tím, že se ve svých politikách ochrany soukromí budou snažit uvádět, kde se uplatní výjimky ze zásad povolené podle písmene b). Z téhož důvodu se očekává, že pokud podle těchto zásad nebo práva Spojených států existuje možnost volby, organizace zvolí pokud možno vyšší úroveň ochrany.
6. Organizace jsou povinny uplatňovat zásady na všechny osobní údaje předávané v režimu rámce EU–USA pro ochranu údajů po svém vstupu do rámce EU–USA pro ochranu údajů. Organizace, která se rozhodne rozšířit výhody plynoucí z rámce EU–USA pro ochranu údajů na osobní informace týkající se lidských zdrojů předávané z EU pro účely využití v rámci zaměstnaneckých vztahů, musí tuto skutečnost oznámit při autocertifikaci u ministerstva a musí splnit požadavky uvedené v doplňkové zásadě autocertifikace.

<sup>(4)</sup> Výkonný dekret ze dne 7. října 2022, „Posílení záruk pro činnosti v oblasti signálového zpravodajství Spojených států amerických“.

7. Na otázky výkladu a dodržování zásad a příslušných politik ochrany soukromí ze strany organizací, které se účastní rámce EU–USA pro ochranu údajů, se bude vztahovat právo USA, s výjimkou případů, kdy se tyto organizace zavázaly ke spolupráci s úřady EU pro ochranu osobních údajů. Není-li stanoveno jinak, uplatní se veškerá ustanovení zásad ve všech relevantních případech.
8. Definice:
- a. „osobními údaji“ a „osobními informacemi“ se rozumí údaje o identifikované nebo identifikovatelné fyzické osobě, které spadají do oblasti působnosti obecného nařízení o ochraně osobních údajů, jež organizace ve Spojených státech obdrží z EU a jež jsou zaznamenány v jakékoli formě;
  - b. „zpracováním“ osobních údajů se rozumí jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění nebo šíření a výmaz 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 rozhodnutí Evropské komise o odpovídající ochraně v platnost.

## II. ZÁSADY

### 1. OZNAMOVACÍ POVINNOST

- a. Organizace musí fyzické osoby informovat o:
- i. své účasti v rámci EU–USA pro ochranu údajů a musí poskytnout odkaz na seznam organizací rámce pro ochranu údajů nebo jeho internetovou adresu;
  - ii. typech shromažďovaných osobních údajů a v příslušných případech o subjektech v USA nebo dceřiných společnostech v USA této organizace, které rovněž zásady dodržují;
  - iii. svém závazku řídit se zásadami u všech osobních údajů obdržených z EU na základě rámce EU–USA pro ochranu údajů;
  - iv. tom, za jakým účelem osobní informace o nich shromažďuje a využívá;
  - v. tom, jak kontaktovat organizaci v případě jakýchkoli dotazů nebo stížností, včetně uvedení příslušného zařízení v EU, které může na tyto dotazy nebo stížnosti reagovat;
  - vi. druhu nebo totožnosti třetích stran, kterým osobní informace zpřístupňuje, a o tom, za jakým účelem tak činí;
  - vii. právu fyzických osob na přístup ke svým osobním údajům;
  - viii. tom, jaké možnosti volby a prostředky tato organizace poskytuje fyzickým osobám, aby mohly omezit používání a zpřístupnění svých osobních údajů;
  - ix. nezávislém subjektu pro řešení sporů, který má řešit stížnosti a fyzickým osobám bezplatně poskytovat příslušné možnosti odvolání, a o tom, zda je jím: 1) panel zřízený úřady pro ochranu osobních údajů; 2) poskytovatel alternativního řešení sporů se sídlem v EU nebo 3) poskytovatel alternativního řešení sporů se sídlem ve Spojených státech;
  - x. tom, zda podléhají vyšetřovacím a donucovacím pravomocem Federální obchodní komise, Ministerstva dopravy nebo jakéhokoli jiného oprávněného subjektu USA zřízeného zákonem;
  - xi. možnosti fyzické osoby uchýlit se za určitých podmínek k závaznému rozhodčímu řízení; <sup>(5)</sup>
  - xii. požadavku zpřístupnit osobní informace v reakci na oprávněné žádosti orgánů veřejné moci, mj. s cílem splnit požadavky v souvislosti s národní bezpečností nebo prosazováním práva, a
  - xiii. své odpovědnosti v případě dalšího předání údajů třetím stranám.

<sup>(5)</sup> Viz např. oddíl c) zásady odvolání, prosazování a odpovědnosti.

- b. Toto oznámení musí být učiněno jasně a zřetelně při první příležitosti, při které je fyzická osoba požádána, aby poskytla organizaci své osobní údaje, nebo co možná nejdříve poté, avšak v každém případě předtím, než tato organizace takové údaje použije pro účely jiné, než pro jaké je předávající organizace původně shromáždila či zpracovala, nebo než je poprvé zpřístupní třetí straně.

## 2. MOŽNOST VOLBY

- a. Organizace musí dát fyzickým osobám možnost si vybrat (tj. opt-out), zda jejich osobní údaje mohou být i) zpřístupněny třetí straně nebo ii) použity k účelu, který se významně liší od účelu (účelů), ke kterému (kterým) byly původně shromážděny nebo následně dotčenými fyzickými osobami schváleny. Dotčeným fyzickým osobám musí být umožněn výkon jejich práva volby jasným, srozumitelným a snadno dostupným postupem.
- b. Odchylně od předchozího odstavce není nutné poskytovat možnost volby, jestliže jsou údaje zpřístupněny třetí straně, která jedná jako zprostředkovatel za účelem plnění úkolů jménem organizace a podle jejích pokynů. Organizace však se zprostředkovatelem vždy uzavře smlouvu.
- c. U citlivých informací (např. osobní údaje vypovídající o zdravotním stavu, rasovém nebo etnickém původu, politických postojích, náboženském nebo filozofickém přesvědčení, členství v odborových organizacích nebo informace o sexuální životě dané osoby) musí organizace od fyzické osoby získat potvrzující výslovný souhlas (tj. opt-in), jestliže mají být tyto informace i) zpřístupněny třetí straně nebo ii) použity k účelu, který neodpovídá účelu, pro který byly původně shromážděny nebo pro který byly následně dotčenými fyzickými osobami schváleny výkonem práva volby. Kromě toho by měla organizace s jakýmkoli osobními informacemi získanými od třetí strany, které třetí strana označí za citlivé a takto s nimi zachází, zacházet jako s citlivými informacemi.

## 3. ODPOVĚDNOST ZA DALŠÍ PŘEDÁVÁNÍ

- a. Při předávání osobních informací třetí straně, která jedná jako správce, musí organizace dodržovat zásady oznamovací povinnosti a možnosti volby. Organizace musí také s třetí stranou, která je správcem, uzavřít smlouvu, jež stanoví, že tyto údaje lze zpracovávat pouze k omezeným a stanoveným účelům v souladu se souhlasem poskytnutým dotýcnou fyzickou osobou a že příjemce poskytne tutéž úroveň ochrany jako tyto zásady a organizaci uvědomí, zjistí-li, že tuto povinnost již není schopen dodržet. Smlouva stanoví, že v případě tohoto zjištění třetí strana, která je správcem, přestane údaje zpracovávat nebo přijme jiné přiměřené a vhodné kroky k nápravě.
- b. Při předávání osobních údajů třetí straně, která jedná jako zprostředkovatel, organizace musí: i) předávat tyto údaje pouze k omezeným a stanoveným účelům; ii) zajistit, aby zprostředkovatel byl povinen poskytnout alespoň tutéž úroveň ochrany soukromí, jakou požadují tyto zásady; iii) přijmout přiměřené a vhodné kroky, jež zajistí, aby zprostředkovatel účinně zpracovával předané osobní informace v souladu s povinnostmi organizace podle těchto zásad; iv) požadovat, aby zprostředkovatel organizaci uvědomil, zjistí-li, že již není schopen dodržet svou povinnost poskytovat tutéž úroveň ochrany, jakou požadují tyto zásady; v) na žádost, a to i 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 uzavřené s uvedeným zprostředkovatelem týkajících se ochrany soukromí.

## 4. ZABEZPEČENÍ

- a. Organizace, které vytvářejí, uchovávají, používají nebo šíří osobní údaje, musí přijmout přiměřená a vhodná opatření, aby zabránily jejich ztrátě, zneužití a neoprávněnému přístupu k nim, jejich zpřístupnění, změně nebo zničení; přitom patřičně přihlédnou k rizikům vyplývajícím ze zpracování a k povaze osobních údajů.

## 5. INTEGRITA ÚDAJŮ A ÚČELOVÉ OMEZENÍ

- a. V souladu s těmito zásadami musí být osobní informace omezeny na informace, které jsou s ohledem na účely zpracování podstatné <sup>(6)</sup>. Organizace nesmí zpracovávat osobní údaje způsobem, který je neslučitelný s účelem, pro který byly původně shromážděny nebo následně dotčenou fyzickou osobou schváleny. V rozsahu nezbytném pro tyto účely je organizace povinna podniknout přiměřené kroky, aby zajistila spolehlivost osobních údajů pro zamýšlený účel, jejich přesnost, úplnost a aktuálnost. Organizace musí tyto zásady dodržovat po celou dobu, kdy si tyto informace ponechá.
- b. Informace lze uchovávat v podobě, která fyzickou osobu identifikuje nebo může identifikovat <sup>(7)</sup>, pouze po dobu, po kterou slouží účelu zpracování ve smyslu bodu 5 písm. a). Tato povinnost nebrání organizacím zpracovávat osobní informace po delší dobu a v rozsahu, kdy toto zpracování přiměřeně slouží účelům archivace ve veřejném zájmu, novinářské činnosti, literatury a umění, vědeckého nebo historického výzkumu a statistické analýzy. V těchto případech se na toto zpracování vztahují ostatní zásady a ustanovení rámce EU–USA pro ochranu údajů. Organizace by měly přijmout přiměřená a vhodná opatření, aby toto ustanovení splnily.

## 6. PRÁVO NA PŘÍSTUP

- a. Fyzické osoby musí mít přístup k osobním údajům, které o nich organizace uchovává, a musí mít možnost opravit, změnit nebo vymazat ty, které jsou nepřesné či byly zpracovány v rozporu s těmito zásadami, ledaže by zátěž nebo náklady spojené s poskytnutím přístupu byly v daném případě neúměrné rizikům pro soukromí dotčené fyzické osoby nebo by byla porušena práva osob jiných než dotčené fyzické osoby.

## 7. ODVOLÁNÍ, PROSAZOVÁNÍ A ODPOVĚDNOST

- a. Účinná ochrana soukromí musí zahrnovat odolné mechanismy zajišťující dodržování těchto zásad, možnosti odvolání pro fyzické osoby, které byly dotčeny nedodržením těchto zásad, jakož i sankce pro organizace, jestliže se zásadami neřídí. Takové mechanismy musí zahrnovat alespoň:
  - i. snadno dostupné nezávislé odvolací mechanismy, v jejichž rámci budou vyšetřovány veškeré stížnosti a spory předkládané fyzickými osobami a bude o nich urychleně bezplatně rozhodnuto s odvoláním na zásady a bude přiznána náhrada škody v případech, ve kterých to stanoví platné právo nebo iniciativy soukromého sektoru;
  - ii. následné postupy, kterými se ověřuje, zda osvědčení a tvrzení organizací o jejich opatřeních na ochranu soukromí jsou pravdivá a že tato opatření jsou prováděna tak, jak se uvádí, zejména pokud jde o případy nedodržování těchto zásad, a
  - iii. povinnost odstranit problémy vzniklé v důsledku nedodržení zásad organizacemi, které prohlásily, že je přijímají, jakož i odpovídající sankce pro takové organizace. Sankce musí být dostatečně přísné, aby bylo zajištěno, že organizace budou tyto zásady dodržovat.
- b. Organizace a jejich vybrané nezávislé odvolací mechanismy budou neprodleně reagovat na dotazy a žádosti ministerstva o informace týkající se rámce EU–USA pro ochranu údajů. Všechny organizace musí rychle reagovat na stížnosti na dodržování zásad postoupené prostřednictvím ministerstva úřady členských států EU. Organizace, které se rozhodly spolupracovat s úřady pro ochranu osobních údajů, včetně organizací, které zpracovávají údaje v oblasti lidských zdrojů, musí těmto úřadům v souvislosti s vyšetřováním a řešením stížností odpovídat přímo.

<sup>(6)</sup> V závislosti na okolnostech mohou příklady slučitelných účelů zpracování zahrnovat zpracování údajů, které přiměřeně slouží pro účely vztahů se zákazníky, dodržování předpisů, zákonných kritérií, auditů, bezpečnosti, předcházení podvodům, zachování nebo obhajoby zákonných práv organizace či pro jiné účely v souladu s přiměřeným očekáváním vzhledem k souvislostem sběru údajů.

<sup>(7)</sup> V této souvislosti je fyzická osoba „identifikovatelná“, pokud by ji organizace nebo třetí strana, měla-li by k údajům přístup, mohla přiměřeně identifikovat vzhledem k prostředkům identifikace, které by bylo možné s přiměřenou pravděpodobností využít (mj. s ohledem na náklady a množství času potřebné k identifikaci a na dostupnou technologii v době zpracování), a k formě, v níž jsou údaje uchovávány.

- c. Organizace jsou povinny rozhodovat o podnětech v rozhodčím řízení a dodržovat podmínky stanovené v příloze I za předpokladu, že se fyzická osoba v souladu s postupy a v závislosti na podmínkách stanovených v příloze I uchýlí k závaznému rozhodčímu řízení doručením oznámení žalované organizaci.
- d. V souvislosti s dalším předáváním nese zúčastněná organizace odpovědnost za zpracování osobních informací, které obdrží na základě rámce EU–USA pro ochranu údajů a následně předá třetí straně, jež jedná jejím jménem jako zprostředkovatel. Zúčastněná organizace zůstane odpovědná podle těchto zásad, jestliže její zprostředkovatel zpracuje tyto osobní informace způsobem, jenž není v souladu se zásadami, pokud organizace neprokáže, že za okolnost, která vedla ke vzniku škody, není odpovědná.
- e. Pokud se na organizaci vztahuje soudní příkaz vydaný z důvodu nedodržení zásad nebo příkaz subjektu USA zřízeného zákonem (např. Federální obchodní komise nebo Ministerstva dopravy) uvedeného v zásadách nebo v budoucí příloze zásad vydaný z důvodu nedodržení zásad, zveřejní organizace veškeré relevantní, rámce EU–USA pro ochranu údajů se týkající části zprávy o dodržování zásad nebo hodnotící zprávy předložených soudu nebo subjektu USA zřízenému zákonem, a to v rozsahu odpovídajícím požadavkům na zachování důvěrnosti. Ministerstvo zřídilo pro úřady pro ochranu osobních údajů specializované kontaktní místo pro případy jakýchkoli problémů zúčastněných organizací s dodržováním těchto zásad. Federální obchodní komise a Ministerstvo dopravy budou přednostně posuzovat případy nedodržování těchto zásad postoupené ministerstvem a orgány členských států EU a v závislosti na omezeních ohledně důvěrnosti údajů si budou s orgány postupujícího státu včas vyměňovat informace o postoupených případech.

### III. DOPLŇKOVÉ ZÁSADY

#### 1. Citlivé údaje

- a. Organizace není povinna získat potvrzující výslovný souhlas (tj. opt-in) s ohledem na citlivé údaje, pokud je zpracování:
  - i. v životně důležitém zájmu subjektu údajů nebo jiné osoby;
  - ii. nezbytné pro určení právních nároků nebo pro obhajobu;
  - iii. nezbytné k poskytnutí zdravotní péče nebo určení diagnózy;
  - iv. prováděno v rámci zákonné činnosti nadace, sdružení nebo jakékoli jiné neziskové organizace s politickým, filozofickým, náboženským nebo odborářským zaměřením a za podmínky, že se zpracování týká výhradně členů této organizace nebo osob, které s ní jsou v pravidelném kontaktu v souvislosti s jejími cíli, a že údaje nebudou zpřístupněny třetím stranám bez souhlasu subjektů údajů;
  - v. nezbytné pro splnění povinností této organizace vyplývajících z pracovního práva; nebo
  - vi. pokud se týká údajů, které dotčená fyzická osoba prokazatelně zveřejnila.

#### 2. Výjimky pro novinářskou činnost

- a. Vzhledem k ústavní ochraně svobody tisku ve Spojených státech musí v případech, ve kterých se právo na svobodný tisk zakotvené v prvním dodatku k Ústavě Spojených států střetává se zájmy na ochranu soukromí, vyvážení těchto zájmů, pokud jde o činnost fyzických či právnických osob v USA, upravovat první dodatek.
- b. Na osobní informace, které se shromažďují za účelem zveřejnění, rozhlasového či televizního vysílání nebo jiných způsobů veřejného sdělování novinářských materiálů, bez ohledu na to, zda jsou skutečně použity či nikoli, jakož i na informace nalezené v dříve uveřejněných materiálech pocházejících z mediálních archivů se požadavky zásad nevztahují.

#### 3. Druhotná odpovědnost

- a. Poskytovatelé internetových služeb, telekomunikační společnosti a jiné organizace nenesou odpovědnost podle zásad, jestliže informace pouze přenášejí, přeměňují, přepojují nebo dočasně ukládají jménem jiných organizací. Rámec EU–USA pro ochranu údajů nezakládá druhotnou odpovědnost. Organizace není odpovědná v rozsahu, v němž zajišťuje pouze prostý přenos údajů přenášených třetími stranami a neurčuje účel ani prostředky zpracování těchto osobních údajů.

#### 4. Provádění hloubkových kontrol a auditů

- a. Činnost auditorů a investičních bankéřů může zahrnovat zpracovávání osobních údajů bez souhlasu či vědomí dotčené fyzické osoby. To za níže popsaných okolností dovolují zásady oznamovací povinnosti, možnosti volby a práva na přístup.
- b. Otevřené i uzavřené akciové společnosti, včetně zúčastněných organizací, se pravidelně podrobují auditům. Tyto audity, zejména takové, které se zabývají potenciálním protiprávním jednáním, mohou být ohroženy, budou-li předčasně prozrazeny. Obdobně bude zúčastněná organizace, která se podílí na potenciální fúzi nebo převzetí firmy, muset provést „hloubkový“ přezkum či se mu podrobit. Tento přezkum s sebou často ponese sběr a zpracování osobních údajů, jako jsou informace o vyšších vedoucích pracovnících a jiných klíčových zaměstnancích. Předčasné prozrazení by mohlo zabránit transakci, nebo dokonce porušit platné předpisy o cenných papírech. Investiční bankéři a advokáti, kteří se zabývají hloubkovou kontrolou, nebo auditoři, kteří provádějí audit, smějí zpracovávat osobní údaje bez vědomí dotčené fyzické osoby pouze v rozsahu nezbytném a po dobu nezbytnou pro splnění zákonných požadavků nebo požadavků vyplývajících z veřejného zájmu a v dalších případech, v nichž by uplatněním těchto zásad byly dotčeny oprávněné zájmy organizace. Mezi takové oprávněné zájmy patří kontrola dodržování zákonných povinností organizací a sledování účetnictví a potřeba zachování důvěrnosti související s případnými akvizicemi, fúzemi, společnými podniky nebo jinými podobnými transakcemi, které provádějí investiční bankéři nebo auditoři.

#### 5. Úloha úřadů pro ochranu osobních údajů

- a. Organizace budou plnit svůj závazek spolupracovat s úřady pro ochranu osobních údajů, jak je popsáno níže. Na základě rámce EU–USA pro ochranu údajů se organizace USA, které přijímají osobní údaje z EU, musí zavázat, že budou používat účinné mechanismy pro zajištění souladu se zásadami. Jak je konkrétněji uvedeno v zásadě odvolání, prosazování a odpovědnosti, zúčastněné organizace musí zajistit: a) i) možnosti odvolání pro fyzické osoby, jichž se údaje týkají; a) ii) následné postupy pro ověření, zda jejich osvědčení a tvrzení o postupech při ochraně soukromí jsou pravdivá, a a) iii) povinnost napravit problémy vyplývající z nedodržení zásad, jakož i důsledky pro takové organizace. Má se za to, že organizace splňuje ustanovení písm. a) bodů i) a iii) zásady odvolání, prosazování a odpovědnosti, jestliže plní požadavky stanovené zde pro spolupráci s úřady pro ochranu osobních údajů.
- b. Organizace se zavazuje ke spolupráci s úřady pro ochranu osobních údajů tím, že v autocertifikaci předložené ministerstvu, kterou přijímá zásady rámce EU–USA pro ochranu údajů (viz doplňková zásada autocertifikace), prohlásí, že:
  - i. se rozhodla splnit požadavky uvedené v písm. a) bodech i) a iii) zásady odvolání, prosazování a odpovědnosti tím, že se zavazuje ke spolupráci s úřady pro ochranu osobních údajů;
  - ii. bude spolupracovat s úřady pro ochranu osobních údajů při vyšetřování a řešení stížností podaných podle zásad a
  - iii. podrobí se doporučení příslušných úřadů pro ochranu osobních údajů v případě, že tyto úřady dojdou k názoru, že organizace musí provést konkrétní opatření, aby splnila zásady, včetně opatření vedoucích k nápravě nebo odškodnění ve prospěch fyzických osob, které byly poškozeny v důsledku nedodržení těchto zásad, a poskytne úřadům pro ochranu osobních údajů písemné potvrzení, že takové opatření provedla.
- c. Fungování panelů zřízených úřady pro ochranu osobních údajů
  - i. Spolupráce ze strany úřadů pro ochranu osobních údajů bude mít podobu informací a doporučení a bude probíhat tímto způsobem:
    1. Úřady pro ochranu osobních údajů budou poskytovat doporučení prostřednictvím svého neformálního panelu zřízeného na úrovni Evropské unie, jehož úkolem bude mimo jiné pomáhat zajišťovat harmonizovaný a soudržný přístup.
    2. Tento panel bude poskytovat doporučení dotčeným organizacím USA v případě nevyřešených stížností fyzických osob na nakládání s osobními údaji, které byly předány z Evropské unie na základě rámce EU–USA pro ochranu údajů. Doporučení mají zajistit, aby zásady byly uplatňovány správně, a budou zahrnovat veškeré opravné prostředky ve prospěch dotčené fyzické osoby (dotčených fyzických osob), jež úřady pro ochranu osobních údajů budou považovat za přiměřené.

3. Tento panel bude poskytovat doporučení na základě žádostí dotčených organizací nebo stížností přijatých přímo od fyzických osob na organizace, které se zavázaly ke spolupráci s úřady pro ochranu osobních údajů pro účely rámce EU–USA pro ochranu údajů, přičemž bude tyto fyzické osoby povzbuzovat a v případě nutnosti jim napomáhat k tomu, aby nejdříve využily vnitřních mechanismů pro vyřizování stížností, které daná organizace nabízí.
  4. Doporučení se budou vydávat teprve poté, co byla oběma stranám sporu poskytnuta dostatečná příležitost zaujmout stanovisko a předložit veškeré důkazy, které si přejí uvést. Panel se bude snažit poskytnout doporučení v co nejkratší době, jak jen to požadavek řádného procesu umožní. Zpravidla se tento panel bude snažit poskytnout doporučení do 60 dnů od přijetí stížnosti nebo žádosti, a pokud to bude možné, rychleji.
  5. Panel zveřejní výsledky svého posouzení předložených stížností, pokud to bude považovat za vhodné.
  6. Poskytování doporučení tímto panelem nezakládá žádnou odpovědnost panelu ani jednotlivých úřadů pro ochranu osobních údajů.
- ii. Jak bylo uvedeno výše, organizace, které se rozhodnou využít pro řešení sporů této možnosti, se musí zavázat, že se podrobí doporučení úřadů pro ochranu osobních údajů. Jestliže se organizace nepodrobí doporučení do 25 dnů od jeho doručení a zpoždění uspokojivě nevysvětlí, oznámí panel svůj záměr buď postoupit věc Federální obchodní komisi, Ministerstvu dopravy či jinému federálnímu nebo státnímu orgánu Spojených států se zákonnými pravomocemi k výkonu rozhodnutí v případech podvodu nebo uvedení v omyl, nebo konstatovat, že dohoda o spolupráci byla závažným způsobem porušena, a musí být proto považována za neplatnou. V posledně jmenovaném případě informuje panel ministerstvo, aby mohl být seznam organizací rámec pro ochranu údajů odpovídajícím způsobem změněn. Jakékoli nesplnění závazku spolupracovat s úřady pro ochranu osobních údajů, jakož i nedodržení zásad je žalovatelné jako klamavé praktiky podle § 5 zákona o Federální obchodní komisi (15 U.S.C. § 45), 49 U.S.C. § 41712 nebo jiných podobných zákonů.
- d. Organizace, která si přeje, aby výhody plynoucí z rámce EU–USA pro ochranu údajů pokrývaly údaje v oblasti lidských zdrojů předávané z EU v rámci zaměstnaneckého vztahu, se musí zavázat ke spolupráci s úřady pro ochranu osobních údajů, pokud jde o tyto údaje (viz doplňková zásada o údajích v oblasti lidských zdrojů).
  - e. Organizace, které se rozhodnou pro tuto možnost, budou povinny platit roční poplatek určený na krytí provozních nákladů panelu. Mohou být navíc požádány, aby uhradily náklady na veškeré potřebné překlady vyplývající z poradenské činnosti panelu v souvislosti s posuzováním žádostí nebo stížností podaných proti nim. Výši poplatku stanoví ministerstvo po konzultaci s Komisí. Výběr poplatku může provádět třetí strana, kterou ministerstvo vybere jako správce finančních prostředků shromážděných za tímto účelem. Ministerstvo bude úzce spolupracovat s Komisí a úřady pro ochranu osobních údajů na zavedení vhodných postupů pro rozdělování finančních prostředků vybraných prostřednictvím tohoto poplatku, jakož i na dalších procesních a správních aspektech panelu. Ministerstvo a Komise se mohou dohodnout na změně četnosti výběru poplatku.

## 6. Autocertifikace

- a. Výhody plynoucí z rámce EU–USA pro ochranu údajů jsou zajištěny ode dne, kdy ministerstvo zařadí organizaci na seznam organizací rámce pro ochranu údajů. Ministerstvo zařadí organizaci na seznam organizací rámce pro ochranu údajů až poté, co rozhodne, že původní autocertifikace organizace je úplná, a organizaci z tohoto seznamu odstraní, jestliže organizace dobrovolně vystoupí, neabsolvuje každoroční opětovnou certifikaci nebo pokud soustavně nedodržuje zásady (viz doplňková zásada o řešení sporů a prosazování).
- b. Za účelem autocertifikace přijetí zásad rámce EU–USA pro ochranu údajů nebo její následné opětovné certifikace musí organizace pokaždé předložit ministerstvu podání vedoucího pracovníka jménem organizace, které autocertifikaci nebo (případně) opětovnou certifikaci dodržování zásad<sup>(8)</sup> uvádí a které obsahuje alespoň tyto informace:

<sup>(8)</sup> Podání musí podat prostřednictvím internetových stránek ministerstva věnovaných rámci pro ochranu údajů fyzická osoba v rámci organizace, která je oprávněna činit jménem organizace a kteréhokoliv z jejích subjektů, na které se vztahuje, prohlášení o dodržování zásad.

- i. název organizace USA, která se autocertifikuje nebo opětovně certifikuje, jakož i název (názyvy) všech jejích subjektů v USA nebo dceřiných společností v USA, jež se rovněž řídí zásadami a které si organizace přeje zahrnout;
  - ii. popis činností organizace v souvislosti s osobními údaji, jež by byly přijímány z EU na základě rámce EU–USA pro ochranu údajů;
  - iii. popis příslušné politiky ochrany soukromí uplatňované danou organizací na takové osobní údaje, který zahrnuje:
    - 1. má-li organizace veřejné internetové stránky, příslušnou internetovou adresu, na které je politika ochrany soukromí dostupná, nebo nemá-li organizace veřejné internetové stránky, údaj o tom, kde je tato politika přístupná k nahlédnutí veřejnosti, a
    - 2. datum, kdy nabyla účinnosti;
  - iv. kontaktní místo v rámci organizace pro vyřizování stížností, žádostí o přístup k informacím a dalších záležitostí vyplývajících ze zásad <sup>(9)</sup>, včetně:
    - 1. jména (jmen), pracovního/pracovních zařazení (v příslušných případech), e-mailové adresy (e-mailových adres) a telefonního čísla (telefonních čísel) příslušné osoby (příslušných osob) nebo příslušného kontaktního místa (příslušných kontaktních míst) v rámci organizace a
    - 2. příslušné poštovní adresy organizace v USA;
  - v. konkrétní subjekt zřízený zákonem, který je příslušný projednávat stížnosti na organizaci ohledně případných nekalých nebo klamavých praktik a porušení předpisů na ochranu soukromí (a který je uveden v zásadách nebo v jejich budoucí příloze);
  - vi. název případného programu na ochranu soukromí, jehož se organizace účastní;
  - vii. způsob ověřování (tj. sebehodnocení; externí přezkumy souladu, včetně uvedení třetí strany, která tyto přezkumy provádí) <sup>(10)</sup> a
  - viii. příslušný nezávislý odvolací mechanismus (příslušné nezávislé odvolací mechanismy) pro vyšetřování nevyřešených stížností týkající se zásad <sup>(11)</sup>.
- c. Pokud si organizace přeje rozšířit výhody plynoucí z rámce EU–USA pro ochranu údajů na údaje v oblasti lidských zdrojů předávané z EU pro využití v rámci zaměstnaneckých vztahů, může tak učinit, jestliže existuje subjekt zřízený zákonem, který je příslušný projednávat stížnosti na organizaci ohledně zpracování těchto údajů v oblasti lidských zdrojů a který je uveden v těchto zásadách nebo v jejich budoucí příloze. Organizace musí navíc uvést tuto skutečnost při původní autocertifikaci i opětovné certifikaci a zavázat se ke spolupráci s příslušným(i) úřadem (úřady) v EU v souladu s použitelnými ustanoveními doplňkové zásady o údajích v oblasti lidských zdrojů a doplňkové zásady o úloze úřadů pro ochranu osobních údajů a k tomu, že bude dodržovat doporučení vydaná těmito úřady. Organizace musí také ministerstvu předat kopii své politiky ochrany soukromí v souvislosti s lidskými zdroji a poskytnout informaci, kde se s uvedenou politikou mohou seznámit dotčení zaměstnanci.

<sup>(9)</sup> Primární „kontakt organizace“ nebo „vedoucí pracovník organizace“ nemohou být externími pracovníky organizace (např. externí poradce nebo externí konzultant).

<sup>(10)</sup> Viz doplňková zásada o ověřování.

<sup>(11)</sup> Viz doplňková zásada o řešení sporů a prosazování.

- d. Ministerstvo povede a zveřejní seznam organizací rámce pro ochranu údajů, které předložily původní dokončené autocertifikace a tento seznam aktualizuje na základě dokončených každoročních předložených opětovných certifikací, jakož i oznámení obdržení podle doplňkové zásady o řešení sporů a prosazování. Opětovné certifikace se musí předkládat alespoň jednou ročně; v opačném případě bude organizace odstraněna ze seznamu organizací rámce pro ochranu údajů a nebudou jí již nadále náležet výhody vyplývající z rámce EU–USA pro ochranu údajů. Všechny organizace, které ministerstvo umístí na seznam organizací rámce pro ochranu údajů, musí mít příslušné politiky ochrany soukromí, které jsou v souladu se zásadou oznamovací povinnosti a v těchto politikách ochrany soukromí musí uvést, že tyto zásady dodržují<sup>(12)</sup>. Je-li příslušná politika ochrany soukromí dostupná on-line, musí v ní organizace uvést hypertextový odkaz na internetové stránky ministerstva týkající se rámce pro ochranu údajů a hypertextový odkaz na internetové stránky nezávislého odvolacího mechanismu pro bezplatné prošetřování nevyřešených stížností týkajících se zásad nebo na formulář tohoto mechanismu pro podávání stížností.
- e. Zásady platí okamžitě po autocertifikaci. Zúčastněné organizace, které se dříve autocertifikovaly, že budou dodržovat zásady štítu EU–USA na ochranu soukromí, budou muset aktualizovat své politiky ochrany soukromí tak, aby namísto toho odkazovaly na „zásady rámce EU–USA pro ochranu údajů“. Tyto organizace uvedou tento odkaz co nejdříve a v každém případě nejpozději do tří měsíců ode dne nabytí účinnosti zásad rámce EU–USA pro ochranu údajů.
- f. Organizace musí těmto zásadám podrobit všechny osobní údaje přijaté z EU na základě rámce EU–USA pro ochranu údajů. Závazek dodržovat zásady není ve vztahu k osobním údajům, které organizace obdržela v době, v níž požívá výhod rámce EU–USA pro ochranu údajů, časově omezen; tento závazek znamená, že se na takové údaje nadále vztahují zásady tak dlouho, dokud je organizace uchovává, používá nebo zpřístupňuje, a to i v případě, že následně z jakéhokoli důvodu rámec EU–USA pro ochranu údajů opustí. Organizace, která si přeje vystoupit z rámce EU–USA pro ochranu údajů, musí tuto skutečnost oznámit ministerstvu předem. V tomto oznámení musí být rovněž uvedeno, jak bude organizace nakládat s osobními údaji, které obdržela na základě rámce EU–USA pro ochranu údajů (tj. údaje uchová, vrátí nebo vymaže, a pokud údaje uchová, uvede schválené prostředky, kterými zajistí ochranu údajů). Organizace, která z rámce EU–USA pro ochranu údajů vystoupí, ale chce si tyto údaje ponechat, musí každý rok ministerstvu potvrdit svůj závazek nadále na tyto údaje uplatňovat zásady, nebo zajistit „odpovídající“ ochranu údajů jinými schválenými prostředky (například pomocí smlouvy, do níž se v plném rozsahu promítají požadavky příslušných standardních smluvních doložek přijatých Komisí); v opačném případě musí organizace informace vrátit nebo vymazat<sup>(13)</sup>. Organizace, která z rámce EU–USA pro ochranu údajů vystoupí, musí z příslušné politiky ochrany soukromí odstranit veškeré odkazy na rámec EU–USA pro ochranu údajů, z nichž vyplývá, že se organizace rámce EU–USA pro ochranu údajů nadále aktivně účastní a má nárok na jeho výhody.

<sup>(12)</sup> Organizace, která se autocertifikuje poprvé, nemůže odkazovat na svoji účast v rámci EU–USA pro ochranu údajů v konečné verzi své politiky ochrany soukromí, dokud jí ministerstvo neoznámí, že tak může učinit. Při předložení své původní autocertifikace musí organizace ministerstvu poskytnout návrh své politiky ochrany soukromí, který je v souladu se zásadami. Jakmile ministerstvo rozhodne, že původní autocertifikace organizace je jinak úplná, oznámí organizaci, že by měla svou politiku ochrany soukromí, která je v souladu s rámcem EU–USA pro ochranu údajů, vydat v konečné verzi (a např. případně zveřejnit). Jakmile je příslušná politika ochrany soukromí vydána v konečné verzi, musí o tom organizace neprodleně uvědomit ministerstvo, přičemž v tomto okamžiku ministerstvo zařadí organizaci na seznam organizací rámce pro ochranu údajů.

<sup>(13)</sup> Pokud se organizace v okamžiku svého vystoupení rozhodne uchovávat osobní údaje, které obdržela na základě rámce EU–USA pro ochranu údajů, a ministerstvu každoročně potvrdí, že na tyto údaje nadále uplatňuje zásady, musí organizace ministerstvu jednou ročně po svém vystoupení z rámce doložit (tj. pokud a dokud organizace neposkytne „odpovídající“ ochranu těmto údajům jiným schváleným způsobem nebo pokud všechny tyto údaje nevrátí či nevymaže a dokud to neoznámí ministerstvu), co s těmito osobními údaji udělala, co s údaji, které nadále uchovává, bude dělat a kdo bude sloužit jako stálý kontaktní bod pro otázky související se zásadami.

- g. Organizace, která přestane existovat jako samostatná právnická osoba v důsledku změny statusu společnosti, například v důsledku fúze, převzetí, konkursu nebo zrušení, musí o této skutečnosti předem uvědomit ministerstvo. V oznámení by mělo být rovněž uvedeno, zda se subjekt vyplývající ze změny statusu společnosti i) bude nadále účastnit rámce EU–USA pro ochranu údajů prostřednictvím stávající autocertifikace; ii) autocertifikuje jako nový účastník rámce EU–USA pro ochranu údajů (např. pokud nový subjekt nebo následnický subjekt ještě nemají stávající autocertifikaci, jejímž prostřednictvím by se mohly účastnit rámce EU–USA pro ochranu údajů); nebo iii) zavede jiné záruky, jako je písemná dohoda, která zajistí trvalé uplatňování zásad na veškeré osobní údaje, které organizace obdržela na základě rámce EU–USA pro ochranu údajů a které budou uchovávány. Pokud se nepoužijí body i), ii) ani iii), musí být veškeré osobní údaje obdržené na základě rámce EU–USA pro ochranu údajů neprodleně vráceny nebo vymazány.
- h. Pokud organizace z jakéhokoli důvodu rámec EU–USA pro ochranu údajů opustí, musí odstranit všechna prohlášení, z nichž vyplývá, že se organizace nadále účastní rámce EU–USA pro ochranu údajů nebo má nárok na výhody, jež z tohoto rámce plynou. Certifikační značka rámce EU–USA pro ochranu údajů, je-li užívána, musí být rovněž odstraněna. Jakákoli nepravdivá prohlášení učiněná vůči veřejnosti o tom, že organizace uplatňuje zásady, mohou být předmětem žaloby podané Federální obchodní komisí, Ministerstvem dopravy nebo jiným příslušným orgánem veřejné správy. Nepravdivá prohlášení učiněná vůči ministerstvu mohou být předmětem žaloby podle zákona o nepravdivých tvrzeních (False Statements Act) (18 U.S.C. § 1001).

## 7. Ověřování

- a. Organizace musí zajistit následné postupy pro ověřování toho, že osvědčení a tvrzení o jejich opatřeních na ochranu soukromí podle rámce EU–USA pro ochranu údajů jsou pravdivá a že se tato opatření provádějí skutečně tak, jak se uvádí, a v souladu se zásadami.
- b. Aby splnila požadavky na ověřování podle zásady odvolání, prosazování a odpovědnosti, musí organizace tato osvědčení a tvrzení ověřit buď prostřednictvím sebehodnocení, nebo prostřednictvím externího přezkumu souladu.
- c. Pokud si organizace zvolila sebehodnocení, musí toto ověření prokázat, že její politika ochrany soukromí týkající se osobních informací přijatých z EU je přesná, komplexní, snadno dostupná, v souladu se zásadami a plně prováděna (tj. je dodržována). Musí rovněž uvádět, že fyzické osoby jsou informovány o vnitřních postupech pro vyřizování stížností a o nezávislých odvolacích mechanismech, jejichž prostřednictvím mohou podávat své stížnosti; že organizace má zavedeny své postupy pro školení zaměstnanců v provádění těchto opatření a že postihuje nedodržování těchto opatření a že má zavedeny vnitřní postupy pro pravidelnou objektivní kontrolu dodržování výše uvedených opatření. Prohlášení ověřující provedení sebehodnocení musí podepsat vedoucí pracovník nebo jiný zmocněný zástupce organizace alespoň jednou ročně a musí být předloženo na žádost fyzických osob nebo v souvislosti s vyšetřováním nebo stížností na nedodržování předpisů.
- d. Pokud si organizace zvolila externí přezkum souladu, musí toto ověření prokázat, že její politika ochrany soukromí týkající se osobních informací přijatých z EU je přesná, komplexní, snadno dostupná, v souladu se zásadami a plně prováděna (tj. je dodržována). Musí rovněž uvádět, že fyzické osoby jsou informovány o mechanismu či mechanismech, jejichž prostřednictvím mohou podávat stížnosti. Metody přezkumu mohou mimo jiné zahrnovat audit, námtkové přezkumy, používání „návny“ nebo případně použití technologických nástrojů. Prohlášení osvědčující úspěšné provedení externího přezkumu musí být podepsáno buď osobou, jež přezkum provedla, nebo vedoucím pracovníkem či jiným zmocněným zástupcem organizace alespoň jednou ročně a musí být předloženo na žádost fyzických osob nebo v souvislosti s vyšetřováním nebo stížností na nedodržování zásad.
- e. Organizace musí uchovávat záznamy o provádění svých opatření na ochranu soukromí vypracovaných podle rámce EU–USA pro ochranu údajů a na žádost v souvislosti s vyšetřováním nebo stížností na nedodržování předpisů je musí předložit nezávislému subjektu pro řešení sporů odpovědnému za vyšetřování stížností nebo orgánu, který je příslušný rozhodovat v případech nekalých a klamavých praktik. Organizace musí také neprodleně reagovat na dotazy a jiné žádosti o informace ze strany ministerstva, které se týkají dodržování těchto zásad organizací.

## 8. Právo na přístup

### a. Zásada práva na přístup v praxi

- i. Podle zásad má právo na přístup pro ochranu soukromí zásadní význam. Konkrétně umožňuje fyzickým osobám ověřovat správnost o nich uchovávaných informací. Zásada práva na přístup znamená, že fyzické osoby mají právo:
  1. získat od organizace potvrzení, zda organizace zpracovává osobní údaje, které se dotčených fyzických osob týkají, či nikoli <sup>(14)</sup>;
  2. na sdělení těchto údajů, aby mohly ověřit jejich přesnost a oprávněnost zpracování, a
  3. na opravu, změnu nebo výmaz údajů, jsou-li nepřesné nebo zpracovány v rozporu s těmito zásadami.
- ii. Fyzické osoby nejsou povinny své žádosti o poskytnutí přístupu ke svým osobním údajům zdůvodňovat. Požaduje-li někdo přístup k údajům, které jsou o něm uchovávány, organizace by se měly řídit především důvodem či důvody, které k žádosti vedly. Například, je-li žádost neurčitá nebo týká-li se příliš široké oblasti, může organizace navázat s danou osobou dialog, aby lépe porozuměla motivu žádosti a našla požadované údaje. Organizace se může dotazovat, se kterou její organizační složkou (složkami) byla osoba v kontaktu nebo jaká je povaha nebo využití údajů, které jsou předmětem žádosti o poskytnutí přístupu.
- iii. Vzhledem k tomu, že právo na přístup je jako takové základem ochrany soukromí, měly by se organizace vždy v dobré víře snažit přístup poskytnout. Například, pokud je třeba určité informace chránit a lze je snadno oddělit od jiných osobních informací, které jsou předmětem žádosti o poskytnutí přístupu, měla by organizace chráněné informace oddělit a ostatní informace dát k dispozici. Jestliže organizace rozhodne, že v některém konkrétním případě je nutno přístup omezit, měla by podat fyzické osobě požadující přístup vysvětlení, proč takto rozhodla, a uvést kontaktní místo, které podá další informace.

### b. Zátěž nebo náklady spojené s poskytnutím přístupu

- i. Právo na přístup k osobním údajům lze za výjimečných okolností omezit, pokud by byla porušena legitimní práva osob jiných než dotčené fyzické osoby nebo pokud by zátěž nebo náklady spojené s poskytnutím přístupu byly v daném případě neúměrné rizikům pro soukromí dotčené fyzické osoby. Náklady a zátěž představují důležité hledisko a měly by být brány v úvahu, avšak nejsou rozhodujícími faktory pro určení toho, zda je poskytnutí přístupu přiměřené.
- ii. Například, jestliže se osobní informace využívají při rozhodnutích, která mají na fyzickou osobu podstatný dopad (např. zamítnutí či přiznání důležitých výhod, jako je pojištění, hypotéka nebo zaměstnání), pak je v souladu s ostatními ustanoveními těchto doplňkových zásad organizace povinna tyto informace zpřístupnit i v případě, že je to relativně obtížné nebo nákladné. Jestliže nejsou požadované osobní informace citlivé nebo se nevyužívají při rozhodnutích, která mají na fyzickou osobu podstatný dopad, avšak jsou snadno dostupné a jejich poskytnutí není nákladné, pak je organizace povinna poskytnout k těmto informacím přístup.

### c. Důvěrné obchodní informace

- i. Důvěrné obchodní informace jsou informace, jejichž zveřejnění se organizace brání zvláštními opatřeními, protože takové zveřejnění by zvýhodnilo konkurenta na trhu. Organizace mohou zamítnout nebo omezit přístup v tom rozsahu, v jakém by jeho plné poskytnutí odhalilo jejich vlastní důvěrné obchodní informace, jako např. marketingové závěry nebo klasifikace vytvořené organizací, nebo důvěrné obchodní informace jiného subjektu, na které se vztahuje povinnost utajení vyplývající ze smlouvy.

<sup>(14)</sup> Organizace by měla odpovědět na žádosti fyzických osob týkající se účelů zpracování, kategorií údajů, na které se zpracování vztahuje, a příjemců nebo kategorií příjemců, kterým jsou osobní údaje poskytovány.

- ii. Pokud lze důvěrné obchodní informace snadno oddělit od jiných osobních informací, které jsou předmětem žádosti o poskytnutí přístupu, měla by organizace důvěrné obchodní informace oddělit a informace, které nejsou důvěrné, dát k dispozici.

d. Uspořádání databází

- i. Přístup může být poskytnut tím způsobem, že organizace fyzické osobě zpřístupní příslušné osobní informace, přičemž se nevyžaduje, aby fyzická osoba získala přístup k databázi organizace.
- ii. Organizace musí poskytnout přístup pouze v rozsahu, v jakém příslušné osobní informace uchovává. Zásada práva na přístup nezakládá sama o sobě žádnou povinnost uchovávat, udržovat, reorganizovat nebo restrukturalizovat soubory s osobními informacemi.

e. Kdy lze přístup omezit

- i. Jelikož organizace vždy musí v dobré víře usilovat o poskytnutí přístupu fyzickým osobám k jejich osobním údajům, jsou okolnosti, za kterých organizace smí tento přístup omezit, limitované a veškeré důvody omezení přístupu musí být konkrétní. Stejně jako podle nařízení GDPR může organizace omezit přístup k informacím v rozsahu, v němž by jejich zpřístupnění pravděpodobně ohrozilo důležité veřejné zájmy, jako je např. národní bezpečnost, obrana nebo veřejná bezpečnost. Přístup lze zamítnout dále v případech, ve kterých se osobní informace zpracovávají výhradně pro výzkumné nebo statistické účely. Dalšími důvody pro odepření nebo omezení přístupu jsou:
  - 1. narušení výkonu či prosazování práva nebo soukromoprávních žalobních důvodů, včetně prevence, vyšetřování nebo odhalování trestných činů nebo práva na spravedlivý proces;
  - 2. okolnosti, za nichž by byla porušena legitimní práva nebo významné oprávněné zájmy jiných osob;
  - 3. porušení zákonného nebo jiného profesního práva nebo povinnosti;
  - 4. narušení bezpečnostních prověrek zaměstnanců nebo postupů pro předkládání stížností či v souvislosti s plánováním nového obsazení pracovních míst a s reorganizací společnosti nebo
  - 5. narušení důvěrnosti nezbytné v souvislosti se sledováním, kontrolou nebo jinými zákonem předepsanými regulačními funkcemi souvisejícími s řádným hospodářským nebo finančním řízením či nezbytné důvěrnosti budoucích nebo probíhajících jednání organizace.
- ii. Organizace, která se odvolává na výjimku, má povinnost prokázat její nutnost a fyzické osobě by měly být sděleny důvody omezení přístupu a kontaktní místo, které podá další informace.

f. Právo obdržet potvrzení a účtovat poplatek na pokrytí nákladů za poskytnutí přístupu

- i. Fyzická osoba má právo obdržet potvrzení, zda tato organizace má její osobní údaje, či nikoli. Fyzická osoba má také právo nechat si své osobní údaje sdělit. Organizace mohou uložit poplatek, který není přemrštěný.
- ii. Uložení poplatku může být odůvodněné, jestliže jsou žádosti o přístup například zjevně nepřiměřené, zvláště z toho důvodu, že se opakují.
- iii. Přístup nesmí být odmítnut z důvodů vysokých nákladů, jestliže je fyzická osoba ochotna tyto náklady uhradit.

g. Opakované nebo kverulantské žádosti o přístup

- i. Organizace mohou přiměřeně omezit počet žádostí o přístup od jedné osoby, které lze v daném časovém období uspokojit. Při stanovování takových omezení by měla organizace brát v úvahu takové faktory, jako je četnost aktualizace informací, účel, k němuž jsou údaje využívány, a povaha informací.

h. Podvodné žádosti o přístup

- i. Organizace není povinna poskytnout přístup, dokud neobdrží dostatečné informace, podle nichž by mohla potvrdit totožnost žadatele.

i. Časový rámec pro reakce

- i. Organizace by měly na žádosti fyzických osob o přístup reagovat v přiměřené lhůtě, přiměřeným způsobem a snadno srozumitelnou formou. Organizace, která poskytuje informace subjektům údajů pravidelně, může žádosti fyzické osoby o přístup vyhovět v rámci svého pravidelného zpřístupňování informací, nedojde-li tak k nadměrnému prodloužení.

9. **Údaje v oblasti lidských zdrojů**

a. Oblast působnosti rámce EU–USA pro ochranu údajů

- i. Pokud organizace usazená v EU předává osobní údaje o svých zaměstnancích (bývalých nebo současných) shromážděné v souvislosti se zaměstnaneckými vztahy mateřské, přidružené či nikoli přidružené společnosti, která poskytuje služby ve Spojených státech a účastní se rámce EU–USA pro ochranu údajů, požívá předávání výhod rámce EU–USA pro ochranu údajů. V takových případech podléhá shromažďování a zpracovávání informací před jejich předáním vnitrostátním právním předpisům toho členského státu EU, ve kterém jsou shromažďovány, a musí být dodržovány veškeré podmínky pro předávání nebo omezení předávání vyplývající z těchto předpisů.
- ii. Zásady se uplatní, pouze pokud se předávají nebo zpřístupňují záznamy o identifikovaných či identifikovatelných fyzických osobách. Statistické výkazy zakládající se na agregovaných údajích o zaměstnancích a neobsahující osobní údaje nebo na využívání anonymních údajů nepředstavují ohrožení soukromí.

b. Používání zásad oznamovací povinnosti a možnosti volby

- i. Organizace v USA, která obdržela informace o zaměstnancích z EU na základě rámce EU–USA pro ochranu údajů, smí tyto informace sdělovat třetím stranám nebo je používat pro jiné účely pouze v souladu se zásadami oznamovací povinnosti a možnosti volby. Například, pokud organizace hodlá využít osobní informace shromážděné v rámci zaměstnaneckého vztahu pro účely nesouvisející se zaměstnáním, jako například pro marketingová sdělení, musí organizace v USA předem poskytnout dotčeným fyzickým osobám předepsanou možnost volby, ledaže již dříve souhlasily s využitím informací pro takové účely. Toto využití nesmí být neslučitelné s účely, pro které byly osobní informace shromážděny nebo se kterými fyzická osoba následně souhlasila. Taková volba navíc nesmí být důvodem k omezení pracovních příležitostí nebo k sankcím vůči takovým zaměstnancům.
- ii. Je nutno upozornit na skutečnost, že určité všeobecně platné podmínky pro předávání údajů z některých členských států EU mohou vyloučit jiné využití takových informací i po uskutečnění jejich předání do zemí mimo EU; takové podmínky je nutno dodržovat.
- iii. Zaměstnavatelé by dále měli vynaložit přiměřené úsilí, aby vyhověli individuálním potřebám zaměstnanců ohledně ochrany soukromí. Může jít například o omezení přístupu k osobním údajům, anonymizaci určitých údajů nebo přidělení kódů či pseudonymů, pokud skutečná jména nejsou pro účel řízení potřebná.
- iv. V rozsahu a po dobu nezbytnou k zachování schopnosti organizace povyšovat, jmenovat nebo přijímat jiná podobná personální rozhodnutí je organizace od oznamovací povinnosti a od povinnosti umožnit volbu osvobozena.

c. Uplatňování zásady práva na přístup

- i. V doplňkové zásadě práva na přístup je uvedeno, z jakých důvodů může být požadovaný přístup k údajům v oblasti lidských zdrojů zamítnut nebo omezen. Zaměstnavatelé v EU musí samozřejmě dodržovat místní právní předpisy a zajistit, aby zaměstnanci z EU měli takový přístup k těmto informacím, jaký požadují právní předpisy v jejich zemích, bez ohledu na to, kde jsou tyto údaje zpracovávány a uchovávány. Rámec EU–USA pro ochranu údajů požaduje, aby organizace, která takové údaje zpracovává ve Spojených státech, spolupracovala při poskytování takového přístupu buď přímo, nebo prostřednictvím zaměstnavatele z EU.

d. Prosazování

- i. Pokud se osobní informace využívají pouze v rámci zaměstnaneckého vztahu, nese vůči zaměstnanci hlavní odpovědnost za údaje nadále organizace v EU. Z toho plyne, že pokud si evropští zaměstnanci stěžují na porušování svých práv na ochranu údajů a nejsou spokojeni s výsledky vnitřní kontroly, řízení o stížnosti a odvolacího řízení (nebo jiných postupů pro předkládání pracovních stížností použitelných podle kolektivní smlouvy), měli by se obrátit na příslušný státní nebo federální úřad pro ochranu osobních údajů nebo orgán příslušný pro pracovněprávní záležitosti v zemi, ve které jsou zaměstnáni. To platí i v případech, kdy za údajné nesprávné nakládání s jejich osobními informacemi nese odpovědnost organizace v USA, která informace od zaměstnavatele obdržela, a jde tedy o údajné porušení zásad. Tímto způsobem se nejúčinněji vyřeší, jak uvést do souladu často se navzájem překrývající práva a povinnosti stanovené místním pracovním právem a kolektivními smlouvami, jakož i právem na ochranu údajů.
- ii. Organizace v USA účastníci se rámce EU–USA pro ochranu údajů, která využívá údaje v oblasti lidských zdrojů předávané z EU v rámci zaměstnaneckého vztahu a která si přeje, aby se na taková předávání vztahoval rámec EU–USA pro ochranu údajů, se tedy musí zavázat, že bude v takových případech spolupracovat při vyšetřováních prováděných příslušnými úřady EU a že se podřídí jejich doporučení.

e. Používání zásady odpovědnosti za další předávání

- i. Pro příležitostné provozní potřeby v rámci zaměstnaneckého vztahu zúčastněné organizace v souvislosti s osobními údaji předanými na základě rámce EU–USA pro ochranu údajů, jako je rezervace letenky nebo hotelového pokoje či pojištění, mohou být osobní údaje malého počtu zaměstnanců předávány správcům, aniž by se uplatnila zásada práva na přístup nebo se s třetí stranou, která je správcem, uzavřela smlouva, jak jinak zásada odpovědnosti za další předávání požaduje, za předpokladu, že zúčastněná organizace dodržela zásady oznamovací povinnosti a možnosti volby.

## 10. Povinné smlouvy pro účely dalšího předávání

a. Smlouvy o zpracování údajů

- i. Jestliže dochází k předávání osobních údajů z EU do Spojených států pouze za účelem jejich zpracování, je nutné uzavřít smlouvu bez ohledu na účast zpracovatele v rámci EU–USA pro ochranu údajů.
- ii. Správci údajů v EU musí vždy při předání za účelem pouhého zpracování údajů uzavřít smlouvu, bez ohledu na to, zda ke zpracování dochází v EU nebo mimo ni a zda se zpracovatel účastní rámce EU–USA pro ochranu údajů či nikoli. Účelem smlouvy je zajistit, že zpracovatel:
1. jedná pouze podle pokynů správce;
  2. přijme vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám, neoprávněnému zpřístupnění nebo přístupu a je si vědom, zda je povoleno další předávání, a
  3. s ohledem na charakter zpracování pomůže správci odpovídat fyzickým osobám uplatňujícím svá práva podle těchto zásad.

- iii. Protože zúčastněné organizace poskytují odpovídající ochranu údajů, nemusí být smlouvy uzavírané s takovýmito organizacemi o pouhém zpracování údajů předem schvalovány.

b. Předávání v rámci kontrolované skupiny korporací nebo subjektů

- i. Jsou-li osobní informace předávány mezi dvěma správci v rámci kontrolované skupiny korporací nebo subjektů, zásada odpovědnosti za další předávání nevyžaduje vždy smlouvu. Správci údajů v rámci kontrolované skupiny korporací nebo subjektů mohou toto předávání založit na jiných nástrojích, jako jsou závazná podniková pravidla EU či jiné vnitroskupinové nástroje (např. programy dodržování předpisů a kontrolní programy), které zajistí kontinuitu ochrany osobních informací podle těchto zásad. V případě takového předávání zůstává za dodržování zásad odpovědná zúčastněná organizace.

c. Předávání mezi správci

- i. U předávání mezi správci nemusí být přijímající správce zúčastněnou organizací ani nemusí mít nezávislý odvolací mechanismus. Zúčastněná organizace musí s třetí stranou, která je přijímajícím správcem, uzavřít smlouvu, jež stanoví tutéž úroveň ochrany, jakou poskytuje rámec EU–USA pro ochranu údajů, a neobsahuje požadavek, aby třetí strana, která je správcem, byla zúčastněnou organizací nebo měla nezávislý odvolací mechanismus, za předpokladu, že zajistí mechanismus rovnocenný.

## 11. Řešení sporů a prosazování

- a. Zásada odvolání, prosazování a odpovědnosti stanoví, jakým způsobem se rámec EU–USA pro ochranu údajů prosazuje. Jak splnit požadavky písm. a) bodu ii) této zásady, je uvedeno v doplňkové zásadě o ověřování. Tato doplňková zásada se věnuje ustanovením písm. a) bodů i) a iii), která obě vyžadují nezávislé odvolací mechanismy. Tyto mechanismy mohou mít různou podobu, avšak musí splňovat požadavky zásady odvolání, prosazování a odpovědnosti. Organizace tyto požadavky splní některým z těchto způsobů: i) dodržováním programů na ochranu soukromí vytvořených v soukromém sektoru, které do svých pravidel zásady zahrnují a které obsahují účinné donucovací mechanismy typu popsaného v zásadě odvolání, prosazování a odpovědnosti; ii) podřízením se dozorovým orgánům vytvořeným na základě zákona nebo nařízení, které zajišťují vyřizování individuálních stížností a řešení sporů; nebo iii) závazkem spolupracovat s úřady pro ochranu osobních údajů nacházejícími se v EU nebo s jejich zmocněnými zástupci.
- b. Zde vyjmenované možnosti představují příklady a výčet není vyčerpávající. Soukromý sektor může vytvořit další donucovací mechanismy, pokud splňují požadavky zásady odvolání, prosazování a odpovědnosti a těchto doplňkových zásad. Upozorňujeme, že požadavky zásady odvolání, prosazování a odpovědnosti doplňují požadavek, že samoregulace musí být vymahatelná podle § 5 zákona o Federální obchodní komisi (15 U.S.C. § 45) zakazujícího nekalé nebo klamavé jednání, ustanovení 49 U.S.C. § 41712 zakazujícího dopravci nebo zprostředkovateli letenek, aby se v letecké dopravě nebo při prodeji letecké dopravy dopouštěli nekalé nebo klamavé praktiky, nebo jiného zákona či předpisu zakazujícího takové jednání.
- c. S cílem pomoci zajistit dodržování závazků rámce EU–USA pro ochranu údajů a podpořit správu programu musí organizace i jejich nezávislé odvolací mechanismy poskytnout informace týkající se rámce EU–USA pro ochranu údajů, když o to ministerstvo požádá. Kromě toho musí organizace rychle reagovat na stížnosti na dodržování zásad postoupené prostřednictvím ministerstva úřady pro ochranu osobních údajů. Odpověď by měla uvádět, zda je stížnost opodstatněná, a pokud ano, jak organizace problém napraví. Ministerstvo bude chránit důvěrnost informací, které obdrží, v souladu s právem USA.

d. Odvolací mechanismy

- i. Fyzické osoby by měly být podporovány, aby vznášely případné stížnosti u příslušných organizací předtím, než se obrátí na nezávislé odvolací mechanismy. Organizace musí fyzické osobě odpovědět do 45 dnů od obdržení stížnosti. To, zda je odvolací mechanismus nezávislý, je faktická otázka, a lze to prokázat zejména jeho nestranností, transparentním složením a financováním a prokazatelným osvědčením odpovídající činnosti. Jak požaduje zásada odvolání, prosazování a odpovědnosti, opravné prostředky musí být pro fyzické osoby snadno dostupné a bezplatné. Nezávislé subjekty pro řešení sporů jsou povinny přezkoumat každou stížnost přijatou od fyzických osob, ledaže by stížnosti byly zjevně bezdůvodné nebo by nebyly míněné vážně. To nebrání tomu, aby nezávislý subjekt pro řešení sporů provozující odvolací mechanismus stanovil kritéria přípustnosti stížností, avšak taková kritéria by měla být transparentní a odůvodněná (mohou například vyloučit stížnosti, které nespádají do oblasti působnosti daného programu nebo mají být řešeny jiným subjektem) a neměla by oslabovat závazek zabývat se oprávněnými stížnostmi. Odvolací mechanismy by dále měly fyzickým osobám při podání stížnosti poskytnout úplné a snadno dostupné informace o tom, jak probíhá postup při řešení sporů. Takové informace by měly obsahovat zmínku o praktikách uplatňovaných mechanismem při ochraně soukromí v souladu se zásadami. Mechanismy by měly rovněž spolupracovat při rozvoji nástrojů pro usnadnění řízení o stížnostech, jako jsou např. standardizované formuláře pro podávání stížností.
- ii. Nezávislé odvolací mechanismy musí na svých veřejných internetových stránkách uvádět informace o zásadách a službách, které na základě rámce EU–USA pro ochranu údajů poskytují. Tyto informace musí obsahovat: 1) informace o požadavcích zásad týkajících se nezávislých odvolacích mechanismů nebo odkaz na uvedené požadavky; 2) odkaz na internetové stránky ministerstva věnované rámci pro ochranu údajů; 3) vysvětlení, že jejich služby v oblasti řešení sporů na základě rámce EU–USA pro ochranu údajů jsou pro fyzické osoby bezplatné; 4) popis způsobu podání stížnosti v souvislosti se zásadami; 5) časovou lhůtu na vyřízení stížností v souvislosti se zásadami a 6) popis nabídky potenciálních opravných prostředků.
- iii. Nezávislé odvolací mechanismy musí zveřejňovat výroční zprávu, ve které uvedou souhrnnou statistiku týkající se jejich služeb v oblasti řešení sporů. Výroční zpráva musí obsahovat: 1) celkový počet stížností souvisejících se zásadami obdržených během sledovaného roku; 2) typy obdržených stížností; 3) měřítko kvality řešení sporů, jako je doba, za jakou jsou stížnosti vyřízeny, a 4) výsledky obdržených stížností, zejména počet a typy opravných prostředků nebo uložených sankcí.
- iv. Jak je stanoveno v příloze I, fyzické osoby mají k dispozici rozhodčí řízení, ve kterém se u zbytkových nároků rozhodne, zda zúčastněná organizace porušila své povinnosti podle těchto zásad vůči uvedené fyzické osobě a zda toto případné porušení zůstalo v plném rozsahu nebo částečně bez nápravy. Tato možnost je k dispozici pouze pro tyto účely. Tato možnost není k dispozici například v souvislosti s výjimkami z těchto zásad <sup>(15)</sup> nebo s ohledem na tvrzení, která se týkají odpovídající úrovně ochrany poskytované rámcem EU–USA pro ochranu údajů. V rámci této možnosti rozhodčího řízení má „panel rámce EU–USA pro ochranu údajů“ (složený z jednoho, či tří rozhodců podle toho, jak se strany dohodnou) pravomoc vydat individuální nepeněžní přiměřené opatření (jako je přístup, oprava, výmaz nebo vrácení údajů dotyčné fyzické osoby) nezbytné k nápravě porušení těchto zásad pouze v souvislosti s dotčenou fyzickou osobou. Fyzické osoby a zúčastněné organizace se budou moci domáhat soudního přezkumu a výkonu rozhodčích nálezů podle práva USA na základě federálního zákona o rozhodčím řízení.

e. Opravné prostředky a sankce

- i. Výsledkem využití opravných prostředků, které poskytuje nezávislý subjekt pro řešení sporů, by mělo být to, že organizace následky nedodržení zásad, pokud je to možné, odstraní nebo napraví a že její budoucí zpracování bude v souladu se zásadami, případně bude ukončeno zpracovávání osobních údajů fyzické osoby, jež vznesla stížnost. Sankce musí být dostatečně přísné, aby bylo zajištěno, že organizace bude zásady dodržovat. Škála různě přísných sankcí umožní subjektům pro řešení sporů přiměřeně reagovat na různě závažné případy nedodržení zásad. Sankce by měly zahrnovat jak zveřejnění zjištěných případů

<sup>(15)</sup> Zásady, přehled, bod 5.

nedodržení zásad, tak za určitých okolností požadavek na vymazání údajů <sup>(16)</sup>. Další sankce by mohly zahrnovat pozastavení a odnětí možnosti prokazovat se pečeti, náhradu škody vzniklé fyzickým osobám v důsledku nedodržení zásad nebo předběžné opatření. Nezávislé subjekty pro řešení sporů a samoregulační orgány soukromého sektoru musí oznamovat případy, kdy zúčastněné organizace nedodržují jejich rozhodnutí, příslušnému orgánu veřejné správy s rozhodovací pravomocí nebo soudům a informovat ministerstvo.

f. Činnost Federální obchodní komise

- i. Federální obchodní komise se zavázala přednostně přezkoumávat věci týkající se údajného nedodržení těchto zásad postoupené: i) samoregulačními orgány na ochranu soukromí a jinými nezávislými subjekty pro řešení sporů; ii) členskými státy EU a iii) ministerstvem, s cílem určit, zda byl porušen § 5 zákona o Federální obchodní komisi, který zakazuje nekalé nebo klamavé jednání či praktiky v oblasti obchodu. Dojde-li Federální obchodní komise k závěru, že existuje důvodné podezření, že ustanovení § 5 bylo porušeno, může dosáhnout vydání úředního příkazu k zastavení činnosti, který zakáže sporné praktiky, nebo může podat žalobu u federálního okrskového soudu, jenž – vyhoví-li žalobě – může vydat soudní příkaz se stejným účinkem. Patří sem nepravdivá tvrzení o dodržování zásad nebo účasti v rámci EU–USA pro ochranu údajů ze strany organizací, které již nejsou na seznamu organizací rámce pro ochranu údajů či se u ministerstva nikdy neautocertifikovaly. Federální obchodní komise může uložit občanskoprávní sankce za porušení úředního příkazu k zastavení činnosti a může postupovat proti neuposlechnutí soudního příkazu federálního soudu občanskoprávní nebo trestněprávní cestou. Federální obchodní komise oznámí veškeré své podniknuté kroky ministerstvu. Ministerstvo podněcuje ostatní orgány veřejné správy, aby mu podávaly informace o konečných výsledcích ve všech takových případech nebo o jiných rozhodnutích ve věci dodržování zásad.

g. Soustavné nedodržování zásad

- i. Jestliže organizace soustavně nedodržuje zásady rámce EU–USA pro ochranu údajů, ztrácí nárok na požívání výhod z něj plynoucích. Organizace, které soustavně nedodržují zásady, budou ministerstvem odstraněny ze seznamu organizací rámce pro ochranu údajů a musí vrátit nebo vymazat osobní informace, které na základě rámce EU–USA pro ochranu údajů obdržely.
- ii. K soustavnému nedodržování dochází tehdy, když se organizace, která se u ministerstva autocertifikovala, odmítá podřídit konečnému rozhodnutí samoregulačního orgánu na ochranu soukromí, nezávislého subjektu pro řešení sporů nebo orgánu veřejné správy či když takový orgán či subjekt, včetně ministerstva, rozhodne, že organizace nedodržuje zásady tak často, že již není věrohodné její tvrzení, že tak činí. V případech, kdy takové rozhodnutí učiní jiný subjekt než ministerstvo, musí organizace tyto skutečnosti neprodleně oznámit ministerstvu. Nesplnění této povinnosti může být předmětem žaloby podle zákona o nepravdivých tvrzeních (18 U.S.C. § 1001). Odstoupení organizace od samoregulačního programu soukromého sektoru na ochranu soukromí nebo nezávislého mechanismu pro řešení sporů ji nezbavuje povinnosti dodržovat tyto zásady a představovalo by jejich soustavné nedodržování.
- iii. Ministerstvo odstraní organizaci ze seznamu organizací rámce pro ochranu osobních údajů za soustavné nedodržování zásad, včetně situace, kdy reaguje na obdržené oznámení o takovém nedodržování od samotné organizace, od samoregulačního orgánu pro ochranu soukromí nebo od jiného nezávislého subjektu pro řešení sporů nebo od orgánu veřejné správy, avšak teprve po uplynutí lhůty 30 dnů poté, co organizaci upozorní a poskytne jí možnost reagovat <sup>(17)</sup>. Ze seznamu organizací rámce pro ochranu údajů vedeného ministerstvem je tedy zřejmé, které organizace mají a které již nemají zajištěny výhody plynoucí z rámce EU–USA pro ochranu údajů.
- iv. Organizace, která požádá o účast v samoregulačním orgánu za účelem opětovného splnění požadavků rámce EU–USA pro ochranu údajů, musí tomuto orgánu poskytnout úplné informace o své předchozí účasti v rámci EU–USA pro ochranu údajů.

<sup>(16)</sup> Nezávislé subjekty pro řešení sporů mají prostor pro uvážení, pokud jde o okolnosti, za nichž tyto sankce uplatňují. Jedním z faktorů, které je třeba při rozhodování o tom, zda by mělo být vyžadováno vymazání údajů, zohlednit, je citlivost daných údajů a dále okolnost, zda organizace shromáždila, používala nebo zpřístupnila informace v očividném rozporu se zásadami.

<sup>(17)</sup> Ministerstvo v oznámení uvede lhůtu, která bude v každém případě kratší než 30 dnů, již má organizace pro svoji reakci na oznámení k dispozici.

## 12. Možnost volby – načasování nesouhlasu

- a. Obecně je účelem zásady možnosti volby zajistit, aby byly osobní informace používány a zpřístupňovány způsobem, který je v souladu s očekáváními a volbami dotčené fyzické osoby. V souladu s tím by měla mít taková osoba právo využít možnosti vyslovit nesouhlas s používáním osobních informací pro přímý marketing kdykoli, v rámci přiměřených omezení stanovených organizací, jako je např. poskytnutí času, aby organizace mohla nesouhlas účinně zohlednit. Organizace může též požadovat dostatečné informace k potvrzení totožnosti osoby, která žádá o odvolání souhlasu. Ve Spojených státech mohou fyzické osoby vykonat tuto volbu prostřednictvím využití centrálního opt-out programu. V každém případě by fyzické osobě měly být poskytnuty snadno přístupné a finančně dostupné mechanismy, aby vykonala své právo volby.
- b. Podobně může organizace použít informace pro určité účely přímého marketingu tehdy, pokud nelze fyzické osobě poskytnout možnost vyslovit nesouhlas před jejich použitím, jestliže poskytne dané osobě bezprostředně poté (a na požádání kdykoli) možnost odmítnout (aniž by fyzické osobě vznikly náklady) příjem dalších sdělení přímého marketingu a jestliže organizace toto její přání splní.

## 13. Informace související s cestováním

- a. Informace o rezervacích letenek a další informace související s cestováním, např. o pravidelných cestujících, hotelových rezervacích nebo zvláštních potřebách, jako např. o zvláštních nábožensky odůvodněných požadavcích kladených na jídelníček či o nutné fyzické asistenci, mohou být předávány organizacím nacházejícím se mimo EU v několika různých případech. Podle nařízení GDPR mohou být osobní údaje v případě neexistence rozhodnutí o odpovídající ochraně předány do třetí země, pokud jsou poskytnuty vhodné záruky ochrany údajů podle článku 46 nařízení GDPR nebo ve zvláštních situacích, je-li splněna jedna z podmínek článku 49 nařízení GDPR (např. pokud subjekt údajů s předáním výslovně souhlasil). Organizace v USA přijímající zásady rámce EU–USA pro ochranu údajů, poskytují odpovídající ochranu osobních údajů, a proto mohou obdržet předávané údaje z EU na základě článku 45 nařízení GDPR, aniž by musely zavést nástroj pro předávání podle článku 46 nařízení GDPR nebo splňovat podmínky článku 49 nařízení GDPR. Vzhledem k tomu, že rámec EU–USA pro ochranu údajů obsahuje zvláštní pravidla pro citlivé informace, mohou být tyto informace (které někdy musí být shromažďovány, např. ve spojitosti s potřebami zákazníků, pokud jde o fyzickou asistenci) zahrnuty v údajích předávaných zúčastněným organizacím. V každém případě však musí organizace, která informace předává, dodržovat právní předpisy členského státu EU, v němž provádí svou činnost; a tyto právní předpisy mohou mimo jiné ukládat zvláštní podmínky pro nakládání s citlivými údaji.

## 14. Léčiva a zdravotnický materiál

- a. Uplatňování právních předpisů EU / členských států nebo zásad
  - i. Právní předpisy EU / členského státu se uplatní na shromažďování osobních údajů a jejich zpracování uskutečněné před předáním do Spojených států. Zásady se uplatní na údaje po jejich předání do Spojených států. Údaje používané pro farmaceutický výzkum a další účely by měly být v příslušných případech anonymizovány.
- b. Budoucí vědecký výzkum
  - i. Osobní údaje získané při konkrétní lékařské nebo farmaceutické výzkumné studii hrají často významnou roli v budoucím vědeckém výzkumu. Jsou-li osobní údaje shromážděné pro účely jedné výzkumné studie předány organizaci USA účastníci se rámce EU–USA pro ochranu údajů, smí organizace použít údaje k nové vědecké výzkumné činnosti, byl-li o tom subjekt údajů v prvním stupni vhodně uvědomen a byla-li mu poskytnuta možnost volby. Takové oznámení by mělo poskytnout informace o budoucím konkrétním využití údajů, jako jsou např. pravidelná následná šetření, související studie nebo uvádění na trh.

- ii. Je zřejmé, že ne všechny budoucí způsoby využití údajů lze vyjmenovat, protože nový způsob využití ve výzkumu může vzniknout na základě nových poznatků o původních údajích, nových lékařských objevů a pokroků, jakož i vývoje ve zdravotnictví a v legislativě. Oznámení by tedy mělo případně obsahovat vysvětlení, že osobní údaje mohou být využity při budoucích lékařských a farmaceutických výzkumných činnostech, které nelze dopředu předvídat. Jestliže využití údajů neodpovídá obecnému výzkumnému záměru (záměrům), pro který byly osobní údaje původně shromážděny nebo s nimiž dotčená fyzická osoba následně souhlasila, je nutno získat nový souhlas.
- c. Odstoupení od klinického hodnocení
  - i. Účastníci se mohou kdykoli rozhodnout odstoupit od klinického hodnocení nebo mohou být požádáni, aby od něj odstoupili. Osobní údaje shromážděné před odstoupením však mohou být nadále zpracovávány spolu s ostatními údaji shromážděnými v rámci klinického hodnocení, jestliže na to byl účastník jasně upozorněn v oznámení v době, kdy souhlasil se svou účastí.
- d. Předávání pro účely regulace a dohledu
  - i. Společnosti vyrábějící léčiva a zdravotnické prostředky smějí poskytovat osobní údaje z klinických hodnocení provedených v EU regulačním orgánům ve Spojených státech pro účely regulace a dohledu. Podobné předávání jiným stranám než regulačním orgánům, jako jsou společnosti a jiní výzkumní pracovníci, je povoleno v souladu se zásadami oznamovací povinnosti a možnosti volby.
- e. „Zaslepené“ studie
  - i. Z důvodu zajištění objektivit nesmějí při mnoha klinických hodnoceních účastníci a často ani samotní výzkumníci mít přístup k informacím o tom, jakému léčení se každý účastník podrobuje. Pokud by k nim měli přístup, ohrozilo by to platnost výzkumu a jeho výsledků. Účastníkům takových klinických hodnocení (označovaných jako „zaslepené“ studie) nemusí být přístup k údajům o jejich léčbě během hodnocení poskytnut, jestliže jim bylo toto omezení vysvětleno předtím, než se účastnili hodnocení, a jestliže by zpřístupnění takových informací ohrozilo integritu výzkumného úsilí.
  - ii. Souhlas s účastí na hodnocení za těchto podmínek je postačující pro vzdání se práva na přístup k informacím. Po dokončení hodnocení a provedení analýzy výsledků by účastníci měli mít přístup ke svým údajům, jestliže o to požádají. Měli by je požadovat především od lékaře nebo jiného poskytovatele lékařské péče, který je ošetřoval v rámci klinického hodnocení, či případně od organizace, jež si klinické hodnocení zadala.
- f. Sledování bezpečnosti a účinnosti výrobků
  - i. Společnost vyrábějící léčiva nebo zdravotnické prostředky nemusí ve svých opatřeních ke sledování bezpečnosti a účinnosti svých výrobků, včetně podávání zpráv o nežádoucích příhodách a sledování stavu pacientů/subjektů užívajících určitá léčiva či používajících určité zdravotnické prostředky, uplatňovat zásady týkající se oznamovací povinnosti, možnosti volby, odpovědnosti za další předávání a práva na přístup, pokud dodržování těchto zásad narušuje dodržování regulačních požadavků. To platí jak pro zprávy např. poskytovatelů lékařské péče společností vyrábějícím léčiva a zdravotnické prostředky, tak pro zprávy společností vyrábějících léčiva a zdravotnické prostředky orgánům veřejné správy, jako je např. Úřad pro potraviny a léčiva.
- g. Údaje kódované pomocí klíče
  - i. Výzkumné údaje jsou u zdroje zásadně kódovány hlavním zkoušejícím pomocí unikátního klíče tak, aby nebyla zřejmá totožnost konkrétních subjektů údajů. Farmaceutické společnosti financující takový výzkum klíč neoddrží. Kód k unikátnímu klíči má pouze výzkumný pracovník, který tak může za určitých okolností danou osobu identifikovat (např. je-li potřebný následný lékařský dohled). Zásady by se vztahovaly na předávání takto kódovaných údajů z EU do Spojených států, které jsou osobními údaji EU podle práva EU.

**15. Veřejné záznamy a veřejně přístupné informace**

- a. Organizace musí na osobní údaje z veřejně dostupných zdrojů uplatňovat zásadu zabezpečení, integrity údajů a účelového omezení a zásadu odvolání, prosazování a odpovědnosti. Tyto zásady se použijí také na osobní údaje shromážděné z veřejných záznamů (tj. z takových záznamů, které vedou vládní orgány nebo subjekty na jakékoli úrovni a které jsou obecně přístupné veřejnosti za účelem nahlédnutí).
- b. Zásady oznamovací povinnosti, možnosti volby a odpovědnosti za další předávání není nutno na informace z veřejných záznamů uplatňovat, pokud nejsou kombinovány s informacemi z neveřejných záznamů a pokud jsou dodrženy podmínky, které pro nahlížení stanovily příslušné orgány. Dále není obecně nutné uplatňovat zásady oznamovací povinnosti, možnosti volby a odpovědnosti za další předávání na veřejně přístupné informace, ledaže evropská předávající organizace upozorní na to, že takové informace podléhají omezením, která vyžadují, aby organizace uplatňovala tyto zásady pro zamýšlené účely. Organizace nenesou odpovědnost za to, jakým způsobem takové informace použijí ti, kteří je získají z uveřejněných materiálů.
- c. Pokud bude zjištěno, že organizace úmyslně zveřejnila osobní informace v rozporu se zásadami, aby ona či jiní mohli mít z těchto výjimek prospěch, přestane splňovat podmínky pro to, aby mohla využívat výhod rámce EU–USA pro ochranu údajů.
- d. Na informace z veřejných záznamů není nutné uplatňovat zásadu práva na přístup, pokud uvedené informace nejsou kombinovány s jinými osobními informacemi (kromě malého počtu informací používaných k indexaci nebo uspořádání informací z veřejných záznamů); je však třeba dodržovat veškeré podmínky nahlížení stanovené příslušnými orgány. Naopak v případech, kdy jsou informace z veřejných záznamů kombinovány s jinými informacemi z neveřejných záznamů (jinými, než je uvedeno výše), musí organizace poskytnout přístup k veškerým takovým informacím, pokud se na ně nevztahují jiné povolené výjimky.
- e. Stejně jako u informací z veřejných záznamů není nutné poskytovat přístup k informacím, které jsou již veřejně dostupné široké veřejnosti, pokud nejsou kombinovány s informacemi, jež veřejně dostupné nejsou. Organizace, které se zabývají prodejem veřejně dostupných informací, mohou za zodpovězení žádostí o poskytnutí přístupu uložit svůj obvyklý poplatek. Eventuálně mohou fyzické osoby žádat o přístup ke svým informacím organizací, která je původně shromáždila.

**16. Žádosti orgánů veřejné moci o přístup**

- a. Za účelem transparentnosti oprávněných žádostí orgánů veřejné moci o přístup k osobním informacím mohou zúčastněné organizace dobrovolně vydávat pravidelné zprávy o transparentnosti, které uvádějí počet žádostí o osobní informace, jež organizace obdržely od orgánů veřejné moci z důvodu prosazování práva nebo národní bezpečnosti, jsou-li tato sdělení přípustná podle platného práva.
- b. Informace poskytnuté v těchto zprávách zúčastněnými organizacemi společně s informacemi zveřejněnými zpravodajskou komunitou a s dalšími informacemi mohou být použity jako podklad pravidelného společného přezkumu fungování rámce EU–USA pro ochranu údajů v souladu s těmito zásadami.
- c. Neoznámení v souladu s písm. a) bodem xii) zásady oznamovací povinnosti nebrání organizaci reagovat na jakoukoli oprávněnou žádost, ani tuto možnost neoslabuje.

## PŘÍLOHA I: ROZHODČÍ MODEL

Tato příloha I stanoví podmínky, za kterých jsou organizace účastníci se rámce EU–USA pro ochranu údajů povinny rozhodovat žaloby podle zásady odvolání, prosazování a odpovědnosti. Možnost závazného rozhodčího řízení popsána níže se vztahuje na určité „zbytkové“ nároky v souvislosti s údaji, pro které platí rámec EU–USA pro ochranu údajů. Účelem této možnosti je poskytnout rychlý, nezávislý a spravedlivý mechanismus podle volby fyzických osob k řešení údajných porušení těchto zásad nevyřešených žádnými jinými případnými mechanismy na základě rámce EU–USA pro ochranu údajů.

**A. Oblast působnosti**

V rozhodčím řízení, které mají fyzické osoby k dispozici, se u zbytkových nároků rozhodne, zda zúčastněná organizace porušila své povinnosti podle těchto zásad vůči uvedené fyzické osobě a zda toto případné porušení zůstalo v plném rozsahu nebo částečně bez nápravy. Tato možnost je k dispozici pouze pro tyto účely. Tato možnost není k dispozici například v souvislosti s výjimkami z těchto zásad<sup>(1)</sup> nebo s ohledem na tvrzení, která se týkají odpovídající úrovně ochrany poskytované rámcem EU–USA pro ochranu údajů.

**B. Dostupné opravné prostředky**

V rámci této možnosti rozhodčího řízení má „panel rámce EU–USA pro ochranu údajů“ (rozhodčí panel složený z jednoho či tří rozhodců podle toho, jak se strany dohodnou) pravomoc vydat individuální nepeněžní přiměřené opatření (jako je přístup, oprava, výmaz nebo vrácení údajů dotyčné fyzické osoby) nezbytné k nápravě porušení těchto zásad pouze v souvislosti s dotčenou fyzickou osobou. To jsou jediné pravomoci panelu rámce EU–USA pro ochranu údajů v souvislosti s opravnými prostředky. Při rozhodování o opravných prostředcích musí vzít panel rámce EU–USA pro ochranu údajů v úvahu jiné opravné prostředky, které již uložily jiné mechanismy na základě rámce EU–USA pro ochranu údajů. K dispozici není náhrada škody, nákladů, poplatků ani jiné opravné prostředky. Každá strana nese náklady na odměny svých advokátů.

**C. Požadavky před rozhodčím řízením**

Fyzická osoba, která se rozhodne využít této možnosti rozhodčího řízení, musí před podáním rozhodčí žaloby učinit tyto kroky: 1) předložit stížnost na údajné porušení přímo organizaci a poskytnout jí příležitost tuto stížnost vyřešit ve lhůtě stanovené v oddíle d) bodě i) doplňkové zásady o řešení sporů a prosazování; 2) využít bezplatný nezávislý odvolací mechanismus podle těchto zásad a 3) předložit věc prostřednictvím svého úřadu pro ochranu osobních údajů ministerstvu a poskytnout mu příležitost vynaložit maximální úsilí na bezplatné vyřešení věci ve lhůtě stanovené v dopise odboru pro mezinárodní obchod ministerstva.

Této možnosti se nelze dovolávat, jestliže totéž údajné porušení těchto zásad, jež je předmětem žaloby fyzické osoby, 1) již bylo předmětem závazného rozhodčího řízení; 2) bylo předmětem pravomocného rozsudku vyneseného v soudním sporu, jehož byla fyzická osoba účastníkem, nebo 3) již bylo stranami urovnáno. Této možnosti se kromě toho nelze dovolávat, jestliže úřad pro ochranu osobních údajů 1) má pravomoc podle doplňkové zásady o úloze úřadů pro ochranu osobních údajů nebo doplňkové zásady o údajích v oblasti lidských zdrojů, nebo 2) je oprávněn řešit údajné porušení přímo s organizací. Pravomoc úřadu pro ochranu osobních údajů řešit tentýž nárok vůči správci údajů z EU sama o sobě nevylučuje využití této možnosti rozhodčího řízení proti jinému právnímu subjektu, který není vázán pravomocí úřadu pro ochranu osobních údajů.

**D. Závaznost rozhodnutí**

Rozhodnutí fyzické osoby dovolávat se této možnosti závazného rozhodčího řízení je zcela dobrovolné. Rozhodčí nálezy budou závazné pro všechny účastníky rozhodčího řízení. Jakmile fyzická osoba uvedené možnosti využije, vzdává se možnosti domáhat se opatření v souvislosti s tímž údajným porušením u jiného orgánu, s výjimkou případů, kdy nepeněžní přiměřené opatření nenapraví údajné porušení v plném rozsahu; tehdy využití rozhodčího řízení fyzickou osobou nevylučuje žalobu o náhradu škody, kterou je jinak možné podat k soudu.

<sup>(1)</sup> Zásady, přehled, bod 5.

## E. Přezkum a prosazování

Fyzické osoby a zúčastněné organizace se budou moci domáhat soudního přezkumu a výkonu rozhodčích nálezů podle práva Spojených států na základě federálního zákona o rozhodčím řízení<sup>(2)</sup>. Veškeré tyto věci musí být předloženy federálnímu okrskovému soudu, který je územně příslušný pro hlavní místo podnikání zúčastněné organizace.

Tato možnost rozhodčího řízení má řešit jednotlivé spory a rozhodčí nálezy nemají fungovat jako přesvědčivý nebo závazný precedens v záležitostech, které se týkají jiných stran, včetně budoucích rozhodčích řízení či řízení u soudů v EU nebo v USA či u Federální obchodní komise.

## F. Rozhodčí panel

Strany vyberou rozhodce pro panel rámce EU–USA pro ochranu údajů ze seznamu rozhodců popsaného níže.

V souladu s použitelným právem zpracuje ministerstvo a Komise seznam alespoň deseti rozhodců vybraných na základě nezávislosti, profesní bezúhonnosti a odborných znalostí. V souvislosti s tímto procesem platí následující:

Rozhodci:

- 1) zůstanou na seznamu po dobu tří let, nenastanou-li výjimečné nebo odůvodněné okolnosti pro odstranění z tohoto seznamu, přičemž toto období lze ministerstvem po předchozím oznámení Komisi prodloužit o další tři roky;
- 2) nepodléhají žádným pokynům žádné ze stran, žádné zúčastněné organizace, Spojených států, EU, žádného členského státu EU ani žádného orgánu státní správy, orgánu veřejné moci nebo donucovacího orgánu, ani k nim nejsou přidruženi a
- 3) musí mít povolení vykonávat právní praxi ve Spojených státech, být odborníky na právo ochrany soukromí Spojených států a mít odborné znalosti právních předpisů EU o ochraně údajů.

<sup>(2)</sup> Kapitola 2 federálního zákona o rozhodčím řízení (Federal Arbitration Act, dále jen „zákon FAA“) stanoví, že „[r]ozhodčí dohoda nebo rozhodčí nálezy vyplývající z právního vztahu, ať již smluvního či mimosmluvního, který se považuje za obchodní, včetně transakce, smlouvy nebo dohody popsané v [§ 2 FAA], spadá pod úmluvu [o uznání 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. Zákon FAA dále stanoví, že „[m]á se za to, že dohoda nebo nálezy vyplývající z tohoto vztahu, který je pouze mezi občany Spojených států, nespadá pod [Newyorskou] úmluvu, pokud se vztah netýká majetku v zahraničí, nepředpokládá plnění či výkon v zahraničí nebo nemá nějaký jiný přiměřený vztah k jedné či více cizím zemím“. *Tamtéž*. Podle kapitoly 2 „kterýkoli z účastníků rozhodčího řízení může kterýkoli soud příslušný podle této kapitoly požádat o vydání příkazu, jenž potvrdí nálezy proti druhé straně rozhodčího řízení. Soud nálezy potvrdí, neshledá-li žádný z důvodů k odepření nebo odložení uznání či výkonu nálezů uvedených v dotyčné [Newyorské] úmluvě“. *Tamtéž*. § 207. Kapitola 2 dále stanoví, že „[p]řevodně příslušné ... k projednání žaloby nebo zahájení řízení [podle Newyorské úmluvy] ... jsou okrskové soudy Spojených států bez ohledu na spornou částku“. *Tamtéž*. § 203.

Kapitola 2 také stanoví, že „kapitola 1 se použije na žaloby vznesené a řízení zahájená podle této kapitoly, pokud uvedená kapitola není v rozporu s touto kapitolou nebo s [Newyorskou] úmluvou ratifikovanou Spojenými státy“. *Tamtéž*. § 208. Kapitola 1 zase stanoví, že „[p]římé ustanovení ve ... smlouvě, která dokládá obchodní transakci, o urovnání sporu vyplývajícího z této smlouvy nebo transakce rozhodčím řízením či o odepření plnit tuto smlouvu nebo transakci v celém či částečném rozsahu nebo písemná dohoda podrobit stávající spor vyplývající z této smlouvy, transakce či odepření rozhodčím řízením jsou platné, neodvolatelné a vykonatelné, neexistují-li podle zákona nebo podle práva ekvity důvody ke zrušení smlouvy“. *Tamtéž*. § 2. Kapitola 1 dále stanoví, že „kterýkoli účastník rozhodčího řízení může takto určený soud požádat o vydání příkazu, který nálezy potvrdí, a soud musí na základě toho tento příkaz vydat, nebude-li nálezy zrušen, upraven nebo opraven, jak předepisují § 10 a 11 [federálního zákona o rozhodčím řízení]“. *Tamtéž*. § 9.

## G. Postupy pro rozhodčí řízení

V souladu s použitelným právem se ministerstvo a Komise se dohodly na přijetí pravidel rozhodčího řízení, která upravují řízení vedená u panelu rámce EU–USA pro ochranu údajů <sup>(3)</sup>. V případě, že je třeba pravidla upravující řízení změnit, se ministerstvo a Komise dohodnou na změně uvedených pravidel nebo případně na přijetí jiného souboru stávajících zavedených postupů pro rozhodčí řízení v USA v závislosti na každém z těchto kritérií:

1. Fyzická osoba může zahájit závazné rozhodčí řízení v závislosti na ustanovení o požadavcích před rozhodčím řízením výše doručení oznámení organizaci. Oznámení obsahuje shrnutí kroků učiněných podle části C za účelem vyřešení nároku, popis údajného porušení a podle vlastního výběru fyzické osoby případné podkladové dokumenty a materiály a/nebo právní výklad, který se týká uplatňovaného nároku.
2. Budou vypracovány postupy, které zajistí, aby u téhož porušení, jež je předmětem žaloby fyzické osoby, nebyly uplatněny duplicitní opravné prostředky nebo postupy.
3. Souběžně s rozhodčím řízením může konat Federální obchodní komise.
4. Těchto rozhodčích řízení se nesmí účastnit žádný zástupce USA, EU, žádného členského státu EU ani žádného orgánu státní správy, orgánu veřejné moci nebo donucovacího orgánu za předpokladu, že na žádost fyzické osoby z EU mohou úřady pro ochranu osobních údajů pouze poskytnout pomoc při přípravě oznámení, ale nesmějí mít přístup k listinám či skutečnostem ani k žádným jiným materiálům spojeným s těmito rozhodčími řízeními.
5. Místem konání rozhodčího řízení budou Spojené státy a fyzická osoba si může vybrat, že se bezplatně zúčastní prostřednictvím videa nebo telefonu. Nebude vyžadována osobní účast.
6. Jazykem rozhodčího řízení bude angličtina, nedohodnou-li se účastníci jinak. Na základě odůvodněné žádosti a s přihlédnutím ke skutečnosti, zda fyzickou osobu zastupuje advokát, bude fyzické osobě bezplatně poskytnuto tlumočení rozhodčího jednání i překlad rozhodčích materiálů, neshledá-li panel rámce EU–USA pro ochranu údajů, že vzhledem k okolnostem konkrétního rozhodčího řízení by to vedlo k neodůvodněným nebo nepřiměřeným nákladům.
7. S materiály předloženými rozhodcům bude zacházeno jako s důvěrnými a budou využity pouze v souvislosti s rozhodčím řízením.
8. V případě potřeby lze povolit individuální zpřístupnění listin nebo skutečností, se kterými budou účastníci zacházet jako s důvěrnými a které budou využity pouze v souvislosti s rozhodčím řízením.
9. Rozhodčí řízení by měla skončit do 90 dnů od doručení oznámení žalované organizaci, nedohodnou-li se strany jinak.

<sup>(3)</sup> Ministerstvo vybralo Mezinárodní středisko pro řešení sporů (International Centre for Dispute Resolution, dále také jako „středisko ICDR“), mezinárodní divizi Americké arbitrážní asociace (American Arbitration Association, dále také jako „asociace AAA“) (společně také jako „středisko ICDR-AAA“), aby řídilo rozhodčí řízení podle přílohy I zásad a spravovalo rozhodčí fond uvedený ve zmíněné příloze. 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 na úpravě pravidel rozhodčího řízení a kodexu chování tak, aby odrážely aktualizace na základě rámce EU–USA pro ochranu údajů, a ministerstvo bude na těchto aktualizacích spolupracovat se střediskem ICDR-AAA.

## H. Náklady

Rozhodci by měli učinit přiměřené kroky k minimalizaci nákladů nebo poplatků spojených s rozhodčím řízením.

V souladu s použitelným právem usnadní ministerstvo správu fondu, do kterého budou zúčastněné organizace muset hradit příspěvky založené částečně na velikosti organizace, jenž pokryjí náklady na rozhodčí řízení, včetně poplatků pro rozhodce, a to do maximální stanovené výše (dále též „strop“). Fond bude spravovat třetí strana, která bude pravidelně předkládat ministerstvu zprávy o fungování fondu. Ministerstvo bude s touto třetí stranou spolupracovat na pravidelném přezkumu fungování fondu, včetně nutnosti upravit výši příspěvků nebo stropů nákladů rozhodčího řízení, a posoudí mj. počet rozhodčích řízení a jejich náklady a načasování, přičemž panuje shoda na tom, že zúčastněné organizace nebudou nadměrně finančně zatíženy. Ministerstvo oznámí Komisi výsledek těchto přezkumů provedených spolu s třetí stranou a předem jí oznámí veškeré úpravy výše příspěvků. Na základě tohoto ustanovení ani z žádného fondu podle tohoto ustanovení se nehradí odměny advokátům.

---

## PŘÍLOHA II



**MINISTERSTVO OBCHODU SPOJENÝCH STÁTŮ**  
**Ministryně obchodu**  
Washington, D.C. 20230

6. července 2023

Vážený pan Didier Reynders  
Komisař pro spravedlnost  
Evropská komise  
Rue de la Loi/Westraat 200  
1049 Bruxelles/Brussel  
Belgique/België

Vážený pane komisaři Reyndersi,

jménem Spojených států bych Vám ráda předala soubor dokumentů rámce EU–USA pro ochranu údajů, který ve spojení s výkonným dekretem č. 14086 „Posílení záruk pro činnosti USA v oblasti signálového zpravodajství“ a s 28 CFR částí 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 nové záruky, které mají zajistit, aby činnosti USA v oblasti signálového zpravodajství byly nezbytné a přiměřené při sledování stanovených cílů národní bezpečnosti, a nový mechanismus, který fyzickým osobám z Evropské unie (dále jen „EU“) umožní domáhat se nápravy, pokud se domnívají, že jsou v rozporu se zákonem cílem činností v oblasti signálového zpravodajství, což společně zajistí ochranu osobních údajů EU. Rámec EU–USA pro ochranu údajů podpoří inkluzivní a konkurenceschopnou digitální ekonomiku. Oba bychom měli být hrdí na zlepšení uvedená v tomto rámci, která posílí ochranu soukromí na celém světě. Tento balíček spolu s výkonným dekretem, nařízeními a dalšími materiály dostupnými z veřejných zdrojů poskytuje velmi pevný základ pro nové zjištění Evropské komise o odpovídající úrovni ochrany (<sup>1</sup>).

Přílohou jsou tyto dokumenty:

- zásady rámce EU–USA pro ochranu údajů, včetně doplňkových zásad (společně dále jen „zásady“) a příloha I těchto zásad (tj. příloha, která stanoví podmínky, za nichž jsou organizace rámce ochrany údajů povinny rozhodovat o určitých zbytkových nárocích týkajících se osobních údajů, na něž se tyto zásady vztahují),
- dopis odboru pro mezinárodní obchod ministerstva, který spravuje program rámce pro ochranu údajů, v němž jsou popsány závazky, které naše ministerstvo přijalo k zajištění účinného fungování rámce EU–USA pro ochranu údajů,
- dopis Federální obchodní komise popisující její postupy prosazování zásad,
- dopis Ministerstva dopravy popisující jeho postupy prosazování zásad,
- dopis vypracovaný Úřadem ředitele národních zpravodajských služeb týkající se záruk a omezení vztahujících se na národní bezpečnostní orgány USA a
- dopis Ministerstva spravedlnosti, který se týká záruk a omezení v souvislosti s přístupem vlády USA k osobním údajům pro účely prosazování práva a veřejného zájmu.

(<sup>1</sup>) Za předpokladu, že se rozhodnutí Komise o odpovídající ochraně poskytované rámcem EU–USA pro ochranu údajů vztahuje na Island, Lichtenštejnsko a Norsko, bude se rámec EU–USA pro ochranu údajů vztahovat jak na EU, tak na tyto tři země.

Balíček týkající se rámce EU–USA pro ochranu údajů bude zveřejněn na internetových stránkách ministerstva věnovaných rámci pro ochranu údajů a zásady a příloha I zásad nabudou účinnosti dnem vstupu rozhodnutí Evropské komise o odpovídající ochraně v platnost.

Ujišťuji Vás, že Spojené státy berou tyto závazky vážně. Těšíme se na spolupráci s Vámi při provádění rámce EU–USA pro ochranu údajů a na to, jak společně zahájíme další fázi tohoto procesu.

S úctou



Gina M. RAIMONDO

---

## PŘÍLOHA III



**UNITED STATES DEPARTMENT OF COMMERCE**  
**International Trade Administration**  
Washington, D C 20230

12. prosince 2022

Vážený pan Didier Reynders  
Komisař pro spravedlnost  
Evropská komise  
Rue de la Loi/Westraat 200  
1049 Bruxelles/Brussel  
Belgique/België

Vážený pane komisaři Reyndersi,

jménem odboru pro mezinárodní obchod bych ráda popsala závazky, které Ministerstvo obchodu (dále jen „ministerstvo“) převzalo k zajištění ochrany osobních údajů prostřednictvím správy programu rámce pro ochranu údajů a dohledu nad ním. Dokončení rámce EU–USA pro ochranu údajů je významným počinem pro ochranu soukromí i pro obchod na obou stranách Atlantiku, neboť díky němu si mohou být obyvatelé EU jisti, že jejich údaje budou chráněny a že budou mít právní prostředky k řešení případných obav, jež by s jejich údaji souvisely, a umožní tisícům podniků nadále investovat a jinak se zapojit do obchodu přes Atlantik ve prospěch našich hospodářství a občanů. Rámec EU–USA pro ochranu údajů odráží roky tvrdé práce a spolupráce s Vámi a Vašimi kolegy v Evropské komisi (dále jen „Komise“). Těšíme se na další spolupráci s Komisí ve snaze zajistit, aby toto společné úsilí účinně fungovalo.

Rámec EU–USA pro ochranu údajů přinese občanům i podnikům značné výhody. Za prvé stanoví významný soubor opatření na ochranu osobních údajů fyzických osob z EU předávaných do Spojených států. Od zúčastněných organizací USA požaduje, aby vypracovaly vyhovující politiku ochrany soukromí, veřejně se zavázaly dodržovat „zásady rámce EU–USA pro ochranu údajů“, včetně doplňkových zásad (dále společně jako „zásady“), a přílohu I zásad (tj. přílohu, která stanoví podmínky, za nichž jsou organizace rámce EU–USA pro ochranu údajů povinny rozhodovat o určitých zbytkových nárocích týkajících se osobních údajů, na něž se tyto zásady vztahují) tak, aby byl jejich závazek právně vymahatelný podle práva Spojených států<sup>(1)</sup>, každý rok u ministerstva opětovně certifikovaly dodržování uvedených zásad, zajistily fyzickým osobám z EU bezplatné nezávislé řešení sporů, podrobily se vyšetřovací a donucovací pravomoci orgánu USA zřízeného zákonem uvedeného v zásadách (např. Federální obchodní komise a Ministerstva dopravy) nebo orgánu USA zřízeného zákonem uvedeného v budoucí příloze zásad. I když rozhodnutí organizace autocertifikovat se je dobrovolné, jakmile se k dodržování rámce EU–USA pro ochranu údajů veřejně zaváže, je její závazek právně vymahatelný podle práva USA. Federální obchodní komise, Ministerstvem dopravy nebo jiným orgánem USA zřízeným zákonem v závislosti na tom, který orgán má nad zúčastněnou organizací pravomoc. Za druhé, rámec EU–USA pro ochranu údajů umožní podnikům ve Spojených státech, včetně dceřiných společností evropských podniků nacházejících se ve Spojených státech, přijímat osobní údaje z Evropské unie, čímž se usnadní toky údajů, které podporují transatlantický obchod. Toky

<sup>(1)</sup> Organizace, které autocertifikovaly svůj závazek dodržovat rámcové zásady štítu EU–USA na ochranu soukromí a chtějí využívat výhod plynoucích z účasti v rámci EU–USA pro ochranu údajů, musí dodržovat „zásady rámce EU–USA pro ochranu údajů“. Tento závazek dodržovat „zásady rámce EU–USA pro ochranu údajů“ musí být co nejdříve, nejpozději však do tří měsíců od data účinnosti „zásad rámce EU–USA pro ochranu údajů“, promítnut do politik ochrany soukromí těchto zúčastněných organizací. (Viz písm. e) doplňkové zásady o autocertifikaci).

údajů mezi Spojenými státy a Evropskou unií jsou největší na světě a jsou základem hospodářského vztahu mezi USA a EU ve výši 7,1 bilionu USD, který podporuje miliony pracovních míst na obou stranách Atlantiku. Podniky, které se opírají o transatlantické toky údajů, pocházejí ze všech průmyslových odvětví a jsou mezi nimi některé z 500 nejvýznamnějších firem podle časopisu Fortune i mnoho malých a středních podniků. Transatlantické toky údajů umožňují organizacím USA zpracovávat údaje potřebné k nabízení zboží, služeb a pracovních příležitostí Evropanům.

Ministerstvo je odhodláno úzce a produktivně spolupracovat se svými protějšky z EU s cílem účinně spravovat program rámce pro ochranu údajů a dohlížet na něj. Tento závazek se odráží ve vývoji a neustálém zdokonalování různých zdrojů ministerstva s cílem pomoci organizacím s procesem autocertifikace, vytvoření internetových stránek pro poskytování cílených informací zúčastněným stranám, spolupráci s Komisí a evropskými úřady pro ochranu osobních údajů s cílem vypracovat pokyny, které objasní důležité prvky rámce EU–USA pro ochranu údajů, aktivní pomoci s cílem zajistit lepší pochopení povinností organizací v oblasti ochrany údajů a dohledu nad dodržováním požadavků programu ze strany organizací a jeho sledování.

Naše pokračující spolupráce s protějšky z EU, kterých si vážíme, umožní ministerstvu zajistit účinné fungování rámce EU–USA pro ochranu údajů. Vláda Spojených států amerických již dlouho spolupracuje s Komisí na prosazování společných zásad ochrany údajů, překlenutí rozdílů v našich právních přístupech a zároveň na podpoře obchodu a hospodářského růstu v Evropské unii a ve Spojených státech. Jsme přesvědčeni, že rámec EU–USA pro ochranu údajů, který je příkladem této spolupráce, umožní Komisi vydat nové rozhodnutí o odpovídající ochraně, které umožní organizacím využívat rámec EU–USA pro ochranu údajů k předávání osobních údajů z Evropské unie do Spojených států v souladu s právem EU.

### **Správa programu rámce pro ochranu údajů a dohled nad ním ze strany Ministerstva obchodu**

Ministerstvo je pevně odhodláno účinně spravovat program rámce pro ochranu údajů a dohlížet na něj a vyvine odpovídající úsilí a vyčlení odpovídající zdroje na dosažení tohoto cíle. Ministerstvo povede a poskytne veřejnosti oficiální seznam organizací USA, jež se u ministerstva autocertifikovaly a přijaly svůj závazek dodržovat tyto zásady (dále též „seznam organizací rámce pro ochranu údajů“), který aktualizuje na základě každoročních podání zúčastněných organizací týkajících se opětovné certifikace, a bude z něj odstraňovat organizace, pokud dobrovolně vystoupí, neabsolvuji každoroční opětovnou certifikaci v souladu s postupy ministerstva nebo bude shledáno, že soustavně nedodržují zásady. Ministerstvo také povede a poskytne veřejnosti oficiální rejstřík organizací USA, které byly ze seznamu organizací rámce pro ochranu údajů odstraněny, a uvede důvod, proč byla každá organizace odstraněna. Výše uvedený oficiální seznam a rejstřík budou veřejnosti k dispozici na internetových stránkách ministerstva věnovaných rámci pro ochranu údajů. Internetové stránky rámce pro ochranu údajů budou zřetelně uvádět, že každá organizace odstraněná ze seznamu rámce pro ochranu údajů musí přestat prohlašovat, že se rámce EU–USA pro ochranu údajů účastní nebo že ho dodržuje, a že může obdržet osobní informace na základě tohoto rámce. Tato organizace však musí i nadále používat tyto zásady na osobní informace, které obdržela během své účasti v rámci EU–USA pro ochranu údajů, pokud si tyto informace ponechá. Ministerstvo se na podporu svého zastřešujícího a trvalého závazku k účinné správě programu rámce pro ochranu údajů a dohledu nad ním konkrétně zavazuje, že učiní následující kroky:

#### **Ověřování požadavků na autocertifikaci**

- Než ministerstvo dokončí počáteční autocertifikaci organizace nebo její každoroční opětovnou certifikaci (dále společně jako „autocertifikace“) a umístí organizaci na seznam organizací rámce pro ochranu údajů či ji na tomto seznamu ponechá, ověří, že organizace splnila alespoň příslušné požadavky uvedené v doplňkové zásadě o autocertifikaci, ve které se stanoví, jaké informace musí organizace ve své autocertifikaci ministerstvu předložit, že v příslušnou dobu poskytla svou politiku ochrany soukromí, ve kterých fyzické osoby informuje o všech třinácti vyjmenovaných prvcích stanovených v zásadě oznamovací povinnosti. Ministerstvo ověří, že organizace:

- identifikovala organizaci, která předkládá svou autocertifikaci, jakož i všechny subjekty v USA nebo dceřiné společnosti v USA organizace, která předkládá autocertifikaci, které rovněž dodržují zásady a u nichž si organizace přeje, aby se na ně její autocertifikace rovněž vztahovala,
- poskytla požadované kontaktní údaje organizace (např. kontaktní údaje konkrétní osoby (osob) a/nebo úřadu (úřadů) v rámci organizace, která předkládá svou autocertifikaci, odpovědných za vyřizování stížností, žádostí o přístup a jakýchkoli dalších otázek vyplývajících z rámce EU–USA pro ochranu údajů),
- popsala účel nebo účely, pro které by organizace shromažďovala a používala osobní údaje získané z Evropské unie,
- uvedla, jaké osobní údaje budou z Evropské unie získány na základě rámce EU–USA pro ochranu údajů, a proto se na ně bude vztahovat její autocertifikace,
- má-li organizace veřejné internetové stránky, poskytla internetovou adresu, na níž je na uvedených internetových stránkách příslušná politika ochrany soukromí dostupná, nebo nemá-li organizace veřejné internetové stránky, poskytla ministerstvu kopii příslušné politiky ochrany soukromí a uvedla, kde se s uvedenou politikou mohou dotčené fyzické osoby seznámit (tj. dotčení zaměstnanci, pokud je příslušná politika ochrany soukromí politikou související s lidskými zdroji, nebo veřejnost, pokud příslušná politika ochrany soukromí nesouvisí s lidskými zdroji),
- zařadila do své politiky ochrany soukromí v příslušnou dobu (tj. zpočátku pouze do návrhu politiky ochrany soukromí společně s podáním počáteční autocertifikace, v opačném případě v konečné a případně zveřejněné verzi politiky ochrany soukromí) prohlášení, že dodržuje zásady, a hypertextový odkaz na internetové stránky ministerstva věnované rámci pro ochranu údajů nebo adresu těchto internetových stránek (např. domovskou stránku nebo internetovou stránku seznamu organizací rámce pro ochranu údajů),
- začlenila do své příslušné politiky ochrany soukromí ve vhodnou dobu všech dvanáct dalších vyjmenovaných prvků stanovených v zásadě oznamovací povinnosti (např. možnost dotčené fyzické osoby z EU uchýlit se za určitých podmínek k závaznému rozhodčímu řízení, požadavek zpřístupnit osobní informace v reakci na oprávněné žádosti orgánů veřejné moci, mj. s cílem splnit požadavky v souvislosti s národní bezpečností nebo prosazováním práva, a svou odpovědnost v případě dalšího předání údajů třetím stranám),
- označila konkrétní subjekt zřízený zákonem, který je příslušný projednávat stížnosti na organizaci ohledně případných nekalých nebo klamavých praktik a porušení předpisů na ochranu soukromí (a který je uveden v zásadách či v jejich budoucí příloze),
- označila případné programy na ochranu soukromí, jichž se organizace účastní,
- určila, zda je příslušnou metodou (tj. následnými postupy, které musí stanovit) pro ověření souladu se zásadami „sebehodnocení“ (tj. interní ověřování) nebo „externí přezkoumání souladu“ (tj. ověřování třetí stranou), a pokud určila, že příslušnou metodou je externí přezkoumání souladu, určila rovněž třetí stranu, která tento přezkoumání provedla,
- označila příslušný nezávislý odvolací mechanismus, který je k dispozici pro řešení stížností podaných podle zásad a pro poskytování náležitého bezplatného opravného prostředku dotčené fyzické osobě.
- Pokud si organizace zvolila nezávislý odvolací mechanismus poskytovaný subjektem pro alternativní řešení sporů ze soukromého sektoru, začlenila do své příslušné politiky ochrany soukromí hypertextový odkaz na příslušné internetové stránky nebo formulář pro podání stížnosti k tomuto mechanismu, který je k dispozici pro šetření nevyřešených stížností podaných na základě zásad, nebo jejich internetovou adresu.
- Pokud má organizace povinnost spolupracovat s úřady pro ochranu osobních údajů při vyšetřování a řešení stížností předložených na základě zásad (tj. pokud jde o údaje v oblasti lidských zdrojů předávané z Evropské unie v rámci zaměstnaneckého vztahu) nebo si takovou spolupráci zvolila, deklarovala svůj závazek spolupracovat s úřady pro ochranu osobních údajů a dodržovat jejich související doporučení přijmout konkrétní opatření k dodržování zásad.

- Ministerstvo rovněž ověří, zda je autocertifikace organizace v souladu s jejími příslušnými politikami ochrany soukromí. Pokud si organizace, která se autocertifikuje, přeje zahrnout některý ze svých subjektů v USA nebo dceřiných společností v USA, které mají své vlastní příslušné politiky ochrany soukromí, ministerstvo rovněž přezkoumá příslušné politiky ochrany soukromí těchto zahrnutých subjektů nebo dceřiných společností, aby zajistilo, že obsahují všechny požadované prvky stanovené v zásadě oznamovací povinnosti.
- Ministerstvo bude spolupracovat se subjekty zřízenými zákonem (např. Federální obchodní komisí a Ministerstvem dopravy) s cílem ověřit, zda organizace podléhají pravomoci příslušného subjektu zřízeného zákonem určeného v jejich podáních k autocertifikaci, pokud má ministerstvo důvod pochybovat o tom, že této pravomoci podléhají.
- Ministerstvo bude spolupracovat se subjekty pro alternativní řešení sporů ze soukromého sektoru s cílem ověřit, zda jsou organizace aktivně registrovány u nezávislého odvolacího mechanismu uvedeného v jejich podáních k autocertifikaci; a spolupracovat s těmito subjekty s cílem ověřit, zda jsou organizace aktivně registrovány k externímu přezkumu souladu uvedenému v jejich podáních k autocertifikaci, mohou-li tyto subjekty nabízet oba druhy služeb.
- Ministerstvo bude spolupracovat s třetí stranou, kterou ministerstvo vybere, aby sloužila jako správce finančních prostředků vybraných prostřednictvím poplatku za panel úřadů pro ochranu osobních údajů (tj. ročního poplatku určeného k pokrytí provozních nákladů panelu úřadů pro ochranu osobních údajů), s cílem ověřit, že organizace tento poplatek za příslušný rok zaplatily, pokud organizace určily úřady pro ochranu osobních údajů jako příslušný nezávislý odvolací mechanismus.
- Ministerstvo bude spolupracovat s třetí stranou vybranou ministerstvem pro vedení rozhodčích řízení podle přílohy I zásad a pro správu rozhodčího fondu uvedeného ve zmíněné příloze s cílem ověřit, že organizace do tohoto fondu přispěly.
- Zjistí-li ministerstvo během přezkumu podání k autocertifikaci organizací jakékoli problémy, informuje je o tom, že musí všechny tyto problémy v přiměřené lhůtě stanovené ministerstvem vyřešit <sup>(\*)</sup>. Ministerstvo je rovněž informuje o tom, že nereagování ve lhůtách stanovených ministerstvem nebo jiné nedokončení autocertifikace v souladu s postupy ministerstva povede k tomu, že se bude mít za to, že od těchto podání týkajících se autocertifikace bylo upuštěno, a že jakékoli nepravdivé tvrzení o účasti organizace v rámci EU–USA pro ochranu údajů nebo o souladu s ním může být předmětem donucovacího opatření ze strany Federální obchodní komise, Ministerstva dopravy nebo jiného příslušného orgánu státní správy. Ministerstvo organizace informuje pomocí kontaktních prostředků, které organizace ministerstvu poskytly.

Usnadnění spolupráce se subjekty pro alternativní řešení sporů, které poskytují služby související se zásadami

- Ministerstvo bude spolupracovat se subjekty pro alternativní řešení sporů ze soukromého sektoru, které poskytují nezávislé odvolací mechanismy, jež jsou k dispozici k prošetřování nevyřešených stížností podaných podle zásad, s cílem ověřit, zda splňují alespoň požadavky stanovené v doplňkové zásadě o řešení sporů a prosazování. Ministerstvo ověří, zda tyto subjekty:
  - uvádí na svých veřejných internetových stránkách informace o zásadách a službách, které na základě rámce EU–USA pro ochranu údajů poskytují, jež musí obsahovat: 1) informace o požadavcích zásad na nezávislé odvolací mechanismy nebo hypertextový odkaz na ně; 2) hypertextový odkaz na internetové stránky ministerstva věnované rámci pro ochranu údajů; 3) vysvětlení, že jejich služby v oblasti řešení sporů na základě rámce EU–USA pro ochranu údajů jsou pro fyzické osoby bezplatné; 4) popis způsobu podání stížnosti v souvislosti se zásadami; 5) lhůtu na vyřízení stížností v souvislosti se zásadami a 6) popis nabídky potenciálních opravných prostředků. Ministerstvo subjektům včas oznámí podstatné změny v dohledu ministerstva nad programem rámce pro ochranu údajů a v jeho správě, pokud tyto změny bezprostředně nastanou nebo již byly provedeny a pokud jsou tyto změny relevantní pro úlohu, kterou tyto subjekty hrají v rámci EU–USA pro ochranu údajů,

<sup>(\*)</sup> Např. pokud jde o opětovnou certifikaci, očekává se, že organizace všechny tyto otázky vyřeší do 45 dnů, ledaže by ministerstvo uvedlo jinou přiměřenou lhůtu.

- zveřejňují výroční zprávu obsahující souhrnné statistiky týkající se jejich služeb pro řešení sporů, která musí obsahovat: 1) celkový počet stížností souvisejících se zásadami obdržených během sledovaného roku; 2) typy obdržených stížností; 3) měřítko kvality řešení sporů, jako je doba, za jakou jsou stížnosti vyřízeny, a 4) výsledky obdržených stížností, zejména počet a druh uložených opravných prostředků nebo sankcí. Ministerstvo poskytne subjektům konkrétní doplňující pokyny ohledně toho, jaké informace by měly poskytovat v těchto výročních zprávách, v nichž se budou zabývat těmito požadavky (např. seznam konkrétních kritérií, která musí stížnost splňovat, aby mohla být pro účely výroční zprávy považována za stížnost týkající se zásad), jakož i určení dalších druhů informací, které by měly poskytnout (např. pokud subjekt rovněž poskytuje ověřovací službu související se zásadami, popis toho, jak se subjekt vyhýbá jakémukoli skutečnému nebo potenciálnímu střetu zájmů v situacích, kdy poskytuje organizaci ověřovací služby i služby pro řešení sporů). Dodatečné pokyny poskytnuté ministerstvem rovněž stanoví datum, do kterého by měly být výroční zprávy subjektů za příslušné vykazované období zveřejňovány.

Sledování organizací, které si přejí být nebo byly odstraněny ze seznamu organizací rámce pro ochranu údajů

- Pokud si organizace přeje vystoupit z rámce EU–USA pro ochranu údajů, bude ministerstvo požadovat, aby organizace odstranila ze všech příslušných politik ochrany soukromí veškeré odkazy na rámec EU–USA pro ochranu údajů, které naznačují, že se nadále rámce EU–USA pro ochranu údajů účastní a že může přijímat osobní údaje na základě rámce EU–USA pro ochranu údajů (viz popis závazku ministerstva vyhledávat nepravdivá tvrzení o účasti). Ministerstvo bude rovněž požadovat, aby organizace vyplnila a předložila ministerstvu příslušný dotazník k ověření:
  - jejího přání z rámce vystoupit,
  - kterou z následujících možností uplatní na osobní údaje, které obdržela na základě rámce EU–USA pro ochranu údajů během své účasti v tomto rámci: a) uchovávat tyto údaje, nadále na tyto údaje uplatňovat zásady a každoročně potvrzovat ministerstvu svůj závazek zásady na tyto údaje uplatňovat; b) uchovávat tyto údaje a poskytovat jim „odpovídající“ ochranu jinými povolenými prostředky, nebo c) všechny tyto údaje do určitého data vrátit nebo vymazat, a
  - kdo bude v rámci organizace sloužit jako stálé kontaktní místo pro otázky týkající se zásad.
- Pokud si organizace zvolila písmeno a), jak je popsáno výše, bude ministerstvo také požadovat, aby každý rok po svém vystoupení vyplnila a ministerstvu předložila (tj. k prvnímu výročí vystoupení, jakož i ke každému následujícímu výročí, pokud organizace nezajistí „odpovídající“ ochranu těchto údajů jiným povoleným způsobem nebo pokud všechny tyto údaje nevrátí či nevymaže a neoznámí tuto skutečnost ministerstvu) příslušný dotazník za účelem ověření, jak s těmito osobními údaji organizace naložila, jak naloží s osobními údaji, které nadále uchovává, a kdo bude v organizaci sloužit jako trvalé kontaktní místo pro dotazy týkající se zásad.
- Pokud organizace nechala svou autocertifikaci propadnout (tj. ani nedokončila každoroční opětovnou certifikaci dodržování zásad, ani nebyla ze seznamu organizací rámce pro ochranu údajů odstraněna z jiného důvodu, než je vystoupení), ministerstvo jí nařídí, aby vyplnila a ministerstvu předložila příslušný dotazník za účelem ověření, zda si přeje z rámce vystoupit, nebo se opětovně certifikovat:
  - a pokud si přeje vystoupit, rovněž za účelem ověření, jak naloží s osobními údaji, které obdržela na základě rámce EU–USA pro ochranu údajů během své účasti v tomto rámci (viz předchozí popis toho, co musí organizace ověřit, pokud chce z rámce vystoupit),
  - a pokud si přeje se opětovně certifikovat, rovněž za účelem ověření, že během doby, kdy měla být certifikovaná, uplatňovala zásady na osobní údaje získané na základě rámce EU–USA pro ochranu údajů, a k objasnění, jaké kroky podnikne k vyřešení nevyřešených problémů, které zdržely její opětovnou certifikaci.

- Je-li organizace ze seznamu organizací rámce pro ochranu údajů odstraněna z některého z těchto důvodů: a) vystoupení z rámce EU–USA pro ochranu údajů; b) nedokončení každoroční opětovné certifikace jejího dodržování zásad (tj. buď byla zahájena, ale organizace nedokončila proces každoroční opětovné certifikace včas, nebo proces každoroční opětovné certifikace ani nezahájila), nebo c) pro „soustavné nedodržování zásad“, zašle ministerstvo oznámení kontaktním osobám uvedeným v podání organizace k autocertifikaci, v němž uvede důvod odstranění a vysvětlí, že musí přestat výslovně nebo implicitně prohlašovat, že se účastní rámce EU–USA pro ochranu údajů nebo že jej dodržuje a že může přijímat osobní údaje na základě rámce EU–USA pro ochranu údajů. V oznámení, které může obsahovat i další obsah přizpůsobený důvodu odstranění, bude uvedeno, že organizace, které uvedou nepravdivé údaje o své účasti v rámci EU–USA pro ochranu údajů nebo o dodržování tohoto rámce, včetně případů, kdy uvedou, že se rámce EU–USA pro ochranu údajů účastní poté, co byly ze seznamu odstraněny, mohou podléhat donucovacím opatřením ze strany Federální obchodní komise, Ministerstva dopravy nebo jiného příslušného orgánu státní správy.

#### Vyhledávání a řešení nepravdivých tvrzení o účasti

- Pokud organizace: a) vystoupí z rámce EU–USA pro ochranu údajů, b) neprovede každoroční opětovnou certifikaci dodržování zásad (tj. buď ji zahájila, ale nedokončila roční proces opětovné certifikace včas, nebo proces roční opětovné certifikace vůbec nezahájila), c) je vyřazena z účasti v rámci EU–USA pro ochranu údajů zejména z důvodu „soustavného nedodržování zásad“, nebo d) nedokončí počáteční autocertifikaci svého dodržování zásad (tj. zahájila ji, ale nedokončila proces počáteční autocertifikace včas), ministerstvo průběžně z moci úřední provede opatření k ověření, že žádná příslušná zveřejněná politika ochrany soukromí organizace neobsahuje odkazy na rámec EU–USA pro ochranu údajů, z nichž vyplývá, že se organizace rámce EU–USA pro ochranu údajů účastní a že může přijímat osobní údaje na základě rámce EU–USA pro ochranu údajů. Pokud ministerstvo takové odkazy objeví, informuje organizaci o tom, že případně postoupí záležitost příslušné agentuře k případnému přijetí donucovacího opatření, pokud bude organizace o své účasti v rámci EU–USA pro ochranu údajů i nadále nepravdivě informovat. Ministerstvo organizaci informuje pomocí kontaktních prostředků, které mu organizace poskytla, nebo případně jinými vhodnými prostředky. Pokud organizace odkazy neodstraní, ani neautocertifikuje své dodržování rámce EU–USA pro ochranu údajů v souladu s postupy ministerstva, postoupí ministerstvo záležitost z moci úřední Federální obchodní komisi, Ministerstvu dopravy nebo jinému příslušnému donucovacímu orgánu nebo přijme jiná vhodná opatření k zajištění řádného používání certifikační značky rámce EU–USA pro ochranu údajů,
- ministerstvo vynaloží další úsilí k odhalení nepravdivých tvrzení o účasti v rámci EU–USA pro ochranu údajů a nesprávného používání certifikační značky rámce EU–USA pro ochranu údajů, a to i ze strany organizací, které na rozdíl od výše popsaných organizací proces autocertifikace nikdy ani nezahájily (např. provede příslušné vyhledávání na internetu s cílem zjistit odkazy na rámec EU–USA pro ochranu údajů v politikách ochrany soukromí organizací). Pokud ministerstvo v rámci tohoto úsilí zjistí nepravdivá tvrzení o účasti v rámci EU–USA pro ochranu údajů a nesprávné používání certifikační značky rámce EU–USA pro ochranu údajů, informuje organizaci o tom, že pokud bude organizace pokračovat v nepravdivých tvrzeních o své účasti v rámci EU–USA pro ochranu údajů, postoupí případně záležitost příslušné agentuře za účelem výkonu donucovacího opatření. Ministerstvo organizaci informuje pomocí kontaktních prostředků, které mu případně organizace poskytla, nebo popřípadě jinými vhodnými prostředky. Pokud organizace odkazy neodstraní, ani neautocertifikuje své dodržování rámce EU–USA pro ochranu údajů v souladu s postupy ministerstva, postoupí ministerstvo záležitost z moci úřední Federální obchodní komisi, Ministerstvu dopravy nebo jinému příslušnému donucovacímu orgánu nebo přijme jiná vhodná opatření k zajištění řádného používání certifikační značky rámce EU–USA pro ochranu údajů,
- ministerstvo neprodleně přezkoumá a vyřeší konkrétní nikoli bezdůvodné stížnosti týkající se nepravdivých tvrzení o účasti v rámci EU–USA pro ochranu údajů, které ministerstvo obdrží (např. stížnosti přijaté od úřadů pro ochranu osobních údajů, nezávislých odvolacích mechanismů poskytovaných subjekty pro alternativní řešení sporů ze soukromého sektoru, subjektů údajů, podniků z EU a USA a jiných druhů třetích stran), a
- ministerstvo může přijmout jiná vhodná nápravná opatření. Nepravdivá prohlášení učiněná vůči ministerstvu mohou být předmětem žaloby podle zákona o nepravdivých tvrzeních (False Statements Act) (18 U.S.C. § 1001).

## Provádění pravidelných úředních přezkumů dodržování zásad a hodnocení programu rámce pro ochranu údajů

- Ministerstvo bude průběžně sledovat účinné dodržování rámce EU–USA pro ochranu údajů organizacemi, které se ho účastní, s cílem zjistit problémy, které mohou vyžadovat následná opatření. Ministerstvo bude zejména z moci úřední provádět běžné kontroly na místě náhodně vybraných organizací rámce EU–USA pro ochranu údajů, jakož i *ad hoc* kontroly na místě konkrétních organizací rámce EU–USA pro ochranu údajů, pokud budou zjištěny potenciální nedostatky v dodržování zásad (např. potenciální nedostatky v dodržování zásad, na které ministerstvo upozorní třetí strany), s cílem ověřit: a) že jsou k dispozici kontaktní místa odpovědná za vyřizování stížností, žádostí o přístup a dalších otázek vyplývajících z rámce EU–USA pro ochranu údajů; b) že politika ochrany soukromí organizace určená veřejnosti je v příslušných případech snadno dostupná pro veřejnost jak na veřejných internetových stránkách organizace, tak prostřednictvím hypertextového odkazu na seznam organizací rámce pro ochranu údajů; c) že politika ochrany soukromí organizace je i nadále v souladu s požadavky na autocertifikaci popsanými v zásadách a d) že nezávislý odvolací mechanismus určený organizací je k dispozici pro řešení stížností podaných podle rámce EU–USA pro ochranu údajů. Ministerstvo bude rovněž aktivně sledovat zpravodajství s cílem objevit zprávy, které poskytují věrohodné důkazy o nedodržování zásad ze strany organizací rámce EU–USA pro ochranu údajů,
- v rámci kontroly dodržování zásad bude ministerstvo vyžadovat, aby organizace rámce EU–USA pro ochranu údajů vyplnila a ministerstvu předložila podrobný dotazník, pokud: a) ministerstvo obdrželo konkrétní nikoli bezdůvodné stížnosti na dodržování zásad organizací; b) organizace uspokojivě nezareaguje na žádosti ministerstva o informace týkající se rámce EU–USA pro ochranu údajů, nebo c) existují věrohodné důkazy o tom, že organizace nedodržuje své závazky vyplývající z rámce EU–USA pro ochranu údajů. Pokud ministerstvo zaslalo organizaci takový podrobný dotazník a organizace na dotazník uspokojivě neodpověděla, ministerstvo organizaci informuje, že pokud od organizace neobdrží včasnou a uspokojivou odpověď, postoupí věc příslušnému orgánu k výkonu případného donucovacího opatření. Ministerstvo organizaci informuje pomocí kontaktních prostředků, které mu organizace poskytla, nebo případně jinými vhodnými prostředky. Pokud organizace neposkytne včasnou a uspokojivou odpověď, postoupí ministerstvo záležitost z moci úřední Federální obchodní komisi, Ministerstvu dopravy nebo jinému příslušnému donucovacímu orgánu nebo přijme jiná vhodná opatření k zajištění dodržování zásad. Ministerstvo bude tyto přezkumy dodržování zásad popřípadě konzultovat s příslušnými úřady pro ochranu osobních údajů a
- ministerstvo bude pravidelně hodnotit správu programu rámce pro ochranu údajů a dohled nad ním s cílem zajistit, aby sledování, které provádí, včetně úsilí vynaloženého prostřednictvím vyhledávacích nástrojů (např. kontrola nefunkčních odkazů na politiky ochrany soukromí organizací rámce EU–USA pro ochranu údajů), dokázalo řešit stávající problémy, jakož i případné nové problémy, když nastanou.

## Uzpůsobení internetových stránek rámce pro ochranu údajů cílovým adresátům

Ministerstvo uzpůsobí internetové stránky rámce pro ochranu údajů tak, aby se zaměřovaly na tyto cílové adresáty: fyzické osoby z EU, podniky z EU, podniky z USA a úřady pro ochranu osobních údajů. Zařazení materiálu přímo zaměřeného na fyzické osoby a podniky z EU v mnoha ohledech pomůže zvýšit transparentnost. Pokud jde o fyzické osoby z EU, internetové stránky zřetelně vysvětlí: 1) práva, která rámec EU–USA pro ochranu údajů poskytuje fyzickým osobám z EU; 2) odvolací mechanismy dostupné fyzickým osobám z EU, jsou-li přesvědčeny, že organizace porušila svůj závazek dodržovat zásady, a 3) jak nalézt informace, jež se týkají autocertifikace organizace rámce EU–USA pro ochranu údajů. Pokud jde o podniky z EU, internetové stránky usnadní ověřování: 1) toho, zda se organizace účastní rámce EU–USA pro ochranu údajů; 2) typu informací, na které se vztahuje autocertifikace organizace rámce EU–USA pro ochranu údajů; 3) politiky ochrany soukromí, jež pro dotčené informace platí, a 4) metody, kterou organizace používá k ověřování toho, že dodržuje zásady. Pokud jde o podniky z USA, internetové stránky zřetelně vysvětlí: 1) výhody účasti v rámci EU–USA pro ochranu údajů; 2) jak se rámce EU–USA pro ochranu údajů účastnit, jak se opětovně certifikovat a jak z rámce EU–USA pro ochranu údajů vystoupit a 3) jak Spojené státy rámec EU–USA pro ochranu údajů spravují a prosazují. Zahrnutí materiálu přímo zaměřeného na úřady pro ochranu osobních údajů (např. informace o specializovaném kontaktním místě ministerstva pro úřady pro ochranu osobních údajů a hypertextový odkaz na obsah související se zásadami na internetových stránkách Federální obchodní komise) usnadní spolupráci i zvýší transparentnost. Ministerstvo bude rovněž v režimu *ad hoc* spolupracovat s Komisí a Evropským sborem pro ochranu osobních údajů na vypracovávání dalších aktuálních materiálů (např. odpovědi na často kladené otázky), které lze použít na internetových stránkách rámce pro ochranu údajů, kde by tyto informace usnadnily účinnou správu programu rámce pro ochranu údajů a dohled nad ním.

## Usnadnění spolupráce s úřady pro ochranu osobních údajů

S cílem rozšířit příležitosti ke spolupráci s úřady pro ochranu osobních údajů bude ministerstvo zajišťovat specializované kontaktní místo, které bude v rámci ministerstva fungovat jako styčný bod pro komunikaci s úřady pro ochranu osobních údajů. Bude-li kterýkoli úřad pro ochranu osobních údajů přesvědčen, že nějaká organizace rámce EU–USA pro ochranu údajů nedodržuje zásady, a to i na základě stížnosti fyzické osoby z EU, může se tento úřad pro ochranu osobních údajů obrátit na specializované kontaktní místo na ministerstvu a požádat o postoupení organizace k dalšímu přezkumu. Ministerstvo vynaloží veškeré úsilí, aby usnadnilo řešení stížnosti s organizací rámce EU–USA pro ochranu údajů. Ministerstvo poskytne úřadu pro ochranu osobních údajů do 90 dnů od obdržení stížnosti aktuální informace. Specializované kontaktní místo bude také přijímat případy organizací, které nepravdivě tvrdí, že se účastní rámce EU–USA pro ochranu údajů. Specializované kontaktní místo bude sledovat všechny případy postoupené úřady pro ochranu osobních údajů ministerstvu a ministerstvo v rámci společného přezkumu popsaného níže poskytne zprávu, která souhrnně analyzuje stížnosti, jež každý rok obdrží. Toto specializované kontaktní místo bude pomáhat úřadům pro ochranu osobních údajů, které potřebují informace o autocertifikaci nebo předchozí účasti určité organizace v rámci EU–USA pro ochranu údajů, a bude odpovídat na dotazy úřadů pro ochranu osobních údajů ohledně provádění zvláštních požadavků rámce EU–USA pro ochranu údajů. Ministerstvo bude rovněž spolupracovat s Komisí a Evropským sborem pro ochranu osobních údajů na procedurálních a správních aspektech panelu úřadů pro ochranu osobních údajů, a to i na stanovení vhodných postupů pro rozdělování finančních prostředků vybraných prostřednictvím poplatku panelu úřadů pro ochranu osobních údajů. Chápeme, že Komise bude s ministerstvem spolupracovat na usnadnění řešení veškerých problémů, které mohou v souvislosti s uvedenými postupy vyvstat. Ministerstvo navíc poskytne úřadům pro ochranu osobních údajů materiál o rámci EU–USA pro ochranu údajů, který budou moci zveřejnit na svých vlastních internetových stránkách za účelem zvýšení transparentnosti vůči fyzickým osobám a podnikům z EU. Větší povědomí o rámci EU–USA pro ochranu údajů a právech a povinnostech, které na jeho základě vznikají, by mělo usnadnit odhalování problémů, jakmile vyvstanou, aby je bylo možné vhodně řešit.

## Plnění závazků podle přílohy I zásad

Ministerstvo bude plnit své závazky podle přílohy I zásad, mimo jiné povede seznam rozhodců vybraných spolu s Komisí na základě nezávislosti, bezúhonnosti a odborných znalostí a případně bude podporovat třetí stranu, kterou ministerstvo vybralo za účelem vedení rozhodčích řízení podle přílohy I zásad a správy rozhodčího fondu uvedeného ve zmíněné příloze<sup>(3)</sup>. Ministerstvo bude spolupracovat s třetí stranou mimo jiné s cílem ověřit, zda třetí strana provozuje internetové stránky obsahující pokyny ohledně rozhodčího řízení, včetně: 1) toho, jak zahájit řízení a předkládat dokumenty; 2) seznamu rozhodců vedeného ministerstvem a způsobu výběru rozhodců z tohoto seznamu; 3) postupů, jimiž se řídí rozhodčí řízení, a kodexu chování rozhodců přijatých ministerstvem a Komisí<sup>(4)</sup> a 4) způsobu výběru u a úhrady odměn rozhodců. Ministerstvo bude kromě toho spolupracovat s třetí stranou na pravidelném přezkumu fungování rozhodčího fondu, včetně potřeby upravit výši příspěvků nebo stropů (tj. maximálních částek) nákladů na rozhodčí řízení, a zváží mimo jiné počet rozhodčích řízení a náklady a načasování rozhodčích řízení, přičemž se rozumí, že na organizace rámce EU–USA pro ochranu údajů nebude kladena přílišná finanční zátěž. Ministerstvo oznámí Komisi výsledek těchto přezkumů provedených spolu s třetí stranou a předem jí oznámí veškeré úpravy výše příspěvků.

## Provádění společných přezkumů fungování rámce EU–USA pro ochranu údajů

Ministerstvo a popřípadě další agentury budou pravidelně pořádat zasedání s Komisí, zúčastněnými úřady pro ochranu osobních údajů a příslušnými zástupci Evropského sboru pro ochranu osobních údajů, na kterých ministerstvo poskytne aktuální informace o rámci EU–USA pro ochranu údajů. Součástí zasedání bude diskuse o aktuálních problémech spojených s fungováním programu rámce pro ochranu údajů, jeho prováděním, dohledem nad ním a jeho prosazováním. Zasedání mohou případně zahrnovat diskusi o souvisejících tématech, jako jsou jiné mechanismy předávání údajů, na něž se vztahují záruky podle rámce EU–USA pro ochranu údajů.

<sup>(3)</sup> Ministerstvo vybralo Mezinárodní středisko pro řešení sporů (International Centre for Dispute Resolution, dále také jako „středisko ICDR“), mezinárodní divizi Americké arbitrážní asociace (American Arbitration Association, dále také jako „asociace AAA“) (společně také jako „středisko ICDR-AAA“), aby vedlo rozhodčí řízení podle přílohy I zásad a spravovalo rozhodčí fond uvedený ve zmíněné příloze.

<sup>(4)</sup> 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 na úpravě pravidel rozhodčího řízení a kodexu chování tak, aby odrážely aktualizace na základě rámce EU–USA pro ochranu údajů, a ministerstvo bude na těchto aktualizacích spolupracovat se střediskem ICDR-AAA.

## Aktualizace právních předpisů

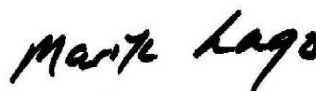
Ministerstvo vynaloží přiměřené úsilí k tomu, aby Komisi informovalo o významných změnách práva ve Spojených státech, budou-li souviset s rámcem EU–USA pro ochranu údajů v oblasti ochrany osobních údajů a omezení a záruk platných pro přístup k osobním údajům ze strany orgánů USA a jejich následné využívání.

## Přístup vlády USA k osobním údajům

Spojené státy vydaly výkonný dekret č. 14086 „Posílení záruk pro činnosti USA v oblasti signálového zpravodajství“ a 28 CFR část 201, kterou se mění předpisy Ministerstva spravedlnosti za účelem zřízení Soudu pro přezkum ochrany údajů, které poskytují silnou ochranu osobních údajů, pokud jde o přístup orgánů státní správy k údajům pro účely národní bezpečnosti. Poskytnutá ochrana zahrnuje: posílení záruk ochrany soukromí a občanských svobod s cílem zajistit, aby činnosti USA v oblasti signálového zpravodajství byly nezbytné a přiměřené při sledování stanovených cílů národní bezpečnosti; vytvoření nového nápravného mechanismu s nezávislým orgánem, jehož rozhodnutí jsou závazná, a posílení stávajícího přísného a víceúrovňového dohledu nad činnostmi USA v oblasti signálového zpravodajství. Prostřednictvím těchto ochranných opatření mohou fyzické osoby z EU usilovat o nápravu prostřednictvím nového víceúrovňového nápravného mechanismu, jehož součástí by byl nezávislý Soud pro přezkum ochrany údajů, který by se skládal z osob vybraných mimo vládu USA, které by měly plnou pravomoc rozhodovat o nárocích a podle potřeby přímo přijímat nápravná opatření. Ministerstvo povede záznamy o fyzických osobách z EU, které podaly kvalifikovanou stížnost na základě výkonného dekretu č. 14086 a 28 CFR části 201. Pět let od data tohoto dopisu a poté každých pět let kontaktuje ministerstvo příslušné agentury ohledně toho, zda byly informace týkající se přezkumu kvalifikovaných stížností nebo přezkumu žádostí o přezkum předložených Soudu pro přezkum ochrany údajů odtajněny. Pokud byly tyto informace odtajněny, bude ministerstvo spolupracovat s příslušným úřadem pro ochranu osobních údajů s cílem fyzickou osobu z EU informovat. Tato zlepšení potvrzují, že s osobními údaji EU předávanými do Spojených států bude nakládáno způsobem, který je v souladu s právními požadavky EU, pokud jde o přístup orgánů státní správy k údajům.

Na základě zásad, výkonného dekretu č. 14086, 28 CFR části 201 a doprovodných dopisů a materiálů, včetně závazků ministerstva týkajících se správy a dohledu nad programem rámce pro ochranu údajů, předpokládáme, že Komise rozhodne, že rámec EU–USA pro ochranu údajů poskytuje odpovídající ochranu pro účely práva EU a že předávání údajů z Evropské unie organizacím, které se účastní rámce EU–USA pro ochranu údajů, bude pokračovat. Očekáváme rovněž, že předávání údajů organizacím v USA prováděné na základě standardních smluvních doložek EU nebo závazných podnikových pravidel EU bude podmínkami uvedených ujednání dále usnadněno.

S úctou



Marisa LAGO



## PŘÍLOHA IV

SPOJENÉ STÁTY AMERICKÉ  
Federální obchodní komise  
WASHINGTON, D.C. 20580

Kancelář předsedkyně

9. června 2023

Didier Reynders  
Komisař pro spravedlnost  
Evropská komise  
Rue de la Loi/Wetstraat 200  
1049 Bruxelles/Brussel  
Belgique/België

Vážený pane komisaři Reyndersi,

Federální obchodní komise Spojených států (dále též „FTC“) si váží příležitosti popsat, jak prosazuje zásady rámce EU–USA pro ochranu údajů. Federální obchodní komise se přeshraniční ochraně spotřebitelů a soukromí věnuje již dlouho a jsme odhodláni prosazovat aspekty tohoto rámce týkající se obchodního sektoru. Federální obchodní komise plní tuto úlohu od roku 2000 v souvislosti s rámcem „bezpečného přístavu“ mezi USA a EU a naposledy od roku 2016 v souvislosti s rámcem štítu EU–USA na ochranu soukromí<sup>(1)</sup>. Dne 16. července 2020 Soudní dvůr Evropské unie (dále jen „SDEU“) zrušil rozhodnutí Evropské komise o odpovídající ochraně poskytované rámcem štítu EU–USA na ochranu soukromí, a to na základě jiných otázek, než jsou obchodní zásady, které Federální obchodní komise prosazovala. USA a Evropská komise od té doby jednaly o rámci EU–USA pro ochranu údajů s cílem řešit toto rozhodnutí Soudního dvora EU.

Obracím se na Vás, abych potvrdila závazek Federální obchodní komise k důslednému prosazování zásad rámce EU–USA pro ochranu údajů. Zejména potvrzujeme svůj závazek ve třech klíčových oblastech: 1) upřednostňování a vyšetřování věcí předložených k přezkoumání; 2) usilování o vydávání příkazů a sledování jejich dodržování a 3) spolupráce v oblasti prosazování práva s úřady EU pro ochranu osobních údajů.

## I. Úvod

### a. Činnost Federální obchodní komise v souvislosti s prosazováním a politikou v oblasti ochrany soukromí

Federální obchodní komise má širokou pravomoc prosazovat občanské právo s cílem podporovat ochranu spotřebitele a hospodářskou soutěž v oblasti obchodu. V rámci svého mandátu chránit spotřebitele prosazuje Federální obchodní komise širokou paletu právních předpisů o ochraně soukromí a bezpečnosti spotřebitelů a jejich údajů. Hlavní zákon

<sup>(1)</sup> Dopis předsedkyně Edithy Ramirezové komisařce pro spravedlnost, spotřebitele a rovnost žen a mužů Evropské komise, Věře Jourové, který popisuje prosazování nového rámce štítu EU–USA na ochranu soukromí Federální obchodní komisí (29. února 2016), k dispozici na adrese <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european>. Federální obchodní komise se rovněž dříve zavázala prosazovat program „bezpečného přístavu“ USA–EU. Dopis, který zaslal Robert Pitofsky, předseda Federální obchodní komise, Johnu Moggovi, řediteli GR pro vnitřní trh Evropská 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 uvedené dřívější závazky.

prosazovaný Federální obchodní komisí, zákon o Federální obchodní komisi, zakazuje „nekalé“ nebo „klamavé“ praktiky při obchodování nebo nekalé a klamavé praktiky, které na obchodování dopadají <sup>(2)</sup>. Federální obchodní komise také prosazuje cílené předpisy, které chrání informace o zdraví a úvěrech a jiných finančních záležitostech a informace o dětech na internetu, a vydala nařízení, jimiž se každý z těchto předpisů provádí <sup>(3)</sup>.

Federální obchodní komise rovněž nedávno zahájila řadu iniciativ na posílení naší činnosti v oblasti ochrany soukromí. V srpnu 2022 Federální obchodní komise oznámila, že zvažuje pravidla, která by zakročila proti škodlivému obchodnímu sledování a laxnímu zabezpečení údajů <sup>(4)</sup>. Cílem projektu je vytvořit spolehlivé veřejné záznamy, které by sloužily jako podklady pro to, zda by Federální obchodní komise měla vydávat pravidla pro řešení postupů v oblasti obchodního dohledu a zabezpečení údajů a jak by tato pravidla měla případně vypadat. Uvítali jsme připomínky zúčastněných stran EU k této i dalším iniciativám.

Na našich konferencích „PrivacyCon“ se i nadále setkávají přední výzkumní pracovníci, aby diskutovali o nejnovějším výzkumu a trendech týkajících se soukromí spotřebitelů a zabezpečení údajů. Rovněž jsme zlepšili schopnost naší agentury držet krok s technologickým vývojem, který je ústředním tématem mnohé naší práce v oblasti ochrany soukromí, a vytvořili jsme rozrůstající se tým technologů a interdisciplinárních výzkumných pracovníků. Jak víte, rovněž jsme oznámili zahájení společného dialogu s Vámi a Vašimi kolegy v Evropské komisi, který zahrnuje řešení takových témat souvisejících s ochranou soukromí, jako jsou temné vzorce a obchodní modely charakterizované všudypřítomným shromažďováním údajů <sup>(5)</sup>. Nedávno jsme rovněž vydali zprávu pro Kongres upozorňující na škody spojené s používáním umělé inteligence k řešení škod na internetu zjištěných Kongresem. Tato zpráva vyjádřila obavy ohledně nepřesnosti, předpojatosti, diskriminace a obchodního sledování <sup>(6)</sup>.

## b. Právní ochrana poskytovaná USA spotřebitelům z EU

Rámec EU–USA pro ochranu údajů funguje v širším prostředí ochrany soukromí zajišťované USA, které řadou způsobů chrání i spotřebitele z EU. Zákaz nekalého nebo klamavého jednání či praktik uvedený v zákoně o Federální obchodní komisi se neomezuje na ochranu spotřebitelů v USA před společnostmi z USA, jelikož se vztahuje na praktiky, které 1) způsobují přiměřeně předvídatelné škody ve Spojených státech nebo je pravděpodobné, že je způsobí, či 2) zahrnují závažné jednání ve Spojených státech. Dále může Federální obchodní komise využít při ochraně zahraničních spotřebitelů všechny opravné prostředky, které má k dispozici na ochranu domácích spotřebitelů <sup>(7)</sup>.

Federální obchodní komise také prosazuje jiné cílené zákony, jejichž ochrana se vztahuje i na spotřebitele mimo Spojené státy, například zákon o ochraně soukromí dětí na internetu (Children's Online Privacy Protection Act, dále také jako „zákon COPPA“). Zákon COPPA mj. vyžaduje, aby provozovatelé internetových stránek a on-line služeb zaměřených na děti nebo stránek pro širokou veřejnost, které vědomě sbírají osobní informace od dětí mladších třinácti let, uvědomili rodiče a získali jejich ověřitelný souhlas. Zákon COPPA musí dodržovat internetové stránky a služby provozované

<sup>(2)</sup> 15 U.S.C. § 45(a). Federální obchodní komise nemá pravomoc prosazovat trestní právo ani se zabývat záležitostmi národní bezpečnosti. Federální obchodní komise nemůže dosáhnout ani na většinu jiných vládních opatření. Kromě toho existují výjimky z pravomoci Federální obchodní komise nad obchodními aktivitami, a to mj. v souvislosti s bankami, leteckými dopravci, pojišťovnictvím a běžnými přenosovými činnostmi poskytovatelů telekomunikačních služeb. Federální obchodní komise také nemá pravomoc nad většinou neziskových organizací, ale má pravomoc nad fiktivními dobročinnými organizacemi nebo jinými neziskovými organizacemi, jejichž cílem je ve skutečnosti zisk. Federální obchodní komise má také pravomoc nad neziskovými organizacemi, jejichž cílem je zisk jejich ziskových členů, a proto jim mj. poskytují podstatné hospodářské výhody. V některých případech se příslušnost Federální obchodní komise překrývá s příslušností jiných donucovacích orgánů. Navázali jsme pevné vztahy s federálními a státními orgány a úzce s nimi spolupracujeme na koordinaci vyšetřování, popřípadě na předkládání záležitostí k přezkoumání.

<sup>(3)</sup> Viz Federální obchodní komise, Ochrana soukromí a bezpečnost, <https://www.ftc.gov/business-guidance/privacy-security>

<sup>(4)</sup> Viz tisková zpráva, Federální obchodní komise, FTC zkoumá pravidla pro zakročení proti postupům v oblasti obchodního sledování a laxního zabezpečení údajů (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>

<sup>(5)</sup> Viz společné tiskové prohlášení Didiera Reynderse, komisaře Evropské komise pro spravedlnost, a Liny Khanové, předsedkyně Federální obchodní komise Spojených států (30. března 2022), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf)

<sup>(6)</sup> Viz tisková zpráva, Federální obchodní komise, Zpráva FTC varuje ohledně používání umělé inteligence při řešení problémů na internetu (16. června 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems>

<sup>(7)</sup> 15 U.S.C. § 45(a)(4)(B). „Nekalým nebo klamavým jednáním nebo praktikami“ se dále rozumí jednání nebo praktiky zahrnující zahraniční obchod, které i) způsobují přiměřeně předvídatelné škody ve Spojených státech nebo je pravděpodobné, že je způsobí, nebo ii) zahrnují závažné jednání, k němuž dochází ve Spojených státech. 15 U.S.C. § 45(a)(4)(A).

poskytovateli se sídlem ve Spojených státech, které podléhají uvedenému zákonu a sbírají osobní informace od nezletilých cizinců. Zákon COPPA musí dodržovat také internetové stránky a on-line služby provozované poskytovateli se sídlem v zahraničí, jestliže se zaměřují na děti ve Spojených státech nebo od nich vědomě sbírají osobní informace. Kromě federálních zákonů Spojených států prosazovaných Federální obchodní komisí mohou další výhody spotřebitelům z EU poskytovat i některé jiné federální a státní zákony týkající se ochrany spotřebitelů a soukromí a porušení zabezpečení údajů.

### c. Činnost Federální obchodní komise v oblasti prosazování

Federální obchodní komise zahájila řízení jak podle programu bezpečného přístavu mezi USA a EU, tak podle rámce štítu EU–USA na ochranu soukromí a v prosazování štítu EU–USA na ochranu soukromí pokračovala i poté, co Soudní dvůr EU zrušil rozhodnutí o odpovídající ochraně, které bylo základem rámce štítu EU–USA na ochranu soukromí<sup>(8)</sup>. Několik nedávných stížností podaných k Federální obchodní komisi obsahovalo obvinění, že firmy porušily ustanovení štítu EU–USA na ochranu soukromí, mj. v řízeních proti společnostem Twitter,<sup>(9)</sup> CafePress,<sup>(10)</sup> a Flo<sup>(11)</sup>. V rámci donucovacího opatření proti společnosti Twitter zajistila Federální obchodní komise od společnosti Twitter 150 milionů USD za porušení dřívějšího příkazu Federální obchodní komise s praktikami dotýkajícími se více než 140 milionů zákazníků, včetně porušení zásady č. 5 štítu EU–USA na ochranu soukromí (integrita údajů a účelové omezení). Příkaz agentury dále vyžaduje, aby společnost Twitter uživatelům umožnila používat bezpečné vícefaktorové metody autentizace, které nevyžadují, aby uživatelé uváděli svá telefonní čísla.

Ve věci *CafePress* Federální obchodní komise tvrdila, že společnost nezabezpečila citlivé informace spotřebitelů, kryla závažné porušení zabezpečení údajů a porušila zásady štítu EU–USA na ochranu soukromí č. 2 (možnost volby), č. 4 (zabezpečení) a č. 6 (právo na přístup). Nařízení Federální obchodní komise vyžaduje, aby společnost nahradila nedostatečná autentizační opatření vícefaktorovou autentizací, podstatně omezila množství údajů, které shromažďuje a uchovává, zašifrovala čísla sociálního zabezpečení a aby si od třetí strany nechala vypracovat posouzení svých programů zabezpečení informací a Federální obchodní komisi poskytla kopii, která může být zveřejněna.

Ve věci *Flo* Federální obchodní komise tvrdila, že aplikace pro sledování plodnosti zpřístupnila informace o zdraví uživatelů poskytovatelům analýzy údajů třetích stran poté, co se zavázala uchovávat tyto informace jako soukromé. Ve stížnosti Federální obchodní komise byla konkrétně zaznamenána interakce společnosti se spotřebiteli z EU a bylo v ní uvedeno, že společnost Flo porušila zásady štítu EU–USA na ochranu soukromí č. 1 (oznamovací povinnost), č. 2 (možnost volby), č. 3 (odpovědnost za další předávání) a č. 5 (integrita údajů a účelové omezení). Nařízení agentury mimo jiné vyžaduje, aby společnost Flo informovala dotčené uživatele o zveřejnění jejich osobních údajů a nařídila jakékoli třetí straně, která informace o zdraví uživatelů obdržela, aby tyto údaje zničila. Důležité je, že nařízení Federální obchodní komise chrání všechny spotřebitele na celém světě, kteří komunikují s podnikem z USA, a nikoli pouze ty spotřebitele, kteří podali stížnost.

Mnoho minulých případů prosazování práva v rámci systému „bezpečného přístavu“ mezi USA a EU a štítu EU–USA na ochranu soukromí se týkalo organizací, které dokončily počáteční autocertifikaci prostřednictvím Ministerstva obchodu, ale neprovedly svou každoroční autocertifikaci, přičemž prohlašovaly, že se i nadále účastní. Další případy se týkaly nepravdivých tvrzení o účasti organizací, které počáteční autocertifikaci prostřednictvím Ministerstva obchodu nikdy nedokončily. V budoucnu očekáváme, že naše proaktivní úsilí v oblasti prosazování práva bude zaměřeno na takové typy závažných porušení zásad rámce EU–USA pro ochranu údajů, jaké byly uvedeny například ve věcech *Twitter*, *CafePress* a *Flo*. Ministerstvo obchodu bude mezitím řídit proces autocertifikace a dohlížet na něj, bude vést úřední seznam účastníků rámce EU–USA pro ochranu údajů a bude se zabývat dalšími otázkami týkajícími se žádostí o účast v programu<sup>(12)</sup>. Důležité je, že společnosti, které tvrdí, že se účastní rámce EU–USA pro ochranu údajů, mohou podléhat hmotněprávnímu prosazování zásad rámce EU–USA pro ochranu údajů, i když neprovedou autocertifikaci prostřednictvím Ministerstva obchodu nebo ji nemají v platnosti.

<sup>(8)</sup> Viz seznam věcí Federální obchodní komise týkajících se „bezpečného přístavu“ a štítu na ochranu soukromí, který je uveden v dodatku A.

<sup>(9)</sup> Viz tisková zpráva, Federální obchodní komise, FTC obvinila společnost Twitter z klamavého používání údajů o zabezpečení účtů za účelem prodeje cílených reklam (25. května 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads>

<sup>(10)</sup> Viz tisková zpráva, Federální obchodní komise, FTC zakročila proti společnosti CafePress za krytí porušení zabezpečení údajů (15. března 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover>

<sup>(11)</sup> Viz tisková zpráva, Federální obchodní komise, FTC vydává nařízení v souvislosti s aplikací Flo Health, aplikací pro sledování plodnosti, která sdílela citlivé zdravotní informace se společnostmi Facebook, Google a dalšími (22. června 2021), <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>

<sup>(12)</sup> Dopis, který zaslala Marisa Lagová, náměstkyně ministryně obchodu pro mezinárodní obchod, váženému panu Didieru Reynndersovi, komisaři Evropské komise pro spravedlnost (12. prosince 2022).

## II. Upřednostňování a vyšetřování věcí předložených k přezkoumání

Stejně jako u programu „bezpečný přístav“ a rámce štítu EU–USA na ochranu soukromí se Federální obchodní komise zavazuje dát věcem týkajícím se zásad rámce EU–USA pro ochranu údajů a předloženým Ministerstvem obchodu a členskými státy EU k přezkoumání Federální obchodní komisi přednost. Budeme také upřednostňovat věci nedodržování zásad rámce EU–USA pro ochranu údajů předložené k přezkoumání samoregulačními organizacemi na ochranu soukromí a jinými nezávislými subjekty pro řešení sporů.

S cílem usnadnit předkládání věcí členskými státy EU k přezkoumání podle rámce EU–USA pro ochranu údajů vytvořila Federální obchodní komise normalizovaný proces předkládání věcí k přezkoumání a poskytuje členským státům EU pokyny k typu informací, které by Federální obchodní komisi při vyšetřování věcí předložených k přezkoumání nejlépe pomohly. V rámci tohoto úsilí určila Federální obchodní komise kontaktní místo pro věci předložené členskými státy EU k přezkoumání. Nejužitečnější je, když předkládající orgán údajné porušení předběžně prošetří a může s Federální obchodní komisí při vyšetřování spolupracovat.

Po obdržení věci předložené Ministerstvem obchodu, členským státem EU nebo samoregulační organizací nebo jiným nezávislým subjektem pro řešení sporů k přezkoumání může Federální obchodní komise přijmout za účelem řešení vznesených otázek řadu opatření. Můžeme například přezkoumat politiku ochrany soukromí dané organizace, získat přímo od dané organizace nebo od třetích stran další informace, dále věc sledovat s předkládajícím subjektem, posoudit, zda je porušování systematické či zda byl postižen významný počet spotřebitelů, určit, zda z věci předložené k přezkoumání vyplývají otázky v kompetenci Ministerstva obchodu, posoudit, zda by bylo užitečné vyvinout další úsilí k upozornění účastníků trhu, a případně zahájit vykonávací řízení.

Kromě upřednostňování věcí k přezkoumání týkajících se zásad rámce EU–USA pro ochranu údajů předložených Ministerstvem obchodu, členskými státy EU nebo samoregulačními organizacemi na ochranu soukromí nebo jinými nezávislými subjekty pro řešení sporů <sup>(13)</sup> bude Federální obchodní komise v příslušných případech i nadále z vlastního podnětu pomocí řady nástrojů prošetřovat závažná porušení zásad rámce EU–USA pro ochranu údajů. V rámci programu Federální obchodní komise týkajícího se vyšetřování problémů s ochranou soukromí a bezpečností, které se týkají obchodních organizací, agentura běžně zkoumala, zda dotčený subjekt činí prohlášení týkající se štítu EU–USA na ochranu soukromí. Jestliže subjekt tato prohlášení činil a vyšetřování odhalilo zjevné porušování zásad štítu EU–USA na ochranu soukromí, zařadila Federální obchodní komise do svých donucovacích opatření obvinění z porušování uvedených zásad. V tomto proaktivním přístupu budeme pokračovat, nyní s ohledem na zásady rámce EU–USA pro ochranu údajů.

## III. Usilování o vydávání příkazů a sledování jejich dodržování

Federální obchodní komise také potvrzuje svůj závazek usilovat o vydávání příkazů k výkonu rozhodnutí a sledovat je za účelem zajištění souladu se zásadami rámce EU–USA pro ochranu údajů. V budoucích příkazech Federální obchodní komise na základě rámce EU–USA pro ochranu údajů budeme požadovat dodržování zásad rámce EU–USA pro ochranu údajů prostřednictvím různých vhodných předběžných opatření. Porušování správních příkazů Federální obchodní komise může vést k občanskoprávním sankcím ve výši až 50 120 USD za každé porušení nebo 50 120 USD za každý den trvajícího porušování <sup>(14)</sup>, což může v případě postupů, které se dotýkají mnoha spotřebitelů, činit miliony dolarů. Každý soudní smír také zahrnuje ustanovení o předkládání zpráv a dodržování předpisů. Subjekty, na které se příkaz vztahuje, musí po určený počet let uchovávat dokumenty, které dokládají, že dodržují předpisy. Příkazy musejí být také rozeslány zaměstnancům odpovědným za zajištění jejich dodržování.

Stejně jako v případě všech svých příkazů Federální obchodní komise systematicky sleduje dodržování stávajících příkazů podle zásad štítu EU–USA na ochranu soukromí a v případě potřeby podává žaloby na jejich výkon <sup>(15)</sup>. Důležité je, že příkazy Federální obchodní komise budou nadále chránit všechny spotřebitele po celém světě, kteří vstoupí s určitým podnikem do interakce, nejen spotřebitele, již podali stížnosti. Federální obchodní komise v neposlední řadě nadále povede online seznam společností, které podléhají příkazům vydaným v souvislosti s prosazováním zásad rámce EU–USA pro ochranu údajů <sup>(16)</sup>.

<sup>(13)</sup> Ačkoli Federální obchodní komise neřeší stížnosti jednotlivých spotřebitelů ani v nich nevystupuje jako mediátor, potvrzuje, že upřednostní věci předložené k přezkoumání na základě rámce EU–USA pro ochranu údajů úřady pro ochranu osobních údajů z EU. Kromě toho využívá Federální obchodní komise stížnosti ve své databázi Consumer Sentinel, do které má přístup mnoho dalších donucovacích orgánů, ke zjišťování trendů, určování priorit v oblasti prosazování předpisů a označování potenciálních cílů vyšetřování. Občané EU mohou k předložení stížnosti Federální obchodní komisi využít tentýž systém podávání stížností, který mají k dispozici občané Spojených států, na adrese <https://reportfraud.ftc.gov/>. V případě individuálních stížností týkajících se zásad rámce EU–USA pro ochranu údajů však může být pro občany EU nejužitečnější předkládat stížnosti úřadu pro ochranu osobních údajů svého členského státu nebo nezávislému subjektu pro řešení sporů.

<sup>(14)</sup> 15 U.S.C. § 45(m); 16 C.F.R. § 1.98. Tato částka se pravidelně upravuje o inflaci.

<sup>(15)</sup> V loňském roce Federální obchodní komise odhlasovala zjednodušení postupu vyšetřování recidivistů. Viz tisková zpráva, Federální obchodní komise, FTC povoluje vyšetřování v oblasti klíčových priorit prosazování práva (1. července 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities>

<sup>(16)</sup> Srov. Federální obchodní komise, Štít na ochranu soukromí, <https://www.ftc.gov/business-guidance/privacy-security/privacy-shield>

#### IV. Spolupráce v oblasti prosazování práva s úřady EU pro ochranu osobních údajů

Federální obchodní komise uznává významnou úlohu, kterou úřady pro ochranu osobních údajů z EU v souvislosti s dodržováním zásad rámce EU–USA pro ochranu údajů hrají, a vybízí k intenzivnějším konzultacím a spolupráci na prosazování předpisů. Koordinovaný přístup k výzvám, které představuje současný vývoj na digitálním trhu a obchodní modely náročné na data, je ve skutečnosti stále významnější. Federální obchodní komise si bude vyměňovat informace o postoupených případech s předkládajícími donucovacími orgány, včetně stavu postoupeného případu, s výhradou právních předpisů a omezení týkajících se důvěrnosti. Bude-li to vzhledem k počtu a typu věcí předložených k přezkoumání proveditelné, budou poskytnuté informace obsahovat vyhodnocení předložených záležitostí, včetně popisu významných vznesených otázek a případného opatření přijatého s cílem vyřešit porušování práva v pravomoci Federální obchodní komise. Federální obchodní komise předkládajícímu orgánu také poskytne zpětnou vazbu k typům věcí předložených k přezkoumání s cílem zefektivnit úsilí o řešení protiprávního jednání. Požádá-li předkládající donucovací orgán pro účely vlastního donucovacího řízení o informace o stavu konkrétní věci předložené k přezkoumání, Federální obchodní komise odpoví s ohledem na počet posuzovaných věcí předložených k přezkoumání a v závislosti na zákonných požadavcích na zachování důvěrnosti a jiných zákonných požadavcích.

Federální obchodní komise bude také úzce spolupracovat s úřady pro ochranu osobních údajů z EU a poskytne jim pomoc při prosazování předpisů. V příslušných případech by uvedená pomoc mohla zahrnovat sdílení informací a pomoc při vyšetřování podle zákona Spojených států o bezpečném internetu (SAFE WEB Act), který Federální obchodní komisi opravňuje pomáhat cizím donucovacím orgánům, prosazují-li zákony, jež zakazují postupy, které se významně podobají postupům zakázaným zákony prosazovanými Federální obchodní komisí<sup>(17)</sup>. V rámci této pomoci může Federální obchodní komise sdílet informace získané v souvislosti s vyšetřováním Federální obchodní komise, zahájit jménem úřadu EU pro ochranu osobních údajů, který provádí vlastní vyšetřování, donucovací proces a vyslechnout v souvislosti s donucovacím řízením úřadu pro ochranu osobních údajů svědky nebo žalované, s výhradou požadavků zákona USA o bezpečném internetu. Federální obchodní komise tuto pravomoc pravidelně využívá, aby pomohla jiným orgánům po celém světě ve věcech ochrany soukromí a spotřebitele.

Kromě konzultace s příslušnými úřady EU pro ochranu osobních údajů v konkrétních záležitostech se Federální obchodní komise bude účastnit pravidelných setkání s určenými zástupci Evropského sboru pro ochranu osobních údajů, aby se obecně diskutovalo o tom, jak zlepšit spolupráci v oblasti prosazování předpisů. Federální obchodní komise se bude spolu s Ministerstvem obchodu, Evropskou komisí a zástupci Evropského sboru pro ochranu osobních údajů rovněž podílet na pravidelném přezkumu rámce EU–USA pro ochranu údajů s cílem projednat jeho provádění. Federální obchodní komise rovněž vybízí k rozvoji nástrojů, které posílí spolupráci v oblasti prosazování předpisů s úřady EU pro ochranu osobních údajů, jakož i s dalšími orgány na ochranu soukromí na celém světě. Federální obchodní komise s potěšením potvrzuje svůj závazek prosazovat aspekty rámce EU–USA pro ochranu údajů týkající se obchodního sektoru. Naše partnerství s kolegy z EU považujeme za zásadní součást zajištění ochrany soukromí jak pro naše občany, tak pro Vaše občany.

S úctou



Lina M. KHAN

předsedkyně, Federální obchodní komise

<sup>(17)</sup> Při určování toho, zda uplatnit svou pravomoc podle zákona Spojených států o bezpečném internetu, Federální obchodní komise mj. zvažuje: „A) zda dožadující agentura souhlasila s poskytnutím reciproční pomoci komisi nebo zda takovou pomoc poskytne, B) zda by vyhovění žádosti ohrozilo veřejný zájem Spojených států a C) zda se vyšetřování či donucovací řízení dožadující agentury týká jednání či praktik, které způsobují nebo je pravděpodobné, že způsobí škody významnému počtu osob“. 15 U.S.C. § 46(j)(3). Tato pravomoc se nevztahuje na prosazování zákonů o hospodářské soutěži.

## Dodatek A

## Prosazování štítu na ochranu soukromí a bezpečného přístavu

|    | Spis FTC č. / Reg. č.                                   | Věc                                                                                                                   | Odkaz              |
|----|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|--------------------|
| 1  | Spis FTC č. 2023062<br>Věc č. 3:22-cv-03070 (N.D. Cal.) | USA v. <b>Twitter, Inc.</b>                                                                                           | Twitter            |
| 2  | Spis FTC č. 192 3209                                    | Ve věci Residual Pumpkin Entity, LLC, dříve d/b/a <b>CafePress</b> , a PlanetArt, LLC, d/b/a <b>CafePress</b>         | CafePress          |
| 3  | Spis FTC č. 192 3133<br>Reg. č. C-4747                  | Ve věci <b>Flo Health, Inc.</b>                                                                                       | Flo Health         |
| 4  | Spis FTC č. 192 3050<br>Reg. č. C-4723                  | Ve věci <b>Ortho-Clinical Diagnostics, Inc.</b>                                                                       | Ortho-Clinical     |
| 5  | Spis FTC č. 192 3092<br>Reg. č. C-4709                  | Ve věci <b>T&amp;M Protection, LLC</b>                                                                                | T&M Protection     |
| 6  | Spis FTC č. 192 3084<br>Reg. č. C-4704                  | Ve věci <b>TDARX, Inc.</b>                                                                                            | TDARX              |
| 7  | Spis FTC č. 192 3093<br>Reg. č. C-4706                  | Ve věci <b>Global Data Vault, LLC</b>                                                                                 | Global Data        |
| 8  | Spis FTC č. 192 3078<br>Reg. č. C-4703                  | Ve věci <b>Incentive Services, Inc.</b>                                                                               | Incentive Services |
| 9  | Spis FTC č. 192 3090<br>Reg. č. C-4705                  | Ve věci <b>Click Labs, Inc.</b>                                                                                       | Click Labs         |
| 10 | Spis FTC č. 182 3192<br>Reg. č. C-4697                  | Ve věci <b>Medable, Inc.</b>                                                                                          | Medable            |
| 11 | Spis FTC č. 182 3189<br>Reg. č. 9386                    | Ve věci NTT Global Data Centers Americas, Inc., jako právní nástupce společnosti <b>RagingWire Data Centers, Inc.</b> | RagingWire         |
| 12 | Spis FTC č. 182 3196<br>Reg. č. C-4702                  | Ve věci <b>Thru, Inc.</b>                                                                                             | Thru               |
| 13 | Spis FTC č. 182 3188<br>Reg. č. C-4698                  | Ve věci <b>DCR Workforce, Inc.</b>                                                                                    | DCR Workforce      |
| 14 | Spis FTC č. 182 3194<br>Reg. č. C-4700                  | Ve věci <b>LotaData, Inc.</b>                                                                                         | LotaData           |
| 15 | Spis FTC č. 182 3195<br>Reg. č. C-4701                  | Ve věci <b>EmpiriStat, Inc.</b>                                                                                       | EmpiriStat         |

|    |                                        |                                                                 |                     |
|----|----------------------------------------|-----------------------------------------------------------------|---------------------|
| 16 | Spis FTC č. 182 3193<br>Reg. č. C-4699 | Ve věci 214 Technologies, Inc., rovněž d/b/a <b>Trueface.ai</b> | Trueface.ai         |
| 17 | Spis FTC č. 182 3107<br>Reg. č. 9383   | Ve věci <b>Cambridge Analytica, LLC</b>                         | Cambridge Analytica |
| 18 | Spis FTC č. 182 3152<br>Reg. č. C-4685 | Ve věci <b>SecureTest, Inc.</b>                                 | SecurTest           |
| 19 | Spis FTC č. 182 3144<br>Reg. č. C-4664 | Ve věci <b>VenPath, Inc.</b>                                    | VenPath             |
| 20 | Spis FTC č. 182 3154<br>Reg. č. C-4666 | Ve věci <b>SmartStart Employment Screening, Inc.</b>            | SmartStart          |
| 21 | Spis FTC č. 182 3143<br>Reg. č. C-4663 | Ve věci <b>mResourceLLC</b> , d/b/a Loop Works LLC              | mResource           |
| 22 | Spis FTC č. 182 3150<br>Reg. č. C-4665 | Ve věci <b>IDmission LLC</b>                                    | IDmission           |
| 23 | Spis FTC č. 182 3100<br>Reg. č. C-4659 | Ve věci <b>ReadyTech Corporation</b>                            | ReadyTech           |
| 24 | Spis FTC č. 172 3173<br>Reg. č. C-4630 | Ve věci <b>Decusoft, LLC</b>                                    | Decusoft            |
| 25 | Spis FTC č. 172 3171<br>Reg. č. C-4628 | Ve věci <b>Tru Communication, Inc.</b>                          | Tru                 |
| 26 | Spis FTC č. 172 3172<br>Reg. č. C-4629 | Ve věci <b>Md7, LLC</b>                                         | Md7                 |
| 30 | Spis FTC č. 152 3198<br>Reg. č. C-4543 | Ve věci <b>Jhayrmaine Daniels (d/b/a California Skate-Line)</b> | Jhayrmaine Daniels  |
| 31 | Spis FTC č. 152 3190<br>Reg. č. C-4545 | Ve věci <b>Dale Jarrett Racing Adventure, Inc.</b>              | Dale Jarrett        |
| 32 | Spis FTC č. 152 3141<br>Reg. č. C-4540 | Ve věci <b>Golf Connect, LLC</b>                                | Golf Connect        |
| 33 | Spis FTC č. 152 3202<br>Reg. č. C-4546 | Ve věci <b>Inbox Group, LLC</b>                                 | Inbox Group         |
| 34 | Spis č. 152 3187<br>Reg. č. C-4542     | Ve věci <b>IOActive, Inc.</b>                                   | IOActive            |
| 35 | Spis FTC č. 152 3140<br>Reg. č. C-4549 | Ve věci <b>Jubilant Clinsys, Inc.</b>                           | Jubilant            |
| 36 | Spis FTC č. 152 3199<br>Reg. č. C-4547 | Ve věci <b>Just Bagels Manufacturing, Inc.</b>                  | Just Bagels         |

|    |                                        |                                                                     |                      |
|----|----------------------------------------|---------------------------------------------------------------------|----------------------|
| 37 | Spis FTC č. 152 3138<br>Reg. č. C-4548 | Ve věci <b>NAICS Association, LLC</b>                               | NAICS                |
| 38 | Spis FTC č. 152 3201<br>Reg. č. C-4544 | Ve věci <b>One Industries Corp.</b>                                 | One Industries       |
| 39 | Spis FTC č. 152 3137<br>Reg. č. C-4550 | Ve věci <b>Pinger, Inc.</b>                                         | Pinger               |
| 40 | Spis FTC č. 152 3193<br>Reg. č. C-4552 | Ve věci <b>SteriMed Medical Waste Solutions</b>                     | SteriMed             |
| 41 | Spis FTC č. 152 3184<br>Reg. č. C-4541 | Ve věci <b>Contract Logix, LLC</b>                                  | Contract Logix       |
| 42 | Spis FTC č. 152 3185<br>Reg. č. C-4551 | Ve věci <b>Forensics Consulting Solutions, LLC</b>                  | Forensics Consulting |
| 43 | Spis FTC č. 152 3051<br>Reg. č. C-4526 | Ve věci <b>American Int'l Mailing, Inc.</b>                         | AIM                  |
| 44 | Spis FTC č. 152 3015<br>Reg. č. C-4525 | Ve věci <b>TES Franchising, LLC</b>                                 | TES                  |
| 45 | Spis FTC č. 142 3036<br>Reg. č. C-4459 | Ve věci <b>American Apparel, Inc.</b>                               | American Apparel     |
| 46 | Spis FTC č. 142 3026<br>Reg. č. C-4469 | Ve věci <b>Fantage.com, Inc.</b>                                    | Fantage              |
| 47 | Spis FTC č. 142 3017<br>Reg. č. C-4461 | Ve věci <b>Apperian, Inc.</b>                                       | Apperian             |
| 48 | Spis FTC č. 142 3018<br>Reg. č. C-4462 | Ve věci <b>Atlanta Falcons Football Club, LLC</b>                   | Atlanta Falcons      |
| 49 | Spis FTC č. 142 3019<br>Reg. č. C-4463 | Ve věci <b>Baker Tilly Virchow Krause, LLP</b>                      | Baker Tilly          |
| 50 | Spis FTC č. 142 3020<br>Reg. č. C-4464 | Ve věci <b>BitTorrent, Inc.</b>                                     | BitTorrent           |
| 51 | Spis FTC č. 142 3022<br>Reg. č. C-4465 | Ve věci <b>Charles River Laboratories, Int'l</b>                    | Charles River        |
| 52 | Spis FTC č. 142 3023<br>Reg. č. C-4466 | Ve věci <b>DataMotion, Inc.</b>                                     | DataMotion           |
| 53 | Spis FTC č. 142 3024<br>Reg. č. C-4467 | Ve věci <b>DDC Laboratories, Inc., d/b/a DNA Diagnostics Center</b> | DDC                  |
| 54 | Spis FTC č. 142 3028<br>Reg. č. C-4470 | Ve věci <b>Level 3 Communications, LLC</b>                          | Level 3              |

|    |                                                                         |                                                                                                                |                      |
|----|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|----------------------|
| 55 | Spis FTC č. 142 3025<br>Reg. č. C-4468                                  | Ve věci <b>PDB Sports, Ltd.</b> , d/b/a the Denver Broncos Football Club, LLP                                  | Broncos              |
| 56 | Spis FTC č. 142 3030<br>Reg. č. C-4471                                  | Ve věci <b>Reynolds Consumer Products, Inc.</b>                                                                | Reynolds             |
| 57 | Spis FTC č. 142 3031<br>Reg. č. C-4472                                  | Ve věci <b>Receivable Management Services Corporation</b>                                                      | Receivable Mgmt      |
| 58 | Spis FTC č. 142 3032<br>Reg. č. C-4473                                  | Ve věci <b>Tennessee Football, Inc.</b>                                                                        | Tennessee Football   |
| 59 | Spis FTC č. 102 3058<br>Reg. č. C-4369                                  | Ve věci <b>Myspace LLC</b>                                                                                     | Myspace              |
| 60 | Spis FTC č. 092 3184<br>Reg. č. C-4365                                  | Ve věci <b>Facebook, Inc.</b>                                                                                  | Facebook             |
| 61 | Spis FTC č. 092 3081<br>Občanskoprávní žaloba č. 09-CV-5276 (C.D. Cal.) | FTC v. Javian Karnani a <b>Balls of Kryptonite, LLC</b> , d/b/a Bite Size Deals, LLC a Best Priced Brands, LLC | Balls of Kryptonite  |
| 62 | Spis FTC č. 102 3136<br>Reg. č. C-4336                                  | Ve věci <b>Google, Inc.</b>                                                                                    | Google               |
| 63 | Spis FTC č. 092 3137<br>Reg. č. C-4282                                  | Ve věci <b>World Innovators, Inc.</b>                                                                          | World Innovators     |
| 64 | Spis FTC č. 092 3141<br>Reg. č. C-4271                                  | Ve věci <b>Progressive Gaitways LLC</b>                                                                        | Progressive Gaitways |
| 65 | Spis FTC č. 092 3139<br>Reg. č. C-4270                                  | Ve věci <b>Onyx Graphics, Inc.</b>                                                                             | Onyx Graphics        |
| 66 | Spis FTC č. 092 3138<br>Reg. č. C-4269                                  | Ve věci <b>ExpatEdge Partners, LLC</b>                                                                         | ExpatEdge            |
| 67 | Spis FTC č. 092 3140<br>Reg. č. C-4281                                  | Ve věci <b>Directors Desk LLC</b>                                                                              | Directors Desk       |
| 68 | Spis FTC č. 092 3142<br>Reg. č. C-4272                                  | Ve věci <b>Collectify LLC</b>                                                                                  | Collectify           |

## PŘÍLOHA V

**THE SECRETARY OF TRANSPORTATION**  
WASHINGTON, DC 20590

6. července 2023

Komisař Didier Reynders  
Evropská komise  
Rue de la Loi/Wetstraat 200  
1049 1049 Bruxelles/Brussel  
Belgique/België

Vážený pane komisaři Reyndersi,

Ministerstvo dopravy Spojených států (dále též „ministerstvo“ nebo „MD“) si váží příležitosti popsat svou úlohu v prosazování zásad rámce EU–USA pro ochranu údajů. Tento rámec bude hrát životně důležitou úlohu v ochraně osobních údajů poskytovaných během obchodních transakcí v čím dál tím propojenějším světě. Umožní podnikům provádět významné operace v rámci celosvětového hospodářství a zároveň zajistí důležitou ochranu soukromí spotřebitelů v EU.

MD nejprve veřejně vyjádřilo svůj závazek prosazovat rámec „bezpečného přístavu“ mezi USA a EU v dopise zaslaném Evropské komisi před více než 22 lety, přičemž tyto závazky byly zopakovány a rozšířeny v dopise z roku 2016 týkajícím se rámce štítu EU–USA na ochranu soukromí. MD se v těchto dopisech zavázalo důrazně prosazovat zásady „bezpečného přístavu“ mezi USA a EU a poté zásady štítu EU–USA na ochranu soukromí. MD tento závazek rozšířilo na zásady rámce EU–USA pro ochranu údajů a tento dopis je toho důkazem.

MD zejména potvrzuje svůj závazek v těchto klíčových oblastech: 1) upřednostňování vyšetřování údajných porušení zásad rámce EU–USA pro ochranu údajů; 2) vhodná donucovací opatření vůči subjektům, které se dopustí nepravdivých nebo klamavých tvrzení o účasti v rámci EU–USA pro ochranu údajů, a 3) sledování a zveřejňování příkazů k výkonu rozhodnutí týkajících se porušování zásad rámce EU–USA pro ochranu údajů. Poskytujeme informace o každém z těchto závazků a pro účely potřebných souvislostí nezbytné základní informace o úloze MD při ochraně soukromí spotřebitelů a prosazování zásad rámce EU–USA pro ochranu údajů.

**1. Souvislosti****A. Pravomoc MD v oblasti ochrany soukromí**

Ministerstvo je pevně odhodláno zajistit ochranu soukromí informací poskytovaných

spotřebiteli leteckým dopravcům a prodejcům letenek. Pravomoc MD přijímat opatření v této oblasti je zakotvena v ustanovení 49 U.S.C. § 41712, který zakazuje, aby se letecký dopravce nebo prodejce letenek při prodeji letenek dopouštěl „nekalých či klamavých praktik“. Vzorem pro § 41712 je

§ 5 zákona o Federální obchodní komisi (Federal Trade Commission Act) (15 U.S.C. § 45). MD nedávno vydalo předpisy definující nekalé a klamavé praktiky, které jsou v souladu s předchozími rozhodnutími MD i Federální obchodní komise (14 CFR § 399.79). Konkrétně je praktika „nekalá“, pokud způsobuje podstatnou újmu, které nelze přiměřeně zabránit, nebo je pravděpodobné, že ji způsobí, a újma není vyvážena

výhodami pro spotřebitele nebo hospodářskou soutěž. Praktika je pro spotřebitele „klamavá“, jestliže je pravděpodobné, že spotřebitele, který za daných okolností jedná přiměřeně, uvede v omyl, pokud jde o významnou záležitost. Záležitost je významná, pokud by mohla ovlivnit chování nebo rozhodnutí spotřebitele ve vztahu k danému výrobku nebo službě. Kromě těchto obecných zásad MD konkrétně vykládá § 41712 v tom smyslu, že zakazuje dopravcům a prodejcům letenek: 1) porušovat podmínky jejich politiky ochrany soukromí; 2) porušovat jakákoli pravidla vydaná ministerstvem, která označují konkrétní praktiky v oblasti 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 Federální obchodní komise, jimiž se zákon COPPA provádí, nebo 4) nedodržovat jako účastník rámce EU–USA pro ochranu údajů zásady rámce EU–USA pro ochranu údajů <sup>(1)</sup>.

Jak je uvedeno výše, podle federálního práva má MD výlučnou pravomoc regulovat postupy leteckých dopravců v oblasti ochrany soukromí a pravomoc sdílenou s Federální obchodní komisí nad postupy prodejců letenek v oblasti ochrany soukromí.

Jakmile se tedy letecký dopravce nebo prodejce letenek veřejně zaváže dodržovat zásady rámce EU–USA pro ochranu údajů, může ministerstvo využívat své zákonné pravomoci uvedené v § 41712, aby zajistilo dodržování uvedených zásad. Jakmile tedy cestující poskytnou informace leteckému dopravci nebo prodejci letenek, který se zavázal ctít zásady rámce EU–USA pro ochranu údajů, představovalo by jakékoli porušení těchto zásad dopravcem či prodejcem letenek porušení § 41712.

#### B. Postupy prosazování předpisů

Věci podle předpisu 49 U.S.C. § 41712 vyšetřuje a stíhá Úřad ministerstva na ochranu spotřebitelů v letectví (Office of Aviation Consumer Protection, dále též „úřad OACP“) <sup>(2)</sup>. Zákonný zákaz nekalých a klamavých praktik stanovený v § 41712 prosazuje převážně jednáním, přípravou příkazů ke zdržení se konání a zpracováváním usnesení o vyměření občanskoprávních sankcí. O potenciálních porušeních předpisů se úřad většinou dozvídá ze stížností, které obdrží od fyzických osob, cestovních agentur, leteckých dopravců a amerických a zahraničních vládních agentur. K podávání stížností ve věci ochrany soukromí na letecké dopravce a prodejce letenek mohou spotřebitelé využít internetové stránky MD <sup>(3)</sup>.

Není-li věc přiměřeně a vhodně urovnána, má úřad OACP pravomoc zahájit donucovací řízení, které zahrnuje důkazní řízení před správním soudcem MD. Správní soudce má pravomoc vydávat příkazy ke zdržení se konání a ukládat občanskoprávní sankce. Porušení § 41712 může vést k vydání příkazů ke zdržení se konání a k uvalení občanskoprávních sankcí do výše 37 377 USD za každé porušení uvedeného paragrafu.

Ministerstvo nemá pravomoc přiznávat jednotlivým stěžovatelům náhradu škody nebo poskytovat finanční odškodnění. Ministerstvo však má pravomoc schvalovat vyrovnání, která jsou výsledkem vyšetřování provedených jeho úřadem OACP a která přinášejí spotřebitelům přímý prospěch (např. hotovost, poukazy), jako kompenzaci za peněžní sankce, jež by jinak byly splatné vládě Spojených států. K tomu v minulosti již došlo a může k tomu také dojít v souvislosti se zásadami rámce EU–USA pro ochranu údajů, vyžádají-li si to okolnosti. Opakované porušování § 41712 leteckým dopravcem by rovněž vzbudilo pochybnosti o připravenosti takového dopravce dodržovat zásady, což by mohlo v mimořádně závažných případech vést k tomu, že letecký dopravce by již nebyl považován za provozuschopného, takže by mu bylo odňato povolení k provozování letecké dopravy.

Dosud MD obdrželo poměrně málo stížností na údajné porušení ochrany soukromí prodejci letenek nebo leteckými dopravci. Vyvstanou-li stížnosti, jsou vyšetřeny podle zásad stanovených výše.

#### C. Právní ochrana poskytovaná Ministerstvem dopravy ve prospěch spotřebitelů z EU

Podle § 41712 se zákaz nekalých nebo klamavých praktik v letecké dopravě či prodeji letenek vztahuje jak na americké, tak na zahraniční letecké dopravce i prodejce letenek. MD často přijímá opatření proti americkým i zahraničním leteckým dopravcům z důvodu postupů, které se dotýkají jak zahraničních, tak amerických spotřebitelů a ke kterým dochází při poskytování dopravy do nebo ze Spojených států. MD využívá a bude nadále využívat všechny opravné prostředky, které má k dispozici k ochraně zahraničních i amerických spotřebitelů před nekalými nebo klamavými praktikami regulovaných subjektů v letecké dopravě.

<sup>(1)</sup> <https://www.transportation.gov/individuals/aviation-consumer-protection/privacy>

<sup>(2)</sup> Dříve známý jako Office of Aviation Enforcement and Proceedings (Úřad pro prosazování předpisů a řízení v letectví).

<sup>(3)</sup> <http://www.transportation.gov/airconsumer/privacy-complaints>

MD také v souvislosti s leteckými dopravci prosazuje další cílené zákony, jejichž ochrana se vztahuje i na spotřebitele mimo Spojené státy, například zákon o ochraně soukromí dětí na internetu (dále též „zákon COPPA“). Zákon COPPA mj. vyžaduje, aby provozovatelé internetových stránek a on-line služeb zaměřených na děti nebo stránek pro širokou veřejnost, které vědomě sbírají osobní informace od dětí mladších třinácti let, rodiče uvědomili a získali jejich ověřitelný souhlas. Zákon COPPA musí dodržovat internetové stránky a služby provozované poskytovateli se sídlem ve Spojených státech, které podléhají uvedenému zákonu a sbírají osobní informace od nezletilých cizinců. Zákon COPPA musí dodržovat také internetové stránky a on-line služby provozované poskytovateli se sídlem v zahraničí, jestliže se zaměřují na děti ve Spojených státech nebo od nich vědomě sbírají osobní informace. Pokud američtí nebo zahraniční letečtí dopravci, kteří podnikají ve Spojených státech, zákon COPPA poruší, má MD pravomoc přijmout donucovací opatření.

## II. Prosazování zásad rámce EU–USA pro ochranu údajů

Jestliže se letecký dopravce nebo prodejce letenek rozhodne účastnit se rámce EU–USA pro ochranu údajů a ministerstvo obdrží stížnost, že tento letecký dopravce či prodejce letenek údajně zásady rámce EU–USA pro ochranu údajů porušil, podnikne za účelem důsledného prosazování těchto zásad tyto kroky.

### A. Přednostní vyšetřování údajných porušení

Úřad OACP vyšetří každou stížnost na údajné porušení zásad rámce EU–USA pro ochranu údajů, včetně stížností obdržených od úřadů pro ochranu osobních údajů z EU, a budou-li existovat důkazy o porušení, přijme donucovací opatření.

Úřad OACP bude dále spolupracovat s Federální obchodní komisí a Ministerstvem obchodu a přednostně posoudí tvrzení, že regulované subjekty nedodržují závazky chránit soukromí učiněné na základě rámce EU–USA pro ochranu údajů.

Po obdržení oznámení o údajném porušení zásad rámce EU–USA pro ochranu údajů může úřad OACP přijmout v rámci svého vyšetřování řadu opatření. Může například přezkoumat politiky ochrany soukromí prodejce letenek nebo leteckého dopravce, získat další informace od prodejce letenek, leteckého dopravce či třetích stran, věc s předkládajícím subjektem dále sledovat a posoudit, zda je porušování systematické nebo zda byl postižen významný počet spotřebitelů. Dále by úřad určil, zda z uvedené věci vyplývají otázky v kompetenci Ministerstva obchodu nebo Federální obchodní komise, posoudil, zda by pomohla osvěta spotřebitelů a podniků, a popřípadě zahájil donucovací řízení.

Dozví-li se ministerstvo o potenciálních porušeních zásad rámce EU–USA pro ochranu údajů, koordinuje svůj postup s Federální obchodní komisí. Rovněž budeme o výsledku případného donucovacího opatření ve věci zásad rámce EU–USA pro ochranu údajů informovat Federální obchodní komisí a Ministerstvo obchodu.

### B. Řešení nepravdivých nebo klamavých tvrzení o účasti

Ministerstvo zůstává odhodláno vyšetřovat porušení zásad rámce EU–USA pro ochranu údajů, včetně nepravdivých nebo klamavých tvrzení o účasti v rámci EU–USA pro ochranu údajů. Přednostně posoudíme věci předložené k přezkoumání Ministerstvem obchodu, které se budou týkat organizací označených za organizace, jež nepravdivě tvrdí, že jsou účastníky rámce EU–USA pro ochranu údajů, nebo bez povolení užívají certifikační ochrannou značku rámce EU–USA pro ochranu údajů.

Kromě toho oznamujeme, že jestliže politika určité organizace na ochranu soukromí tvrdí, že organizace dodržuje zásady rámce EU–USA pro ochranu údajů, a uvedená organizace neprovede autocertifikaci u Ministerstva obchodu nebo svou certifikaci neprodlouží, tato skutečnost ji nezpřestí prosazování uvedených závazků Ministerstvem dopravy.

### C. Sledování a zveřejňování příkazů k výkonu rozhodnutí týkajících se porušování rámce EU–USA pro ochranu údajů

Úřad OACP je také nadále odhodlán sledovat podle potřeby výkon příkazů s cílem zajistit dodržování zásad rámce EU–USA pro ochranu údajů. Konkrétně vydá-li úřad příkaz, aby se letecký dopravce nebo prodejce letenek v budoucnu zdržel porušování zásad rámce EU–USA pro ochranu údajů a § 41712, bude sledovat, zda subjekt ustanovení o zdržení se konání uvedené v příkazu dodržuje. Kromě toho úřad zajistí, aby příkazy ve věcech zásad rámce EU–USA pro ochranu údajů byly dostupné na jeho internetové stránce.

Těšíme se na pokračování naší spolupráce se svými federálními partnery i zúčastněnými subjekty v EU ve věcech rámce EU–USA pro ochranu údajů.

Doufám, že Vám tyto informace budou nápomocny. Prosím, obraťte se na mě, budete-li mít jakékoli otázky nebo budete-li potřebovat další informace.

S úctou



Pete BUTTIGIEG

---

## PŘÍLOHA VI



Ministerstvo spravedlnosti USA

Trestní oddělení

Úřad náměstka ministra spravedlnosti

Washington, D.C. 20530

23. června 2023

Paní Ana Gallego Torresová  
Generální ředitelka pro spravedlnost a spotřebitele  
Evropská komise  
Rue Montoyer/Montoyerstraat 59  
1049 Bruxelles/Brussel  
Belgique/België

Vážená paní generální ředitelko Gallego Torresová,

tento dopis poskytuje krátký přehled primárních vyšetřovacích nástrojů využívaných pro získávání obchodních údajů a dalších informací ze záznamů od společností ve Spojených státech pro účely prosazování trestního práva nebo veřejného zájmu (občanského a regulačního), včetně omezení přístupu stanovených v těchto oprávněních<sup>(1)</sup>. Všechny zákonné postupy popsání v tomto dopise nerozlišují státní příslušnost ani místo pobytu subjektu údajů, jehož informace mají být získány od společností ve Spojených státech, včetně společností, které se budou autocertifikovat prostřednictvím rámce EU–USA pro ochranu údajů. Dále společnosti, které ve Spojených státech obdrží soudní příkaz, jej mohou napadnout u soudu, jak je uvedeno níže<sup>(2)</sup>.

Pokud jde o zachytávání údajů orgány veřejné moci, je důležitý zejména čtvrtý dodatek Ústavy Spojených států, který stanoví, že „[p]rávo lidí na ochranu svobody osobní, domovní, písemností a majetku před nepřiměřenými prohlídkami, zadržením a zabavením nesmí být porušeno a příkaz k prohlídce smí být vydán, jen pokud existuje důvodné podezření podložené výpovědí pod přísahou nebo jinak potvrzené, a musí konkrétně popisovat místo, jež má být prohledáno, osoby, které mají být zadrženy, nebo předměty, které mají být zabaveny“. Čtvrtý dodatek Ústavy Spojených států amerických. Jak rozhodl Nejvyšší soud Spojených států amerických ve věci *Berger v. State of New York*, „[h]lavním cílem tohoto dodatku, jak bylo uznáno v bezpočtu rozhodnutí tohoto soudu, je ochránit soukromí a bezpečnost fyzických osob před jejich svévolným narušováním ze strany vládních úředníků.“ 388 U.S. 41, 53 (1967) (citující věc *Camara v. Mun. Court of San Francisco*, 387 U.S. 523, 528 (1967)). Při vnitrostátních trestních vyšetřováních čtvrtý dodatek obecně vyžaduje, aby pracovníci donucovacích orgánů před provedením prohlídky získali soudní příkaz k prohlídce. Viz věc *Katz v. United States*, 389 U.S. 347, 357 (1967). Normy pro vydání příkazu, jako je důvodné podezření a zvláštní požadavky, se vztahují na příkazy k fyzickým prohlídkám a zajištění věci, jakož i na příkazy k uloženému obsahu elektronických komunikací

<sup>(1)</sup> V tomto přehledu nejsou popsány vyšetřovací nástroje národní bezpečnosti využívané donucovacími orgány při vyšetřování terorismu a při jiných vyšetřováních v oblasti národní bezpečnosti, včetně National Security Letters pro některé informace ze záznamů v úvěrových zprávách, finančních záznamech a elektronickém odběru a v transakčních záznamech, 12 U.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 elektronický dohled, příkazy k prohlídce, obchodní záznamy a další shromažďování informací podle zákona FISA, 50 U.S.C. § 1801 a násl.

<sup>(2)</sup> V tomto dopise se hovoří o pravomocích federálních donucovacích a regulačních orgánů. Porušení státních zákonů jsou vyšetřována donucovacími orgány jednotlivých států USA a souzena soudy těchto států. Státní donucovací orgány používají soudní příkazy a předvolání vydané podle státního práva v podstatě stejným způsobem, jaký je popsán zde, ale s možností, že soudní řízení na úrovni státu může podléhat další ochraně podle ústavy nebo zákonů daného státu, která může jít nad rámec Ústavy Spojených států. Ochrana podle státního práva musí být minimálně na stejné úrovni jako ochrana podle Ústavy Spojených států, mimo jiné včetně čtvrtého dodatku.

vydané podle zákona o uchovávaných komunikacích, jak je uvedeno níže. Pokud se na danou situaci požadavek soudního příkazu nevztahuje, podléhá vládní činnost zkoušce „přiměřenosti“ podle čtvrtého dodatku. Sama Ústava tedy zabezpečuje, aby vláda Spojených států neměla neomezenou nebo svévolnou moc zachycovat soukromé informace <sup>(3)</sup>.

Orgány pro prosazování trestního práva:

Federální státní zástupci, kteří jsou pracovníky Ministerstva spravedlnosti, a federální vyšetřovatelé, včetně agentů Federálního úřadu pro vyšetřování (FBI), donucovacího orgánu patřícího pod Ministerstvo spravedlnosti, jsou oprávněni vyžadovat předložení dokumentů a dalších informací ze záznamů společností ve Spojených státech pro účely trestního vyšetřování prostřednictvím několika typů povinných zákonných postupů, včetně předvolání velkou porotou, správních předvolání a příkazů k prohlídce, a mohou získat další komunikaci v rámci federálních pravomocí odposlechu telefonních rozhovorů a získávání informací ze zařízení pro zaznamenávání informací o odchozí komunikaci sledovaného zařízení (pen registers).

Předvolání velkou porotou nebo soudní předvolání: Předvolání v trestní věci se používají k podpoře zacílených vyšetřování prováděných donucovacími orgány. Předvolání velkou porotou je úřední žádost vydaná velkou porotou (obvykle na žádost federálního státního zástupce) na podporu vyšetřování před velkou porotou ve věci konkrétního podezření z porušení trestního práva. Velké poroty jsou vyšetřovací větví soudu, porotci jsou vybíráni soudcem nebo vyšetřujícím soudcem. Předvoláním lze předvolat osobu ke svědecké výpovědi v řízení nebo k předložení či zpřístupnění obchodních záznamů, elektronicky uložených informací nebo jiných hmotných předmětů. Informace musí mít pro vyšetřování význam a předvolání nesmí být nepřiměřené z důvodu přílišné šíře, represivnosti nebo tíže břemene. Na základě takových skutečností totiž může adresát předvolání napadnout. Viz Fed. R. Crim. P. 17. V omezených případech lze poté, co v případě došlo k obžalování velkou porotou, využít předvolání k předložení dokumentů v soudním řízení.

Pravomoc vydávat správní předvolání: Pravomoc vydávat správní předvolání lze vykonávat v trestněprávním i občanskoprávním vyšetřování. V kontextu prosazování trestního práva několik federálních zákonů povoluje využití správního předvolání k předložení nebo zpřístupnění obchodních záznamů, elektronicky uložených informací či jiných hmotných předmětů ve vyšetřováních týkajících se podvodů v oblasti zdravotní péče, zneužívání dětí, ochrany tajné služby a případů kontrolovaných létek a ve vyšetřováních generálního inspektora týkajících se vládních agentur. Usiluje-li vláda o uplatnění správního předvolání u soudu, může adresát správního předvolání, stejně jako adresát předvolání velkou porotou, tvrdit, že je předvolání nepřiměřené z důvodu přílišné šíře, represivnosti nebo tíže břemene.

Soudní příkazy týkající se zařízení pro zaznamenávání informací o odchozí komunikaci sledovaného zařízení (pen register) nebo zařízení pro zaznamenávání informací o příchozí komunikaci sledovaného zařízení (trap and trace): Podle trestněprávních ustanovení o zařízeních pro zaznamenávání informací o odchozí komunikaci sledovaného zařízení a zařízeních pro zaznamenávání informací o příchozí komunikaci sledovaného zařízení mohou donucovací orgány obdržet soudní příkaz k získání informací v reálném čase o vytáčení, směrování, adresování a signálování, které se netýkají obsahu, ohledně telefonního čísla nebo e-mailu, a to na základě certifikace toho, že poskytované informace jsou důležité pro probíhající trestní vyšetřování. Viz 18 U.S.C. § 3121–3127. Nezákonné použití nebo nainstalování takových zařízení je federálním trestným činem.

Zákon o soukromí elektronických komunikací (Electronic Communications Privacy Act, ECPA): Další pravidla upravují přístup vlády k informacím o odběratelích, k údajům o provozu a k uchovávanému obsahu komunikací v držení poskytovatelů internetových služeb, telefonních společností a jiných třetích stran poskytujících služby podle hlavy II zákona o soukromí elektronických komunikací, kterému se též říká zákon o uchovávaných komunikacích (Stored Communications Act, SCA) (18 U.S.C. § 2701–2712). Zákon o uchovávaných komunikacích stanovuje systém zákonných práv na ochranu soukromí, který omezuje přístup donucovacích orgánů k údajům nad rámec toho, co je podle ústavního práva požadováno od zákazníků a odběratelů poskytovatelů internetových služeb. Zákon o uchovávaných komunikacích poskytuje zvýšenou úroveň ochrany soukromí v závislosti na míře narušování soukromí shromažďováním informací. Pro získání registračních informací, IP adres a souvisejících časových razítek a vyplněných fakturačních informací

<sup>(3)</sup> Pokud jde o zásady čtvrtého dodatku týkající se ochrany soukromí a bezpečnostních zájmů, které jsou projednávány výše, soudy USA tyto zásady pravidelně uplatňují na nové typy vyšetřovacích nástrojů donucovacích orgánů, které jsou umožněny technologickým vývojem. Například v roce 2018 Nejvyšší soud rozhodl, že získávání historických záznamů o poloze mobilních telefonů od mobilní telefonní společnosti po delší dobu vládou v rámci vyšetřování v oblasti vymáhání práva je „prohlídkou“, na kterou se vztahuje požadavek čtvrtého dodatku. *Carpenter v. Spojené státy*, 138 S. Ct. 2206 (2018).

o odběratelích musí donucovací orgány získat soudní předvolání. Pro většinu ostatních uchovávaných informací netýkajících se obsahu, jako jsou hlavičky e-mailů bez předmětu, musí donucovací orgány předložit soudci konkrétní fakta, která dokazují, že požadované informace jsou relevantní a závažné pro probíhající trestní vyšetřování. Pro získání uchovávaného obsahu elektronických komunikací, musí donucovací orgány od soudce obvykle získat příkaz založený na důvodném podezření, že dotčený účet obsahuje důkaz trestného činu. Zákon o uchovávaných komunikacích také upravuje občanskoprávní odpovědnost a trestní sankce <sup>(4)</sup>.

Soudní příkazy sledování podle federálního zákona o odposlechu: Dále podle federálního zákona o odposlechu mohou donucovací orgány pro účely trestního vyšetřování zachycovat v reálném čase telefonické, ústní nebo elektronické komunikace. Viz 18 U.S.C. § 2510–2523. Tuto pravomoc mohou vykonávat pouze v souladu se soudním příkazem, v němž soudce mimo jiné shledá, že existuje důvodné podezření, že odposlech nebo elektronické zachycování povedou k získání důkazu o federálním trestném činu nebo o místě, kde se nachází osoba vyhýbající se stíhání. Tento zákon také upravuje občanskoprávní odpovědnost a trestní sankce za porušení ustanovení o odposlechu.

Příkaz k prohlídce – Fed R. Crim. P. pravidlo 41: Donucovací orgány mohou fyzicky prohledávat prostory ve Spojených státech, pokud jim to povolil soudce. Musí soudci na základě důvodného podezření prokázat, že došlo či v blízké době dojde ke spáchání trestného činu a že prvky související s ním se pravděpodobně nacházejí na místě uvedeném v příkazu. Této pravomoci se často využívá v případech, kdy je zapotřebí, aby policie provedla prohlídku určitého místa, protože hrozí nebezpečí, že by důkazy mohly být zničeny, pokud by společnosti bylo doručeno předvolání nebo jiný příkaz k předložení informací. Osoba, která je předmětem prohlídky nebo jejíž majetek je předmětem prohlídky, může usilovat o to, aby byly prohlášený za neplatné důkazy získané při nezákonné prohlídce nebo z této prohlídky odvozené, pokud jsou tyto důkazy použity proti této osobě během trestního řízení. Viz věc *Mapp v. Ohio*, 367 U.S. 643 (1961). Je-li držitel údajů povinen údaje na základě příkazu zpřístupnit, může povinná strana požadavek na zpřístupnění napadnout jako nepřiměřeně zatěžující. Viz věc *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir. 1979) (ve které bylo rozhodnuto, že „řádný proces vyžaduje slyšení o otázce zátěže před tím, než bude telefonní společnost nucena poskytnout“ pomoc na základě příkazu k prohlídce), *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980) (stejný závěr vychází z dozorového úřadu soudu).

Pokyny a postupy Ministerstva spravedlnosti: Navíc k těmto ústavním, zákonným a na pravidlech založeným omezením vládního přístupu k údajům vydal ministr spravedlnosti pokyny, které dále omezují přístup donucovacích orgánů k údajům a které také obsahují ochranu soukromí a občanských svobod. Například pokyny ministra spravedlnosti pro vnitrostátní operace úřadu FBI (září 2008), dostupné na adrese <http://www.justice.gov/archive/opa/docs/guidelines.pdf>, stanoví omezení pro využití vyšetřovacích prostředků pro získávání informací souvisejících s vyšetřováním, které se týká federálních trestných činů. Tyto pokyny vyžadují, aby úřad FBI využíval co nejméně obtěžující proveditelné vyšetřovací metody se zohledněním jejich účinku na ochranu soukromí a občanských svobod a na možné poškození dobrého jména. Dále se v nich uvádí, že „úřad FBI zásadně musí svá vyšetřování i jiné činnosti vést zákonným a přiměřeným způsobem, který respektuje svobodu a soukromí a vyhýbá se zbytečnému narušování životů lidí dodržujících zákony“. Viz Pokyny ministra spravedlnosti pro vnitrostátní operace úřadu FBI, s. 5. Úřad FBI tyto pokyny provedl prostřednictvím operační příručky úřadu FBI pro vnitrostátní vyšetřování, která je dostupná na adrese <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DI0G%29>, a která je komplexní příručkou, jež zahrnuje podrobná omezení týkající se používání vyšetřovacích nástrojů a pokyny pro zajištění ochrany občanských svobod a soukromí ve všech vyšetřováních. Další pravidla a postupy ukládající omezení vyšetřovacích činností federálních státních zástupců jsou stanoveny v příručce pro výkon spravedlnosti, která je rovněž dostupná online na adrese <https://www.justice.gov/jm/justicemanual>.

#### Občanské a regulační orgány (veřejný zájem):

<sup>(4)</sup> Kromě toho § 2705 písm. b) zákona o uchovávaných komunikacích opravňuje vládu k získání soudního příkazu na základě prokázané potřeby ochrany před zveřejněním, který poskytovateli komunikačních služeb zakazuje dobrovolně informovat své uživatele o přijetí právního postupu podle zákona o uchovávaných komunikacích. V říjnu 2017 vydal zástupce ministra spravedlnosti Rod Rosenstein pro právníky a agenty Ministerstva spravedlnosti memorandum, v němž stanovil pokyny s cílem zajistit, aby žádosti o vydání takových ochranných příkazů byly přizpůsobeny konkrétním skutečnostem a obavám šetření, a stanovil obecný strop na jeden rok, pokud jde o dobu, po kterou se může žádost domáhat odkladu. V květnu 2022 vydala zástupkyně ministra spravedlnosti Lisa Monacová doplňující pokyny k tomuto tématu, které mimo jiné stanovily interní požadavky na schválení Ministerstvem spravedlnosti pro žádosti o prodloužení ochranného příkazu nad rámec počátečního období jednoho roku a vyžadovaly ukončení ochranných příkazů na konci vyšetřování.

Existují také významná omezení přístupu občanských nebo regulačních orgánů (tj. „orgánů ve veřejném zájmu“) k údajům držným společnostmi ve Spojených státech. Agentury s občanskými a regulačními úkoly mohou vydávat předvolání pro společnosti k předložení obchodních záznamů, elektronicky uchovávaných informací nebo hmotných předmětů. Výkon pravomoci vydávat správní nebo občanská předvolání mají tyto agentury omezen nejen prostřednictvím svých institucionálních zákonů, ale také prostřednictvím nezávislého soudního přezkumu předvolání před jejich potenciálním soudním výkonem. Viz např. Fed. R. Civ. P. 45. Agentury mohou usilovat o přístup pouze k těm údajům, které jsou relevantní pro záležitosti v rámci jejich regulační pravomoci. Dále může adresát správního předvolání napadnout výkon předvolání u soudu tím, že předloží důkazy, že agentura nejednala v souladu se základními standardy přiměřenosti, o nichž se zde hovořilo dříve.

Podle specifických odvětví společností a typů údajů, které vlastní, existují ještě další právní základy k tomu, aby mohly společnosti napadnout žádosti vládních agentur o poskytnutí údajů. Například finanční instituce mohou správní předvolání k předložení určitých typů informací napadnout jako porušení zákona o bankovním tajemství a jeho prováděcích předpisů. 31 U.S.C. § 5318; 31 C.F.R. kapitola X. Další podniky se mohou opřít o zákon o spravedlivém informování o úvěrové spolehlivosti (Fair Credit Reporting Act), 15 U.S.C. § 1681b, nebo o řadu dalších zákonů specifických pro daná odvětví. Zneužití pravomoci agentury vydávat předvolání může vést k odpovědnosti agentury nebo k osobní odpovědnosti jejích pracovníků. Viz např. zákon o právu na finanční soukromí (Right to Financial Privacy Act), 12 U.S.C. § 3401–3423. Soudy ve Spojených státech tak chrání před neoprávněnými regulačními požadavky a poskytují nezávislý dohled nad kroky federálních agentur.

A konečně, veškeré zákonné pravomoci, které vládní orgány mají ohledně fyzického zadržení záznamů společnosti ve Spojených státech na základě administrativní prohlídky, musí splňovat požadavky čtvrtého dodatku. Viz *See v. City of Seattle*, 387 U.S. 541 (1967).

Závěr:

Veškeré činnosti prosazování práva a regulační činnosti ve Spojených státech musí být v souladu s příslušným právem, včetně Ústavy Spojených států, zákonů, pravidel a dalších předpisů. Tyto činnosti také musí být v souladu s příslušnými postupy, včetně pokynů ministra spravedlnosti, které upravují federální činnosti prosazování práva. Výše popsany právní rámec omezuje schopnost donucovacích a regulačních agentur Spojených států získávat informace od společností ve Spojených státech – ať už jde o informace týkající osob USA nebo osob, které nejsou osobami USA –, a navíc umožňuje soudní přezkum veškerých žádostí vlády o údaje v rámci těchto pravomocí.

  
Bruce C. Swartz  
Deputy Assistant Attorney General and  
Counselor for International Affairs

## PŘÍLOHA VII

## GENERÁLNÍ RADA ÚŘADU ŘEDITELE NÁRODNÍCH ZPRAVODAJSKÝCH SLUŽEB

WASHINGTON, DC 20511

9. prosince 2022

Generální poradkyně  
Leslie B. Kiernanová  
Ministerstvo obchodu  
USA 1401 Constitution  
Ave., NW Washington, DC 20230

Vážená paní Kiernanová,

dne 7. října 2022 podepsal prezident Biden výkonný dekret č. 14086 o posílení záruk pro činnosti USA v oblasti signálového zpravodajství, který posiluje soubor přísných záruk v oblasti soukromí a občanských svobod, jež se vztahují na činnosti USA v oblasti signálového zpravodajství. Mezi tyto záruky patří: požadavek, aby činnosti v oblasti signálového zpravodajství splňovaly vyjmenované legitimní cíle, výslovné vyloučení těchto činností pro účely konkrétních zakázaných cílů, zavedení nových postupů pro zajištění toho, aby činnosti v oblasti signálového zpravodajství podporovaly tyto legitimní cíle a nepodporovaly cíle zakázané, požadavek, aby činnosti v oblasti signálového zpravodajství byly prováděny pouze poté, co bylo na základě přiměřeného posouzení všech relevantních faktorů rozhodnuto, že tyto činnosti jsou nezbytné k prosazování potvrzené zpravodajské priority, a pouze v rozsahu a způsobem, který je přiměřený potvrzené zpravodajské prioritě, pro kterou byly schváleny, a směřování prvků zpravodajské komunity k aktualizaci jejich politik a postupů tak, aby odrážely požadované záruky činností v oblasti signálového zpravodajství podle výkonného dekretu. Nejpodstatnější je, že výkonný dekret rovněž zavádí nezávislý mechanismus, jehož rozhodnutí jsou závazná, který fyzickým osobám z „kvalifikovaných států“ určených na základě výkonného dekretu umožňuje domáhat se nápravy, pokud se domnívají, že byli vystaveni nezákonným činnostem USA v oblasti signálového zpravodajství, včetně činností porušujících ochranu stanovenou ve výkonném dekretu.

Vydání výkonného dekretu č. 14086 prezidentem Bidenem bylo výsledkem podrobných jednání trvajících déle než rok mezi zástupci Evropské komise (EK) a Spojených států amerických a řídí kroky, které Spojené státy podniknou k plnění svých závazků vyplývajících z rámce EU–USA pro ochranu údajů. V duchu spolupráce, ve kterém byl tento rámec vypracován, jsem si vědom toho, že jste od EK obdržela dva soubory otázek ohledně toho, jak bude zpravodajská komunita výkonný dekret provádět. Jsem rád, že mohu v tomto dopise na tyto otázky odpovědět.

*Ustanovení § 702 zákona o dohledu nad zahraniční informační službou z roku 1978 (zákon FISA, § 702)*

První soubor otázek se týká ustanovení § 702 zákona FISA, který umožňuje shromažďování zahraničních zpravodajských informací prostřednictvím zacílení na osoby, které nejsou osobami USA a o nichž se lze důvodně domnívat, že se nacházejí mimo Spojené státy, s povinnou součinností poskytovatelů služeb elektronických komunikací. Konkrétně se otázky týkají vzájemného působení tohoto ustanovení a výkonného dekretu č. 14086, jakož i dalších záruk, které se vztahují na činnosti prováděné podle ustanovení § 702 zákona FISA.

Na úvod můžeme potvrdit, že zpravodajská komunita použije záruky stanovené ve výkonném dekretu č. 14086 na činnosti prováděné podle ustanovení § 702 zákona FISA.

Kromě toho se na použití ustanovení § 702 zákona FISA vládou vztahuje řada dalších záruk. Například všechna osvědčení podle ustanovení § 702 zákona FISA musí být podepsána jak ministrem spravedlnosti, tak ředitelem národních zpravodajských služeb a vláda musí předložit všechna tato osvědčení ke schválení Soudu pro uplatňování zákona FISA, který se skládá z nezávislých soudců, kteří vykonávají funkci soudce doživotně, ale u tohoto soudu působí pouze po dobu sedmi let bez možnosti prodloužení. Osvědčení určují kategorie zahraničních zpravodajských informací, jež mají být shromažďovány, které musí splňovat zákonnou definici zahraničních zpravodajských informací, prostřednictvím zacílení na osoby, které nejsou osobami USA a o nichž se lze důvodně domnívat, že se nacházejí mimo Spojené státy. Osvědčení obsahují informace týkající se mezinárodního terorismu a dalších témat, jako je získávání informací o zbraních hromadného ničení. Každoroční osvědčení musí být předložena Soudu pro uplatňování zákona FISA ke schválení v balíčku žádosti o osvědčení, který zahrnuje osvědčení ministra spravedlnosti a ředitele národních zpravodajských služeb, čestná prohlášení některých vedoucích pracovníků zpravodajských služeb a postupy cíleného sběru, minimalizační postupy a postupy dotazování, které jsou pro vládu závazné. Postupy cíleného sběru mimo jiné vyžadují, aby zpravodajská komunita na základě souhrnu okolností přiměřeně posoudila, že cílení pravděpodobně povede ke shromažďování zahraničních zpravodajských informací uvedených v osvědčení podle § 702 zákona FISA.

Kromě toho při shromažďování informací podle § 702 zákona FISA musí zpravodajská komunita: poskytnout písemné vysvětlení základu pro své posouzení v době zacílení, že se očekává, že daný cíl má, obdrží nebo pravděpodobně předá zahraniční zpravodajské informace uvedené v osvědčení podle § 702 zákona FISA, potvrdit, že norma pro cílení stanovená v § 702 zákona FISA je stále naplňována, a v případě, že norma již není plněna, zastaví sběr. Viz podání vlády USA k Soudu pro uplatňování zákona FISA, 2015, *shrnutí významných požadavků podle § 702 zákona*, s. 2–3 (15. července 2015).

Požadavek, aby zpravodajská komunita písemně zaznamenávala a pravidelně potvrzovala platnost svého posouzení, že cíle § 702 zákona FISA splňují platné normy pro cílení, usnadňuje dohled Soudu pro uplatňování zákona FISA nad činnostmi zpravodajské komunity v oblasti cílení. Každé zaznamenané posouzení cílení a odůvodnění jsou každé dva měsíce přezkoumávány zástupci pro dohled nad zpravodajskými službami Ministerstva spravedlnosti, kteří tuto funkci dohledu vykonávají nezávisle na zahraničních zpravodajských operacích. Oddělení Ministerstva spravedlnosti, které tuto funkci vykonává, je pak podle dlouho zavedeného pravidla Soudu pro uplatňování zákona FISA odpovědné za to, že bude Soudu pro uplatňování zákona FISA oznamovat veškerá porušení platných postupů. Toto oznamování spolu s pravidelnými schůzkami mezi Soudem pro uplatňování zákona FISA a tímto oddělením Ministerstva spravedlnosti, které se týkají dohledu nad cílením podle § 702 zákona FISA, umožňuje Soudu pro uplatňování zákona FISA vymáhat dodržování § 702 zákona FISA a dalších postupů a jinak zajistit, aby činnost vlády byla zákonná. Soud pro uplatňování zákona FISA tak může učinit zejména několika způsoby, mimo jiné vydáním závazných nápravných rozhodnutí o ukončení pravomoci vlády shromažďovat údaje proti určitému cíli nebo o změně či odložení shromažďování údajů podle § 702 zákona FISA. Soud pro uplatňování zákona FISA může rovněž požadovat, aby vláda poskytla další zprávy nebo informace o tom, jak dodržuje předpisy týkající se cílení a jiné postupy, nebo může požadovat změny těchto postupů.

#### *Hromadné shromažďování informací prostřednictvím signálového zpravodajství*

Druhý soubor otázek se týká „hromadného“ shromažďování informací prostřednictvím signálového zpravodajství, které je ve výkonném dekretu č. 14086 definováno jako „oprávněný sběr velkého objemu údajů v oblasti signálového zpravodajství, které jsou z technických nebo operativních důvodů získávány bez použití diskriminantů (například bez použití konkrétních identifikátorů nebo selekčních termínů).“

Pokud jde o tyto otázky, je třeba nejprve konstatovat, že ani zákon FISA, ani National Security Letters nepovolují hromadné shromažďování. Pokud jde o zákon 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 důvodné podezření, že cílem je cizí moc nebo agent cizí moci. Viz 50 U.S.C. § 1805, 1824.
- Zákon USA FREEDOM Act z roku 2015 změnil hlavu IV zákona FISA, která na základě soudního příkazu povoluje použití zařízení pro zaznamenávání informací o odchozí komunikaci sledovaného zařízení (pen register) nebo zařízení pro zaznamenávání informací o příchozí komunikaci sledovaného zařízení (trap and trace) (s výjimkou mimořádných okolností), s cílem požadovat, aby vláda založila své žádosti na „konkrétním selekčním termínu“. Viz 50 U.S.C. § 1842 (c)(3).

- Hlava V zákona FISA, která umožňuje Federálnímu úřadu pro vyšetřování (FBI) získat určité druhy obchodních záznamů, vyžaduje soudní příkaz založený na návrhu, který upřesňuje, že „existují konkrétní a srozumitelné skutečnosti, které odůvodňují domněnku, že osoba, jíž se záznamy týkají, je cizí mocí nebo agentem cizí moci.“ Viz 50 U.S.C. § 1862(b)(2)(B) <sup>(1)</sup>.
- Konečně § 702 zákona FISA povoluje „cílení na osoby, o nichž se lze důvodně domnívat, že se nacházejí mimo Spojené státy, za účelem získání zahraničních zpravodajských informací.“ Viz 50 U.S.C. § 1881a(a). Jak tedy uvedl Výbor pro dohled nad ochranou soukromí a občanských svobod, shromažďování údajů vládou podle § 702 zákona FISA „zahrnuje výhradně cílení na jednotlivé osoby, od nichž vláda oprávněně očekává, že získá určité druhy zahraničních zpravodajských informací, a získávání komunikace s těmito osobami spojené“, takže „program nefunguje na základě hromadného shromažďování komunikací.“ Výbor pro dohled nad ochranou soukromí a občanských svobod, *Zpráva o programu sledování podle § 702 zákona o dohledu nad zahraniční informační službou*, s. 103 (2. července 2014) <sup>(2)</sup>.

Pokud jde o National Security Letters, zákon USA FREEDOM Act z roku 2015 stanoví pro jejich použití požadavek na „konkrétní selekční termín“. 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 dekret č. 14086 dále stanoví, že „cílený sběr je upřednostňován“ a že pokud zpravodajská komunita provádí hromadné shromažďování, „musí být hromadné shromažďování informací prostřednictvím činností v oblasti signálového zpravodajství povoleno pouze na základě rozhodnutí [...], že informace nezbytné k prosazování potvrzené zpravodajské priority nelze přiměřeně získat cíleným sběrem.“ Viz výkonný dekret č. 14086, § 2(c)(ii)(A).

Kromě toho, pokud zpravodajská komunita rozhodne, že hromadný sběr tyto normy splňuje, stanoví výkonný dekret č. 14086 další záruky. Výkonný dekret konkrétně vyžaduje, aby zpravodajská komunita při hromadném shromažďování „používala přiměřené metody a technická opatření s cílem omezit shromažďované údaje pouze na to, co je nezbytné k dosažení souladu s potvrzenou zpravodajskou prioritou, a zároveň minimalizovat shromažďování informací, které nejsou relevantní.“ Viz *tamtéž*. Dekret rovněž uvádí, že „činnosti v oblasti signálového zpravodajství“, které zahrnují dotazování na informace signálového zpravodajství získané hromadným shromažďováním, se provádějí pouze na základě rozhodnutí založeného na přiměřeném posouzení všech relevantních faktorů, že tyto činnosti jsou nezbytné k dosažení potvrzené zpravodajské priority.“ Viz *tamtéž*. § 2(a)(ii)(A). Dekret tuto zásadu dále provádí tím, že uvádí, že se zpravodajská komunita může dotazovat na informace signálového zpravodajství, které nejsou minimalizované a které jsou získané hromadně, pouze při sledování šesti přípustných cílů a že tato dotazování musí být prováděna v souladu s politikami 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 *tamtéž*. § 2(c)(iii)(D). V neposlední řadě dekret stanoví kontroly nakládání se shromážděnými údaji, jejich zabezpečení a kontroly přístupu k nim. Viz *tamtéž*. § 2(c)(iii)(A) a § 2(c)(iii)(B).

\* \* \* \* \*

Doufáme, že tato objasnění budou užitečná. Neváhejte se na nás obrátit, máte-li další dotazy ohledně toho, jak zpravodajská komunita USA plánuje tento výkonný dekret č. 14086 provést.

<sup>(1)</sup> Od roku 2001 do roku 2020 umožňovala hlava V zákona FISA, aby úřad FBI požádal Soud pro uplatňování zákona FISA o povolení k získání „hmatatelných věcí“, které jsou relevantní pro určitá povolená vyšetřování. Viz zákon 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 metadata o telefonních hovorech. Ještě předtím, než toto ustanovení přestalo platit, však bylo zákonem USA FREEDOM Act změněno tak, aby vláda musela žádost k Soudu pro uplatňování zákona FISA opřít o „konkrétní selekční termín“. Viz USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268, § 103 (2015).

<sup>(2)</sup> Ustanovení § 703 a § 704, které povolují, aby se zpravodajská komunita zaměřovala na osoby USA nacházející se v zahraničí, vyžadují soudní příkaz (s výjimkou mimořádných okolností) a vždy vyžadují důvodné podezření, že cílem je cizí moc, agent cizí moci nebo vedoucí pracovník či zaměstnanec cizí moci. Viz 50 U.S.C. § 1881b, 1881c.

Sincerely,

A handwritten signature in black ink, appearing to read 'C. FONZONE', followed by a horizontal line that ends in a vertical bar.

Christopher C. FONZONE  
generální rada

\_\_\_\_\_

## PŘÍLOHA VIII

**Seznam zkratk**

V tomto rozhodnutí jsou uvedeny tyto zkratky:

|                                 |                                                                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AAA                             | Americká arbitrážní asociace                                                                                                                                                                                |
| AGG-DOM                         | Pokyny ministra spravedlnosti pro vnitrostátní operace úřadu FBI                                                                                                                                            |
| APA                             | Zákon o správním řízení                                                                                                                                                                                     |
| CIA                             | Ústřední zpravodajská služba                                                                                                                                                                                |
| CNSS                            | Výbor pro národní bezpečnostní systémy                                                                                                                                                                      |
| DNI                             | Ředitel národních zpravodajských služeb                                                                                                                                                                     |
| ECPA                            | Zákon o soukromí elektronických komunikací                                                                                                                                                                  |
| EHP                             | Evropský hospodářský prostor                                                                                                                                                                                |
| EO 12333                        | Výkonný dekret č. 12333 „Zpravodajské činnosti USA“                                                                                                                                                         |
| EO 14086                        | Výkonný dekret č. 14086 „Posílení záruk pro činnosti USA v oblasti signálového zpravodajství“                                                                                                               |
| FBI                             | Federální úřad pro vyšetřování                                                                                                                                                                              |
| FISA                            | Zákon o dohledu nad zahraniční informační službou                                                                                                                                                           |
| FISC                            | Soud pro uplatňování zákona FISA                                                                                                                                                                            |
| FISCR                           | Odvolací soud pro uplatňování zákona FISA                                                                                                                                                                   |
| FOIA                            | Zákon o svobodě informací                                                                                                                                                                                   |
| FRA                             | Zákon o federálních záznamech                                                                                                                                                                               |
| FTC                             | Federální obchodní komise                                                                                                                                                                                   |
| ICDR                            | Mezinárodní středisko pro řešení sporů                                                                                                                                                                      |
| MD                              | Ministerstvo dopravy USA                                                                                                                                                                                    |
| Nařízení (EU) 2016/679          | 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 |
| Nařízení ministra spravedlnosti | Nařízení ministra spravedlnosti o Soudu pro přezkum ochrany údajů                                                                                                                                           |
| NSA                             | Národní bezpečnostní agentura                                                                                                                                                                               |
| NSL                             | tzv. <i>National Security Letter(s)</i>                                                                                                                                                                     |
| ODNI                            | Úřad ředitele národních zpravodajských služeb                                                                                                                                                               |
| ODNI CLPO, CLPO                 | Úředník pro ochranu občanských svobod Úřadu ředitele národních zpravodajských služeb                                                                                                                        |
| OMB                             | Úřad pro řízení a rozpočet                                                                                                                                                                                  |
| OPCL                            | Úřad pro ochranu soukromí a občanských svobod ministerstva spravedlnosti                                                                                                                                    |
| PCLOB                           | Výbor pro dohled nad ochranou soukromí a občanských svobod                                                                                                                                                  |
| PPD 28                          | Prezidentská politická směrnice 28                                                                                                                                                                          |
| Rámec pro ochranu údajů         | Rámec EU–USA pro ochranu údajů                                                                                                                                                                              |

|             |                                                                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rozhodnutí  | Prováděcí rozhodnutí Komise podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o odpovídající úrovni ochrany osobních údajů poskytované rámcem EU–USA pro ochranu údajů |
| SAOP        | Vyšší úředník agentury pro ochranu soukromí                                                                                                                                    |
| Soudní dvůr | Soudní dvůr Evropské unie                                                                                                                                                      |
| USA         | Spojené státy                                                                                                                                                                  |
| Unie        | Evropská unie                                                                                                                                                                  |
| Zásady      | Zásady rámce EU–USA pro ochranu údajů                                                                                                                                          |